Improving Privacy in e-Governance in a Country like India using Attribute-based Cryptographic Schemes

Thesis submitted in partial fullfilment of the requirements
for the award of the degree of

Doctor of Philosophy

in

Computer Science and Engineering

by

Puneet Bakshi
146101009

Under the supervision of

Prof. Sukumar Nandi

Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati
Guwahati - 781039 Assam India
August 17, 2021

This page intentionally left blank.

Dedication

Dedicated to all my teachers who taught me to assimilate the information to convert it into knowledge.

This page intentionally left blank.

Acknowledgement

I would like to express my sincere thanks and gratitude to my supervisor *Prof. Sukumar Nandi*, who always provided his support, knowledge and guidance throughout my research work. Even during my M.Tech., he was one of the most inspiring teachers. I am truly grateful to him for his constant endeavour to ensure that I am on the right direction in my research work. Other than academic leanings, I also learned quite many things from him in my professional as well as in my personal life, which helped me improve my learnings, attitude and personality.

I am also very thankful to my doctoral committee members, *Prof. Jatindra Kumar Deka*, *Dr. Aryabartta Sahu* and *Dr. Gaurav Trivedi* for providing their valuable comments which helped me refine my research work.

I would also like to express my hearty gratitude to *Prof. Dr. T. G. Sitharam* (the present director of the institute), all the past directors, all the Deans and other officials of IIT Guwahati, whose collective efforts have made this institute a place for world-class studies and research. I am thankful to all the faculties and the staffs of the Department of Computer Science and Engineering for extending their cooperation in terms of technical and official support. It is difficult to include all the names, but, I also want to express my thanks for the research scholars with whom I worked closely and who helped me in various ways.

I also want to express my sincere thanks to *Prof. Rajat Moona*, the ex-Director General of Centre for Development of Advanced Computing (C-DAC) with whom I had many insightful, technical and motivating discussions. I am also very grateful to C-DAC in general for providing me with the opportunity to pursue my research work along with my official commitments and also to provide the necessary support to carry out the same.

Last, but not the least, I want to express my gratitude for my parents *Sh. T K Bakshi* and *Smt. Asha Bakshi*, who took all the pains to raise me, to educate me and to nurture me in many facets of my life. I want to express my sincere thanks to my wife *Preeti Bakshi* who took most of the family responsibilities to her shoulder so that I can concentrate on my research work.

Finally, I also want to acknowledge the collaborators and anonymous reviewers who helped me explore innovative research areas, refine my work and encourage me

to solve new problems.

Place: IIT Guwahati
Date:

Puneet Bakshi
Department of Computer Science and Engineering,
Indian Institute of Technology Guwahati,
Guwahati, India 781039

Declaration

I declare that

1. The work contained in this thesis is original and has been done by myself under the general supervision of my supervisor.

2. The work has not been submitted to any other Institute for any degree or diploma.

3. Whenever I have used materials (data, theoretical analysis, results) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.

4. Whenever I have quoted written materials from other sources, I have put them under quotation marks and given due credit to the sources by citing them and giving required details in the references.

Place: IIT Guwahati
Date: August 17, 2021

Puneet Bakshi
Research Scholar
Department of Computer Science and Engineering,
Indian Institute of Technology Guwahati,
Guwahati, India 781039

This page intentionally left blank.

Department of Computer Science and
Engineering
Indian Institute of Technology Guwahati
Guwahati - 781039 Assam India

Certificate

This is to certify that this thesis titled **"Improving Privacy in e-Governance in a Country like India using Attribute-based Cryptographic Schemes"** submitted by **Puneet Bakshi** (Roll No. 146101009), in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy, to the Indian Institute of Technology Guwahati, Assam, India, is a record of the bonafide research work carried out by him under my guidance and supervision at the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, Assam, India. To the best of my knowledge, no part of the work reported in this thesis has been presented for the award of any degree at any other institutions.

Place: IIT Guwahati
Date: August 17, 2021

Sukumar Nandi
Thesis Supervisor
Department of Computer Science and Engineering,
Indian Institute of Technology Guwahati,
Guwahati, India 781039

This page intentionally left blank.

ABSTRACT

To improve Governance and curb inefficiencies in it, Government of India entrusted UIDAI to initiate an ambitious project in the year 2009 to assign a unique identity to each resident of India. UIDAI started its mission to enrol residents of India and has so far enrolled more than one billion adult residents above the age of 18. As part of enrollment of a resident, his/her personal and demographic information is registered in a central repository and a unique 12 digit identity number, referred to as *Aadhaar*, is assigned to the resident. Since the establishment of Aadhaar, Government has built various online digital services such as eSign, DigiLocker, etc. using APIs known as India Stack. Recently, critiques have raised some privacy and security-related concerns in the Aadhaar project. Although the remedial measures have been prescribed by researchers, they are at a very high level. Even amidst these concerns, we think Aadhaar is a courageous initiative in a developing country like India and if implemented in the right way has the potential to help India compete in digital revolution across the world. This research presents schemes to improve the privacy of Aadhaar based e-Governance services. The proposed schemes use Attribute-based Access Control and cryptographic mechanisms such as Attribute-Based Signature, Attribute-Based Encryption and Ciphertext Policy Attribute-Based Encryption. This research presents five major contributions to improve privacy of Aadhaar-based e-Governance services in India.

The first contribution is to present privacy-enhanced eSign model in which participating entities such as users, UIDAI and ESP can enforce their privacy policies by encoding them in specially devised digital tokens. In the present model of eSign, subscriber's eKYC information is retrieved in full and is given in full for unlimited time to all the entities who receives boolean consent from the subscriber. This access mechanism reflects a restrictive *self-only, full-resource and unlimited* access control. A subscriber may wish to have a better fine-grained access control mechanism that allows third entities to access part of a resource that can be used only for a specific purpose and only for a limited time. The proposed scheme reflects a *third-entity-also, partial resource, use-limited and time-limited* fine-grained access mechanism. A formal security analysis is presented using Burrows-Abadi-Needham (BAN) logic.

The second contribution is to present privacy-enhanced eSign model in which the signer signs the document using his attributes and does not have to reveal his identity for the verifier to verify the signed document. This is an improvement over the present model of eSign in which identity of the signer is revealed to the receiver, which may not be required in some cases and may not even be suitable.

For example, the same person can hold multiple roles in an organisation such as an employee of an organization, principal investigator of a project, executive director of an organisation and even an interim director-general. In certain cases, the role of the person is important in signature rather than his/her name. The proposed scheme uses attribute-based signature and devised a digital token to improve the performance of the eSign process.

The third contribution is to present privacy-enhanced DigiLocker in which subscriber can encrypt his documents with a privacy policy so that only those requesters whose attributes satisfy the privacy policy can decrypt and retrieve the document. In the present model of DigiLocker, subscriber's documents are hosted on a public cloud which is assumed to be a trusted entity. However, cloud storage may not be trustworthy and may be susceptible to insider attacks. Moreover, instead of providing a reactive access authorization to a single requester, a subscriber may want to provide a proactive fine-grained access authorization to multiple requesters meeting certain criteria of attributes. The proposed scheme is proved to be secure against an adaptive chosen-plaintext attack (CPA) if any polynomial-time adversary has only a negligible advantage in the IND-sAtt-CPA game.

The fourth contribution is to present a privacy-enhanced scheme in an automated toll tax collection service in which a vehicle does not have to disclose its identity to the toll station to get a toll ticket. The proposed scheme uses lightweight operations such as cryptographic hash, XOR and concatenation functions. A formal security analysis is presented using Burrows-Abadi-Needham (BAN) logic.

The fifth contribution is to present privacy-enhanced scheme for registered devices in which a genuine device is recognized not just by its model number and serial number but by its attributes which can be assigned to it by multiple authorities and the device signs each message with its attributes. Registered devices are designated devices in the Aadhaar ecosystem which is used to capture and transmit biometric. Biometric is sensitive data and utmost care should be taken to ensure the security of devices carrying them. The use of these devices is expected to grow more and such devices are expected to carry more than just biometric data such as personal identifiable information, financial data, medical data, etc. Although at present, this model may suffice, with the proliferation of connected devices and online services, registered devices may soon become ubiquitous, required to operate remotely and to process other sensitive personal data as well. In a ubiquitous world of registered devices, an application may want to query and use a valid registered device having a specific set of attributes rather than a registered device having a specific random string of serial number or model number. Since the identity of the device may be

correlated with the identity of its owner, the owner of the device may not want to disclose the identity of the device to protect his privacy. The owner may just want to let the device be recognized as a valid registered device having a certain set of attributes.

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

List of Tables

This page intentionally left blank.

Chapter 1

Introduction

1.1 Introduction

The economic and social growth of a country depends significantly on its Governance policies. *Governance* of a nation is defined by a set of rules, regulations and policies about how decisions are taken on public resources and how those decisions are implemented by public organizations. These rules, regulations and policies are mutually decided by Government, citizens and entrepreneurs in the country. *Good Governance* is a relative term to indicate better transparency, efficiency and effectiveness in the process of Governance. Using Information and Communication Technology (ICT) in Governance is commonly referred to as e-Governance.

Since Governance is one of the most vital factors in the economic and social growth of a country, removing inefficiencies in it has straight implication on the betterment of a country. For example, although the Government of India has taken several initiatives for the social welfare of the country, their effectiveness is not as expected [1]. For the success of any welfare scheme, it is expected that the benefits of that scheme are received by an expected set of people and should not have leakages. Some of the hindrances in the effectiveness of such schemes are the inability of people to prove their identity and the presence of fake or duplicate identities [1]. To improve the efficiency and the effectiveness of such schemes, the Government of India entrusted Unique Identification Authority of India (UIDAI) with a mission to assign each resident of India, a unique identity. UIDAI started its mission to enrol each resident of India in the year 2009. To enrol himself/herself, a resident needs to provide his/her personal and demographic information such as address, mobile number, biometric (10 fingerprint, 2 iris scans and one photograph) to UIDAI which

are registered in a central repository. Once registered, each resident is assigned a unique 12 digit identity number called *Aadhaar*. UIDAI has so far registered 90% of the adult population above the age of 18 and has also become the world's largest biometric program with over 1.2 billion people enrolled [2].

Layer	**Provider**	**Functionality**	**Uses**
Presenceless	UIDAI	Authentication	Service Delivery Authentication Direct Benefits Transfer
Paperless	UIDAI	KYC	Bank Account Opening SIM issuance
	CAs	eSign DIgital Signature	Contracts, Agreements
	MeitY	Document	Consented Document Sharing
	DigiLocker		
Cashless	NPCI/UPI	Payments	Retail payments, including P2P, P2M, Govt. through mobile
	AEPS, Aadhaar Pay	Payments	Cash deposit/Withdrawl, Transfers, Merchant payments using biometric auth
	IMPS	Payments	Remittances, Mobile Payments
Consent	NBCFC-AA	Financial Data	Personal Finance Management,

Table 1.1: India Stack APIs

Since the establishment of Aadhaar, the government has built various online digital services such as eSign, DigiLocker, etc. using application programming interfaces, known as India Stack, which is spearheaded by private think tank iSPIRT [3]. iSPIRT describes India Stack as a set of APIs that allows governments, businesses, startups and developers to utilize a unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery. Table 1.1 lists some of the most common India Stack APIs grouped in four layers.

Though promoters of Aadhaar and India Stack consider them the instruments to conduct transparent interactions among entrepreneurs, residents and Government [4] [5], critiques of Aadhaar have raised concerns about the impact, limitations and effectiveness of the project in improving the overall welfare system in the country. For example, Khera [6] pointed out three common frauds that happen in society. First is "Eligibility Fraud", in which ineligible persons are able to enrol in social welfare schemes by providing fake documents. Second is "Quantity Fraud", in which

eligible persons are unable to receive their full entitlements. Third is "Identity Fraud", in which one person's benefits are claimed by another person by providing duplicate identities. Khera mentioned that Aadhaar ecosystem can help eliminate identity fraud only and not the eligibility fraud or the quantity fraud. Thaker [1] also cautions out against a possible conflict of interest due to relationship among Aadhaar, India Stack and certain private-sector firms. Apart from these, more recently, researchers [1], [6], [7], have raised concerns over privacy and security issues related to Aadhaar. Some of these concerns are listed below.

1 *Identity Theft.* Aadhaar is vulnerable to illegal usage of biometrics and identity frauds because biometrics are not secret information. Moreover, possible leakage of biometric and demographic data, either from the central Aadhaar repository or from a point-of-sale or an enrollment device, adds to the risk.

2 *Identification without consent using Aadhaar data.* There may be unauthorized use of biometrics to identify people illegally. Such violations may include identifying people by inappropriate matching of fingerprint or iris scans, or facial photographs stored in the Aadhaar database, or using the demographic data to identify people without their consent and beyond legal provisions.

3 *Correlation of identities across domains.* It may become possible to track an individual's activities across multiple domains of service using their global Aadhaar IDs, which are valid across these domains. This would lead to identification without consent.

4 *Illegal tracking of individuals.* Individuals may be tracked or put under surveillance without proper authorization or legal sanction using the authentication and identification records and trails in the Aadhaar database, or in one or more authentication-requesting-agencies. Such records may reveal information on location, time and context of authentication and the services availed.

5 *Authentication without authorization.* Aadhaar does not record the purpose of authentication. Authentication without authorization and accounting puts users at serious risks of fraud because authentication or KYC meant for one purpose may be used for another. Recording the purpose of authentication is crucial, even for offline use. Privacy-by-design is not achieved by self-imposed blindness.

6 *Lack of protection against insider attack.* The likelihood of above-mentioned attacks gets even more severe if the attacker colludes with an insider.

7 *Lack of virtual identities (which were retrofitted in a limited way).* Virtual identities can mitigate correlating identities of people across domains partially. This was missing at the beginning and was later added in a limited way.

8 *Abscence of a clear data usage policy and regulatory oversight*

9 *Lack of robust consent and purpose limitation framework and a regulatory access control architecture*

Although the same researchers have also presented possible measures to address these privacy and security-related concerns, they are described at a very high level for the actual remedial implementation.

Moreover, a direct interaction between an e-governance service and the user may not always be possible and may involve third-party entities which the user may not want to trust upon. For example, while passing through a toll booth, a user may not want to reveal his personal data including his vehicle registration number to the toll booth. Rather than providing his/her details to toll booth, he may want to hide these details from intermediate toll booth and communicate the same directly to the Regional Transport Office (RTO). At the same time, toll booth also wants to ensure that it can provide the necessary assurance to RTO that it has not granted access to any vehicle without letting it pay the necessary toll.

1.2 Research Motivation

Most of the literature on Aadhaar based eGovernance has focused on the critical reviews citing the possibility of mass surveillance and breach of individual's privacy by identifying the individual without his consent using his Aadhaar number, demographic data or biometric data. Since Aadhaar is a unique identification number, it can be used to track individual's activities across multiple agencies. This would lead to identification without consent. Biometrics may also be obtained by unauthorized means such as copying fingerprints, iris scans or facial photographs and may be used to illegally identify people without their consent. Individuals may be tracked or put under surveillance without proper authorization using authentication and identification logs in the Aadhaar database. These logs may also contain precise location, time and context of the authentication and the services used. Insider attacks may also pose serious threats. For example, the attacks are much more likely if an attacker colludes with an insider and gain access to various components of the Aadhaar system.

This raises a few questions. The first is to what extent the user data, the authentication information and the identification information are protected from unauthorized surveillance. The second is to what extent the operating processes are working as expected, for example, are these processes approved, adhere to necessary frameworks, maintain tamper-proof logs, etc.

For effective privacy protection, the Aadhaar system requires protection not only from external attacks but from insider attacks also and three fundamental requirements may be envisaged to achieve the same. The first is that the decryption control should not be with a single entity but with all the stakeholders in a collusion-resistant manner such that all stakeholders must participate to reveal the decryption key. This ensures that even if the storage server of one stakeholder is compromised, the decryption key remains protected. The second is that the subscriber's data is kept secure even if the storage server is untrusted or gets compromised. The third is that the subscriber should have control over the disclosure of his data at a fine-grained level.

Even amidst this criticism, we think Aadhaar is a courageous initiative in a developing country like India and if implemented in the right way, has the potential to help India compete in the digital revolution across the world. This motivated us to address some of the privacy concerns cited above. We think that attribute-based schemes and lightweight cryptography may be more suitable than other possible mechanisms such as homomorphic and functional encryption because of their maturity and practicality. This motivated us to use attribute-based schemes such as attribute-based access control, attribute-based signatures, attribute-based encryption and ciphertext-policy attribute-based encryption.

1.3 Research Problem

This research work aims to improve privacy of some of the Aadhaar-based e - Governance services such as eSign, DigiLocker, Registered Devices and toll-payment using attribute-based schemes and lightweight cryptography. This work also aims to ensure that the proposed schemes are cryptographically secure by doing necessary cryptanalysis.

1.4 Research Benefits

This research work does not claim that it has addressed all of the privacy concerns related to Aadhaar based e-Governance or even that the outcome of this work can

be applied directly to the actual project, but the outcome of this work can certainly be helpful as one of the reference model which if applied in the right way can address some of the privacy concerns in Aadhaar based e-Governance, benefitting all participating entities, namely, Government, resident and entrepreneurs.

1.5 Research Focus

The focus of this research work is to use attribute-based schemes such as attribute-based access control, attribute-based signatures, attribute-based encryption, ciphertext - policy attribute-based encryption and lightweight cryptography in some of the existing e-Governance schemes such as eSign, DigiLocker, Registered Devices and toll-payment and propose corresponding privacy enhanced e-Governance schemes. Necessary cryptanalysis is done to ensure security of proposed schemes. For the practical realization of the proposed work, many other aspects should also be considered such as laying out appropriate standards, guidelines, policies and procedures for software development, testing, auditing, and infrastructure, but they are kept out of scope for this work.

1.6 Contributions of this thesis

The major contributions of this thesis are listed below in brief.

1 The present model of eSign is based on traditional RSA-based cryptography in which subscriber's eKYC information is retrieved in full and is given in full for unlimited time to all the entities who receives boolean consent from the subscriber. This access mechanism reflects a restrictive *self-only, full-resource and unlimited* access control. A subscriber may wish to have a better fine-grained access control mechanism that allows third entities to access part of a resource that can be used only for a specific purpose and only for a limited time. One of the contributions of this thesis is to present a privacy-enhanced eSign in which subscribers, UIDAI and ESP can enforce their policies by encoding them in specially designed digital tokens.

2 The present model of eSign also reveals the identity of the signer which may not be required in some cases and may not even be suitable. For example, the same person can hold multiple roles in an organisation such as an employee of an organization, principal investigator of a project, executive director of an organisation and even an interim director-general. In certain cases, the role of the person is important in signature rather than his/her name. One

contribution of this thesis is to present a privacy-enhanced eSign in which the subscriber digitally signs his document using his/her attributes rather than his/her identity. Digital tokens are used to improve the performance of the eSign process.

3 The present model of DigiLocker is also based on traditional RSA-based cryptography in which subscriber's documents are hosted on a public cloud which is assumed to be a trusted entity. However, cloud storage may not be trustworthy and may be susceptible to insider attacks. Moreover, instead of providing a reactive access authorization to a single requester, a subscriber may want to provide a proactive fine-grained access authorization to multiple requesters meeting certain criteria of attributes. One contribution of this thesis is to present a privacy-enhanced DigiLocker in which a subscriber can encrypt documents using a privacy policy and only the entities whose attributes satisfy the policy can decrypt and retrieve the document.

4 Another contribution of this thesis is to present a mechanism to ensure security, privacy and anonymity in a vehicle to infrastructure communication in an automated collection of toll tax payment using lightweight operations such as one-way cryptographic hash, XOR and concatenation.

5 Registered devices are designated devices in the Aadhaar ecosystem which is used to capture and transmit biometric. Biometric is sensitive data and utmost care should be taken to ensure the security of devices carrying them. The use of these devices is expected to grow more and such devices are expected to carry more than just biometric data such as personal identifiable information, financial data, medical data, etc. Although at present, this model may suffice, with the proliferation of connected devices and online services, registered devices may soon become ubiquitous, required to operate remotely and to process other sensitive personal data as well. In a ubiquitous world of registered devices, an application may want to query and use a valid registered device having a specific set of attributes rather than a registered device having a specific random string of serial number or model number. Since the identity of the device may be correlated with the identity of its owner, the owner of the device may not want to disclose the identity of the device to protect his privacy. The owner may just want to let the device be recognized as a valid registered device having a certain set of attributes. One contribution of this thesis is to present a privacy-enhanced scheme of registered devices in which a registered device can sign a message using its assigned attributes which ensures that the device is a genuine and expected device.

1.7 Organization of the thesis

Following is the organization of the thesis.

1 Chapter 1 presented the research motivation, research problem, research benefits, research focus, research approach and potential limitations.

2 Chapter 2 presents the literature overview including privacy related regulations, digital identity system across world and mechanisms to address some of the privacy related concerns using tools and techniques.

3 Chapter 3 presents privacy enhanced e-Governance service, named eSign using attribute-based access control.

4 Chapter 4 presents privacy enhanced e-Governance service, named eSign using another mechanism based on Attribute-based Signature.

5 Chapter 5 presents privacy enhanced e-Governance service, named DigiLocker using Ciphertext Policy Attribute-based Encryption.

6 Chapter 6 presents privacy enhanced access to e-Governance service taking toll payment as an example

7 Chapter 7 presents privacy enhanced registered devices used to capture sensitive personal information such as biometric.

8 Chapter 8 presents the recommendations for improving the research work even further.

9 Chapter 9 presents the conclusion of the research work.

1.8 Summary

This chapter gave a brief introduction of Governance in India, Aadhaar-based initiative to achieve Good Governance, a set of APIs known as India Stack which is used to build various online digital services and some of the privacy-related concerns in Aadhaar based ecosystem. This is followed by the motivation of the research, the problem statement of the research and the benefits of the research. The chapter concludes with the contributions of the research work and the organization of the rest of the thesis.

Chapter 2

Literature Review

2.1 Introduction

This chapter presents a review of three relevant areas for this research work. First is privacy-related legislation, well-established standards, frameworks and best practices. Second is the ecosystem of digital identity systems used across the world. Third, is modern cryptography mechanisms which can facilitate in improving the privacy of existing schemes. Review of these will help in understanding state of the art in these areas, arrive at necessary privacy-related requirements, compare features of similar systems across the world and evaluate available mechanisms which can be used to address these requirements.

2.2 Privacy

2.2.1 The Concept of Privacy

It is not easy to articulate precisely the meaning of privacy. Privacy is contextual and may require protection of different information in different contexts. The information to be protected can be Personally Identifiable Information (PII), personal healthcare information, individual's financial information, personal location information, etc. More specifically, PII, for example, is commonly defined as, non-public personal information related to an identified person such as name, address, date of birth, contact number, email address, government identifiers (such as PAN number, PF account number, etc.), bank account number, driving license number, IP address, biometric identifier, photograph and any unique identifier related to the person. With the growth of digital services, more and more organizations are storing

more and more personal information of people, which leads to the following three concerns.

- How personal information is used by organizations or shared by them to others?
- How personal information is protected by organizations?
- Who is accountable for any breach?

Daniel [8] defines four groups of activities which can result in actions harmful to people privacy. Each of these groups can further be subdivided into subgroups of harmful activities (refer figure 2.1). These group and their subgroups are listed below.

1 Information collection. The group of activities which collect information from the subject.
   - *Surveillance.* It is watching, listening to or recording of an individual's activities.
   - *Interrogation.* It consists of various forms of questioning or probing for information

2 Information processing. The group of activities which store, process and use the collected information.
   - *Aggregation.* It involves the combination of various pieces of data about a person.
   - *Identification.* It is linking information to a particular person.
   - *Insecurity* involves a carelessness in protecting stored information from leaks and improper access.
   - *Secondary use.* It is the use of collected information for a purpose different from the use for which it is collected without the data subject's consent.
   - *Exclusion.* It concerns the failure to allow the data subject to know about the data that others have about him/her and participate in its handling and use.

3 Information dissemination. The group of activities which distribute processed information.

- *Breach of confidentiality.* It is breaking a promise to keep a person's information confidential.
- *Disclosure.* It involves the revelation of truthful information about a person that affects the way others judge her reputation
- *Exposure.* It involves revealing another's nudity, grief, or bodily functions.
- *Increased accessibility.* It is amplifying the accessibility of information.
- *Blackmail.* It is a threat to disclose personal information.
- *Appropriation.* It involves the use of the data subject's identity to serve another's aims and interests
- *Distortion.* It consists of disseminating false or misleading information about individuals.

4 Invasion. The group of activities which invade into people's affairs.

- *Intrusion.* It concerns invasive acts that disturb one's tranquility or solitude.
- *Decisional interference.* It involves incursion into the data subject's decisions regarding her private affairs.

2.2.2 Privacy regulations across world

Since privacy can tend to be too general and can encompass several things in different contexts, many guidelines and regulations are drafted by various national and international bodies. This section presents, in brief, some of the most common privacy-related regulations, standards, frameworks and best practices followed across the world. Table 2.1 presents a mapping of privacy requirements across the globe.

Asia

Asia Pacific Economic Cooperation (APEC) created a voluntary "APEC Privacy Framework" [9] in the year 2004 to promote a flexible approach to protect information privacy across APEC member economies while avoiding the creation of unnecessary barriers to information flows. APEC Privacy Framework defines the following nine information privacy principles.

- Preventing Harm: The framework should prevent the wrongful collection and

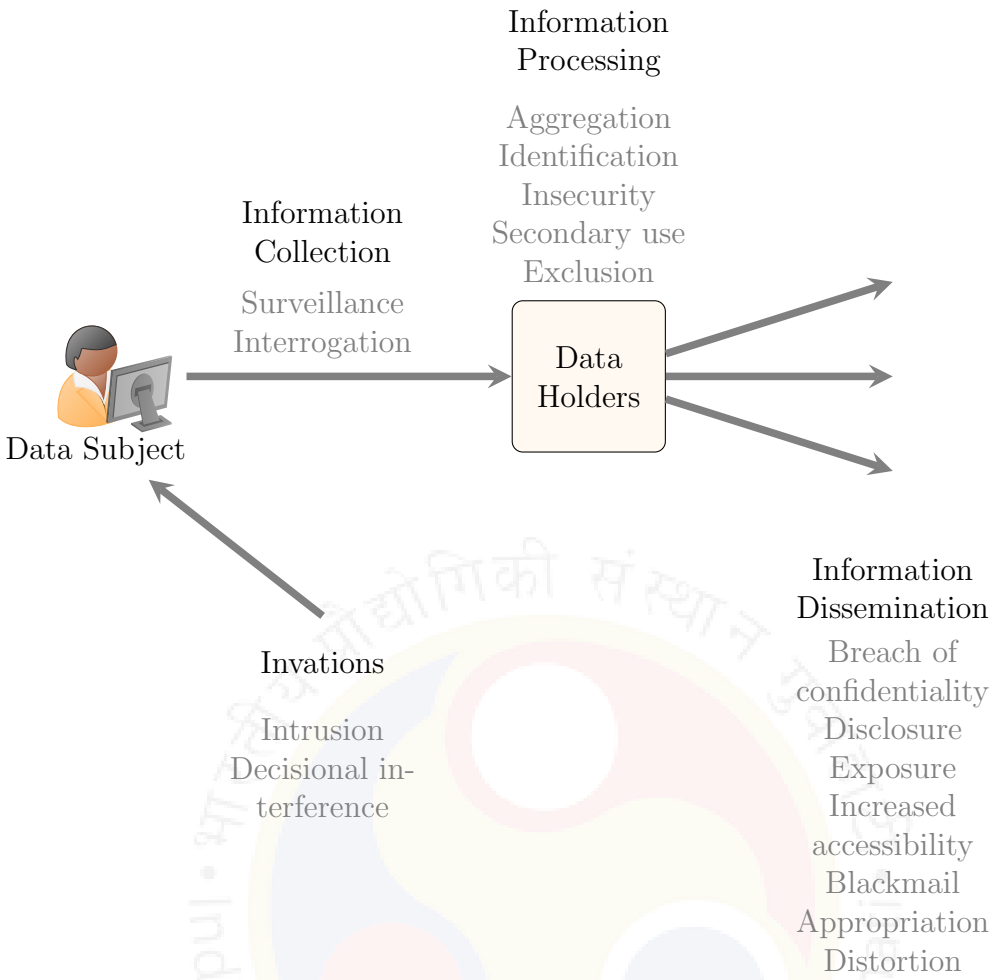


Figure 2.1: Model of taxonomy

misuse of collected information and the remedies for privacy infringements should be proportionate to the likelihood and severity of the risk of harm.

- Notice: Personal information controllers should clearly explain their practices and policies about personal information such as the purpose of collecting information, consumers of collected information, details about personal information controller, means available to subjects to limit disclosure of their personal information and how subjects can update the collected information.

- Collection limitations: Personal information should be obtained by lawful and fair means with appropriate consent and should be limited to what is relevant to the purpose of collection.

- Use of personal information: Personal information collected should be used only for the stated purposes of collection. To use the collected personal information for any other purpose, a clear and explicit consent should be taken from the subject.

- Choice: Where appropriate, subjects should be provided with clearly understandable choice in relation to the collection, use and disclosure of their personal information.

- Integrity of personal information: Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

- Security safeguards: Appropriate security safeguards should be applied to personal information which are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held.

- Access and correction: Subjects should have rights of access to their personal information, to challenge the accuracy of the information and as appropriate to request correction of such information.

- Accountability: Personal information controller is accountable for complying with measures that give effect to the principles. When transferring personal information, reasonable steps should be taken to ensure recipients protect the information in a manner consistent with these principles.

Europe

"General Data Protection Regulation (GDPR)" [10] is a regulation in European Union on data protection and privacy. It is drafted in 2018 and defines following six principles.

- Lawfulness, fairness and transparency: Personal data must be processed lawfully, fairly and transparently in relation to the data subject.

- Purpose limitation: The purpose of collecting personal data must be clearly stated, personal data must be collected for that purpose only.

- Data minimisation: Personal data collected must be minimized which is sufficient enough to serve the purpose.

- Accuracy: Every reasonable step must be taken to keep the collected personal data accurate. Data subjects have the right to request erase or rectification of their personal data which is erroneous.

- Storage limitation: Personal data collected must be deleted when it is no longer needed.

- Integrity and confidentiality: Personal data must be protected against unauthorized processing, unlawful processing, accidental loss or accidental destruction using appropriate technical and organizational measures.

United Nations

"UN Personal Data Protection and Privacy Principles" [11] is a collection of ten principles which sets out a basic framework for the processing of personal data.

- Fair and legitimate processing: Organizations should process personal data in accordance with governing instruments, consent of the data subject, the best interests of the data subject and any other related legislation.
- Purpose specification. Personal data should be processed for stated purposes only.
- Proportionality and necessity: The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.
- Retention: Personal data should only be retained for the time that is necessary for the specified purposes.
- Accuracy: Personal data should be accurate and where necessary up to date to fulfill the specified purposes.
- Confidentiality: Personal data should be processed with due regard to confidentiality.
- Security: Appropriate technical and administrative safeguards should be implemented to protect the security of personal data.
- Transparency: Processing of personal data should be carried out with transparency to the data subjects.
- Transfers: In case the organization chose to transfer personal data to a third party, it should satisfy itself that the third party provides appropriate protection to the personal data.
- Accountability: Organizations should have adequate policies and mechanisms in place to adhere to these principles.

OECD: An intergovernmental economic organisation

Organisation for Economic Co-operation and Development (OECD) [12] is an intergovernmental economic organisation with 36 member countries with an aim to foster economic progress and world trade. OECD formulated the following principles for fair information practices.

- Collection limitation: Data collection and usage for a remote service should be limited only to data that is required to offer an appropriate service.
- Data quality: Data should only be used for the relevant purposes for which it is collected.
- Purpose specification: Remote services should specify upfront how they are going to use the data and end-users should be notified in advance when a system will use it for any other purposes.
- Use limitation: Data should not be used for purposes other than those disclosed under the purpose specification principle without end-user consent.
- Security safeguards: Data should be protected with reasonable security safeguards (encryption, secure transmission channels, etc.).
- Openness: The end-user should be notified upfront when the data collection and usage practices started.
- Individual participation: End-users should have the right to insert, update, and erase data in their profiles stored on remote services.
- Accountability: Remote services are responsible for complying with the principles mentioned above.

ISO/IEC 29100

ISO/IEC 29100 [13] is an international standard which defines following privacy principles.

- Openness, transparency and notice: Data subjects must be informed about policies of the organization and organization must be transparent in its actions and inform data subjects whenever there is a change in any of the privacy-related policies.
- Consent and choice: Data subjects have to provide their consent on a knowledgeable basis such that they know the implications of granting or withholding

consent.

- Purpose legitimacy and specification: Data subjects must be informed about the purpose of data collection and use before it is used for the first time or for a new purpose.
- Collection limitation: Only the bare minimal data must be collected from the data subjects.
- Accountability: Organizations must take necessary action for any privacy breaches and must inform data subjects of the same.
- Information security: Organizations must protect the data subject's personal data and must inform data subjects about the security mechanisms used.

	APEC Frame-work	OECD Guide-lines	US Privacy Act 1974	EU Data Protec-tion	Australia ANPP	JPIPA
Accountability	✓	✓		✓		
Notice	✓	✓	✓	✓	✓	✓
Consent	✓	✓	✓	✓	✓	✓
Collection Limitation	✓	✓	✓	✓	✓	✓
Use Limitation	✓	✓	✓	✓	✓	✓
Disclosures	✓		✓		✓	✓
Access and Corrections	✓	✓	✓	✓	✓	✓
Securit / Safeguards	✓	✓	✓	✓	✓	✓
Data Quality	✓	✓	✓	✓	✓	✓
Enforcement	✓			✓		✓
Openness	✓	✓	✓	✓	✓	✓
Anonymity					✓	
Transborder Data Flow	✓	✓		✓		
Sensitivity				✓		

Table 2.1: Mapping of privacy requirements across the globe (courtesy DSCI)

Privacy by Design

Privacy by design [14] is initially developed by Ann Cavoukian and formalized in a joint report from "Information and Privacy Commissioner of Ontario (Canada)", the "Dutch Data Protection Authority" and the "Netherlands Organisation for Applied

Scientific Research" in the year 1995. Privacy by design defines the following seven privacy principles.

- Proactive not reactive; preventive not remedial: Anticipates and prevents privacy-invasive events before they happen. Privacy by design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring.

- Privacy as the default setting: If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

- Privacy embedded into the design: Privacy is not added as an additional plug-in, it is embedded into the design and architecture of IT systems as well as business practices. The result is that privacy becomes an essential component of the core functionality being delivered.

- Full functionality – positive-sum, not zero-sum: Privacy by design should demonstrate that it is possible to have both privacy and security. All objectives should be accomplished in a positive-sum "win-win" manner, not in a zero-sum manner, in which unnecessary trade-offs are made.

- End-to-end security – full lifecycle protection: Privacy by design seeks cradle-to-grave, secure end-to-end lifecycle management of information. Strong security measures are essential to privacy, from start to finish to ensure that all data are securely retained and then securely destroyed at the end of the process.

- Visibility and transparency – keep it open: Privacy by design seeks to ensure that all stated promises and objectives are open and transparent to stakeholders subject to independent verification. The motto is "trust but verify".

- Respect for user privacy – keep it user-centric: Privacy by design seeks to keep the interests of users at the top through strong privacy defaults, appropriate notices and user-friendly options. The motto is "keep it user-centric".

2.2.3 Privacy regulations in India

In India, Information Technology Act, 2000 (ITA-2000) is the primary law dealing with cybercrime and e-Governance, which had a major amendment in the year 2008. In the year 2017, the Supreme Court of India gave a landmark judgement in which it upholds the right to privacy of a person. At the end of the year 2019,

the Personal Data Protection (PDP) bill was tabled in the Indian Parliament which aims to provide a legal framework for the protection of personal data. In the year 2008, National Association of Software and Service Companies (NASSCOM) set up an independent, self-regulatory organization, named Data Security Council of India (DSCI) to promote data protection, develop security and best practices in India.

Information Technology Act (ITA), 2000

ITA-2000 provides a legal framework for e-Governance, recognizes electronic records and digital signatures, defines cybercrimes and prescribes penalties for them, directed the formation of Controller of Certifying Authority (CCA), a central national body, to regulate the issuance of digital signatures, establishes a Cyber Appellate Tribunal to resolve disputes arising from this new law and amended several sections of other Acts to make them compliant with new technologies.

Information Technology (Amendement) Act, 2008

In the year 2008, a major amendment was made in ITA, which introduced Section 66A, which penalized sending "offensive messages", Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource", Section 43A, which provides rules for the implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain, Section 72A, which provides rules for the fines imposed to the persons found involved in the wrongful loss or wrongful gain by disclosing personal information of another person while providing lawful services and provisions to address pornography, child porn and cyber terrorism.

Justice Puttaswamy vs Union of India, Supreme Court, 2017

Recently, in the year 2017, Supreme Court of India held that right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of Constitution of India [15].

Personal Data Protection (PDP) Bill, 2019

PDP, provides a legal framework for the protection of personal data and directed the formation of the Data Protection Authority of India for the same.

The bill defines personal data and a subset of it, sensitive personal data. The bill further defines different types of sensitive personal data such as genetic data,

health data, financial data and biometric data. *Personal data* is defined as any characteristic, trait, attribute, etc. of a person which can directly or indirectly identify a person. *Sensitive personal data* is defined as personal data revealing information about passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation. *Genetic data* is defined as personal data related to the inheritance or genetic characteristics of a person. *Health data* is defined as the personal data related to the physical or mental health of the person. *Financial data* is defined as the personal data used to identify a bank account, a card or payment instrument of the person, *Biometric data* is defined as personal data resulting from the physical, physiological or behavioural characteristic of a person such as facial images, fingerprints, iris scans, etc. Other than that, the bill also defines *anonymised data*, which is obtained by applying an irreversible process on personal data.

The bill defines eight obligations for protecting the personal data of a person. These obligations are similar to the principles defined by GDPR and OECD (refer section 2.2.2).

- Fair and reasonable processing: Personal data of a person should be processed in a fair and reasonable manner which respects data principal's privacy.
- Purpose limitation: Personal data should be processed only for the purposes that are clear, specific and lawful.
- Collection limitation: Collection of personal data should be limited to what is necessary for the purpose of processing.
- Lawful processing: Both personal data and sensitive personal data should be processed only on the basis of prescribed grounds of processing.
- Notice: Data fiduciary shall provide necessary relevant notices to data principals as soon as possible.
- Data quality: Data fiduciary shall ensure that personal data is complete, accurate, clear and up-to-date.
- Data storage limitation: Data fiduciary shall retain personal data as long as may be reasonably necessary to satisfy the purpose for which it is processed.
- Accountability: The data fiduciary is accountable with obligations specified in the bill.

The bill also defines the grounds on which personal data and sensitive personal data can be processed. Some of the grounds mentioned in the bill are listed below.

- On the basis of the consent of the data principal. The consent must be free, informed, specific, clear and capable of being withdrawn.
- For functions of the State such as Parliament or any State Legislature.
- In compliance with law or any order of any court or tribunal.
- Necessary for prompt action such as in case of a medical emergency, to ensure safety during any disaster or breakdown.
- Necessary for purposes related to employment such as recruitment, termination, provision of any benefit to the employee, verifying the attendance of the employee or the assessment of the performance of an employee.

Other than that, the bill also defines the following rights of the data principal.

- Right to confirmation and access: Data principal can obtain confirmation on whether his/her personal data is processed or is being processed, a brief summary of his/her personal data which is either processed or being processed, a brief summary of processing activities.
- Right to correction: Data principal can ask for correction, completion and updating of his/her personal data.
- Right to data portability: Data principal can receive his/her personal data from one data fiduciary and transfer the same to other data fiduciary.
- Right to be forgotten: Data principal has the right to restrict or prevent continuing disclosure of his/her personal data by data fiduciary.

2.3 Privacy Practices in e-Governance across World

This section presents e-Governance practices in three countries, namely, Estonia, Austria and India.

2.3.1 Estonia

Estonia has one of the most digitally advanced e-Governance systems in place. Almost all public services are available online including the election vote service. This is made possible by the strong legal and regulatory framework which is supported by robust technology. With such wide adoption of digital services, Estonian citizens are relatively digitally more literate compared to other parts of the world and also have a high level of confidence in the country's e-Governance system.

Legal and Institutional

The constitution of Estonia recognizes privacy of its citizens by specifying three artefacts, first, the right to privacy, second, the right to free self-realization, and third, the right of data subjects to request information about him/her. The Public Information Act is drafted to implement the same by specifying four details, first, the conditions for accessing and refusing to grant access to public information, second, the public information for which access is restricted, third, the conditions for establishing and administering databases, and fourth, the mechanism for state and administrative supervision of organization access to public information.

The Estonian Data Protection Inspectorate is the regulatory body governed by Data Protection Act, Public Information Act and Electronic Communication Act, which aims to protect three rights of citizens, first, the right to obtain information about the activities of public authorities, second, the right to have private and family life in the use of personal data and third, the right to access data gathered in regard to the data subject.

ICT Systems

The e-Governance in Estonia depends on following three fundamental building blocks.

Estonia Digital ID: Almost all public and private services can be accessed through the digital ID of the resident. Every resident of Estonian above the age of 15 is mandatorily required to have the Estonian Digital Identifier, which is available in three form factors, namely, physical ID card, mobile ID (special mobile SIM with digital certificates) and smart-ID7 which can be accessed through Android and iOS smartphones. The ID has two digital certificates, first for authentication of the user and second for digitally signing the document. Access to these certificates is protected by a Personal Identification Number (PIN). Hence, even if the card or the SIM is lost, the same cannot be used by other users without having the PIN.

X-Road: The "X-Road" is a data exchange platform that allows various

databases in the public and private sector to securely exchange data. The data across these databases are linked by the unique identification number called Personal Identification code (PIC) in Estonia.

RIHA is *Administration system for State Information System* which serves as a catalogue for the state's information system and provides the following information.

- The information systems and databases that make up the state's information system;
- Data collected and processed by these information systems;
- Services, including X-Road services, provided by these information systems and the list of users (organizations) of these services;
- Responsible and authorized processors of the information systems and databases and services and contact details of these individuals;
- Legal basis for the database operations and processing; and
- The reusable components that ensure the interoperability of information systems (XML assets, classifications, dictionaries).

Estonian e-governance Systems Architecture

- A user wanting to use an online service "XYZ" of Department "ABC" authenticates their identity by using the citizen portal using their digital ID (smart card or mobile ID). (Single sign-on solution enables the user to request service from any department seamlessly.)
- Using X-Road, the service being accessed itself obtains the data needed to process the service request from other databases.
- The Security Server component of the requesting system encrypts the data and sends it to the system (database) from which data are desired over the Internet.
- The security server at the data provider system end authenticates the requesting system, and if the authorization check succeeds, forwards the request to the system.
- The security server time stamps, digitally signs, and logs the transaction and

sends an encrypted response, provided by, the data provider system to the requestor system.

- The security server decrypts the response, and then the service processes the request based on data fetched in realtime and returns the response to the user.

2.3.2 Austria

With a population of 8.7 million, Austria was one of the first countries to implement a national ID system that enables residents to access public services online using an electronic ID card. Tokenization is the focus of study in the country case study of Austria and hence a detailed assessment is not presented with reference to the Ann Cavoukian's Fair information practices. Austria's tokenization - privacy by design features is analogous to the Indian one which uses virtual IDs and tokenization. However, unlike India's centralized ID authentication system, Austria's system is decentralized.

Legal and Institutional

Legal: Being an EU member, Austria is bound by GDPR which is locally implemented through the Austrian Data Protection Act. The SourcePIN Register Regulation specifies the tasks of the SourcePIN Register Authority which are necessary for the implementation of the citizen card concept and the cooperation with its service providers.

Institutional: The functions of SourcePIN Register Authority sets out in SourcePIN Register Regulation are carried out by the Austrian Data Protection Authority (DPA), which is an independent authority entrusted with protecting individual rights and interests in the privacy of personal data.

ICT Systems

sPIN and *ssPIN*: Austria maintains "Central Register of Residents" (CRR), which is a national information system that contains data about every resident of Austria. Austria mandates that all residents register their presence in the country. The data in this register include details such as full name, sex, date of birth, citizenship, full address and a unique 12 digit identifier, named, CRR number. The CRR in this register is available to the public. A source PIN (sPIN) is generated from CRR number and is kept secret by the resident. Further to this, a sector-specific PIN (ssPIN) is also generated from sPIN to keep privacy across sectors.

Citizen Card: Austria uses a Citizen Card (CC) which, unlike a physical ID

card, is a model that provides a series of functions for carrying out e-Government and e-Commerce transactions securely. The data contained on a CC is called Identity Link and consists of full name, date of birth, the sPIN and the cryptographic keys required for digital signature and encryption. To ensure integrity and authenticity, the Identity Link object is digitally signed by the SourcePIN Register Authority. Access to sPIN and cryptographic keys on CC is protected by a PIN. The Citizen Card can, in particular, be used to create and verify electronic signatures for electronic documents, to encrypt and decrypt electronic documents, to calculate and check hash values for electronic documents, and to record data in a data storage area and retrieve it from there.

MOA-ID and *CCE*: For secure communication, both service providers and residents use specific software at their end. Service providers use a trusted software named MOA-ID which manages identification and authentication based on CC and residents use a trusted software named Citizen Card Environment (CCE) that provides the CC functions.

Data Sharing within the sector: Unlike sPIN, ssPIN can be stored in administrative procedures. Public authorities can use the same ssPIN to retrieve a citizen's data stored within the same procedural sector, for example, if they need to view the citizen's records or use it to pre-fill forms. However, authorities do not have access to ssPINs from other sectors.

Data Sharing across sectors: Administrative procedures often require authorities from different sectors to work together. For example. If an authority requires a sector-specific person identifier from another procedural sector in order to identify a natural person, they can request it from the SourcePIN Register Authority by providing the ssPIN from their own procedural sector, the person's first and last name, and their date of birth. The SourcePIN Register Authority sends the desired ssPIN to the authority that requested it in encrypted form, and the ssPIN can only be decrypted by the public authority that is responsible for the other procedural sector.

2.3.3 India

In the year 2009, UIDAI was established with a mission to assign a unique identification number assigned to each resident of India. To enrol himself/herself, a resident needs to provide his/her personal and demographic data such as full name, address, mobile number and 12 biometric (10 fingerprints, 2 iris-scans and one facial image) to UIDAI which are registered securely in a central repository. Once registered,

each resident is assigned a unique 12 digit identity number called Aadhaar. Unlike other systems, like Estonia, no physical card or credential is provided to the resident. Instead, all authentication is done using biometrics. Since the establishment of Aadhaar, the Government has built various online digital services such as eSign, DigiLocker, etc. using application programming interfaces (APIs) known as India Stack, which is spearheaded by private think tank iSPIRT. iSPIRT describes India Stack as a set of APIs that allows governments, businesses, startups and developers to utilise a unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery. At the end of the year 2019, the Personal Data Protection (PDP) bill was tabled in the Indian Parliament which aims to provide a legal framework for the protection of personal data.

Legal and Institutional

Legal: The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act is drafted in the year 2016 with the aim to provide a legal support to Aadhaar and the unique identification number project which was launched in 2009.

Institutional: In the year 2009, UIDAI was established with a mission to assign a unique identification number, called Aadhaar, to each resident of India so that duplicate and fake identities can be removed and identity verification can be done in a more cost-effective way. The Aadhaar ecosystem includes Authentication Service Agencies (ASAs) and Authentication User Agencies (AUAs). ASAs provide UIDAI compliant network connectivity to requesting agencies. AUAs are empanelled agencies which provide Aadhaar Enabled Services to end-users which are Aadhaar holders.

ICT Systems

The key components of the Aadhaar system include the following:

Enrolments Software: The enrolment software, owned by UIDAI, captures demographic information and biometric data with the consent of the user obtained at registration. The software then securely transmits that information to the Aadhaar system.

CIDR: The Central Identity Repository system stores the demographic and biometric data after issuance of the Unique ID number (Aadhaar number).

Aadhaar services/APIs: UIDAI has open APIs to allow service providers in the public and private sector to authenticate users based on one or more of the

following: biometrics, demographics, and One Time Password (OTP) on registered mobile phones. The service providers must register as AUA/sub AUA with UIDAI and access the APIs via the ASA.

eKYC service shares the demographic data and the photograph of the user with the service provider when the user provides consent. This enables the onboarding of users for services such as opening bank accounts, getting up a SIM card, etc. Recently, UIDAI has announced that a limited eKYC API would also be made available for a category of service providers with limited KYC data.

Aadhaar authentication system: The workflow of Aadhaar authentication system is briefly summarized below.

- The user with an Aadhaar number presents the Aadhaar number or Virtual ID number and a biometric or OTP to the service provider (AUA).
- The encrypted biometric from the UIDAI certified biometric device is packaged by the AUA as per the API specification and sent to ASA.
- ASA transmits this packet over a leased line and invokes the authentication API of the Aadhaar system.
- The API checks the incoming data against the CIDR and returns a YES/NO response based on the result of the match.
- This response is conveyed by ASA to AUA and onwards to the user. AUA provides the service when the response is YES.

Virtual ID: A 16-digit random number is mapped to an Aadhaar number. Once you have generated a Virtual ID, you can provide that 16-digit number, instead of your Aadhaar number, to any agency seeking to use your Aadhaar number for authentication. A key privacy-enhancing aspect is that the Virtual ID is temporary and revocable. This means that service providers cannot rely on it or use it for correlation across databases. The users can change their Virtual ID whenever they wish just as one would reset their computer password/PIN.

Tokenization: When a user gives Aadhaar/Virtual ID for authentication, the ID system generates a unique token (72 char alphanumeric code) which is specific to that agency and Aadhaar number. Different agencies are given different tokens to identify the same person in their system, thereby eliminating the linkability of information in the databases based on an Aadhaar number. Only the Aadhaar system knows the mapping between the Aadhaar number and the tokens provided

to the service providers.

Service providers or AUA's are categorized as global AUA or local AUA. Global AUAs are allowed to store and use Aadhaar numbers and use full eKYC API which returns an Aadhaar number along with the token. On the other hand, local AUAs are only allowed to use limited eKYC API and use the token to identify the user instead.

2.4 Mechanisms to improve Privacy

In the recent past, several new mechanisms have been developed in computer science and mathematics which can help improve privacy in systems. This section presents some of these mechanisms in brief. It should be noted that although the focus of this section is on cryptographic mechanisms, other practices should also be followed diligently such as "Distributed key management", "Necessary audit", "Tamper-proof code", "Tamper-proof hardware", etc.

2.4.1 Fine Grained Access Control

One scheme to improve the privacy of the data is to restrict access to the object through privacy policy rules and grant access to only those requests which satisfies the access policy rules. The access policy rules can encode in it the expected attributes of the requester, the purpose of accessing the object, the duration for which the data is supposed to be used, the number of times the data is supposed to be used, etc. Fine-Grained Access Control sometimes is also referred to as Attribute-based Access Control (ABAC).

[16], [17], [18] propose extensions to RBAC. In P-RBAC [16] the privacy policies are incorporated to protect access to private and sensitive data. [17] Proposes to add a purpose component and a new language dedicated to the conditions. The privacy policy is enforced by permission assignments. [18] discusses the definition of invariance. It focuses on the proof of the consistency between the practices of data collection and privacy policy.

2.4.2 Secret Sharing

Secret sharing scheme was introduced by Shamir [19] in which a secret is shared among a group of participating entities in such a way that the secret can only be reconstructed when sufficient number shares are applied together. A $\langle \mathrm{t}, \mathrm{n} \rangle$-threshold scheme is a type of secret sharing scheme in which the secret is shared among n

participants and at least t participants are required to reconstruct the secret. Secret sharing scheme is a foundation of some other schemes such as secure multi party computation. One limitation of this scheme is an increased overhead of sharing the secret shares among participating entities. [20] provides an approach to conduct privacy preserving decision tree classification based on the Shamir's secret sharing technique. [21] used secret sharing scheme to split the Electronic Health Record (EHDR) into shares that are stored with different people.

2.4.3 Attribute based Authentication/Encryption/Signature

Attribute-based authentication (ABA) is an authentication scheme in which users are authenticated based on user's attributes rather than the user's identity. This authentication scheme makes the user anonymous within the group of users having the same set of attributes. Attribute-based encryption (ABE) is an encryption scheme in which the encrypted data can be decrypted by only those users who possess the specified set of attributes. This encryption scheme limits access to user's data even if data is hosted by untrusted servers. ABE can be of two types, namely, key-policy attribute based encryption (KP-ABE) and ciphertext-policy attribute based encryption (CP-ABE). In KP-ABE, user's secret keys are generated based on an access tree which depicts the privilege of the user and data is encrypted over a set of attributes. In CP-ABE, a user's set of attributes are generated based over a set of attributes and the data is encrypted using the access tree. Although quite promising, ABE also has its limitations such as lack of attribute revocation mechanism and challenges such as key coordination, key escrow and key revocation. Attribute based Signature (ABS) is a digital signature scheme in which the signer digitally signs a document using his attributes rather than his identity.

Li et al. [22] presented a flexible and fine-grained CP-ABE scheme, which was applied in cloud storage. Goyal et al. [23] first introduced KP-ABE scheme that supports any monotone access policy. Bethencourt et al. [24] first provided a CP-ABE scheme, which was proven secure in the generic group model. In order to resist collusion attack, Li et al. [25] presented a user collusion resistant CP-ABE scheme, which supports efficient attribute revocation. Recently, some outsourced ABE schemes [26] - [27] were proposed, which improves computation efficiency. In addition, ABE schemes [28] and [29] with constant ciphertext length were proposed, which improves communication cost.

2.4.4 Other Mechanisms

Homomorphic Encryption

Homomorphic encryption (HE) allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of operations as they had been performed on the plaintext. This scheme allows untrusted parties to do computation on encrypted data while still ensuring the privacy of data. Although homomorphic encryption can be very useful in improving data privacy, the latency of its operations is still low, limiting its practical useability.

Since the seminal work of Gentry [30], introducing the first Homomorphic Encryption, many other simpler and more efficient schemes have been proposed [31, 32, 33]. The spectrum of applications of homomorphic encryption is rather large, in particular in the domain of cloud-based applications [34, 35, 36].

Functional Encryption

Functional encryption (FE) is a public-key encryption scheme in which possession of a decryption key allows a function (corresponding to that decryption key) to be evaluated on encrypted data. This is different from homomorphic encryption, in which result of function evaluation is an encrypted data while in functional encryption, the result of function evaluation is in plaintext. Similar to homomorphic encryption, although functional encryption can be very useful in improving data privacy, the latency of its operations is still low, limiting its practical useability.

Many recent papers [37, 38, 39, 40, 41] developed various FE encryption schemes with an aim to make such schemes practical. Nevertheless, most of them remain theoretical, since they do not provide implementation or practical evaluation of the schemes.

Searchable Encryption

Searchable encryption is an encryption scheme which enables search on encrypted data. Unlike homomorphic encryption and functional encryption, searchable encryption schemes are relatively efficient and practical. Searchable encryption can be useful in investigative and surveillance kind of applications.

Searchable encryption cannot only perform the search on ciphertexts but also protect the security and privacy of data in a semihonest cloud model. Golle et al. [42], the first proposer of symmetric searchable encryption, indicated to bind the files to their corresponding keywords, and find the corresponding ciphertext files

through the search of the keywords to realize the ciphertext search. After that, many symmetric-based searchable encryption schemes [43], [44] have been proposed. The authors in [45] and [46] put forward a keyword ranking search scheme, which mainly achieves the accurate ranking of search results by encrypting the correlation score. For achieving a higher security, some schemes [47, 48, 49] were proposed to build searchable encryptions by using the public-key cryptography technique.

Oblivious Transfer

Oblivious transfer (OT) is a scheme to transfer one out of many pieces of information in which the sender remains oblivious as to what piece has been transferred and the receiver remains oblivious to other (than what he wants) pieces of information available with the sender. This scheme improves the privacy of the receiver by not letting the sender know which piece of information has actually been transferred to receiver.

Oblivious transfer is introduced by [50] to protect users' privacy in electronic commerce and it is a basic cryptographic method in various privacy-preserving technologies [51], [52]. To solve the privacy in data utilization and computing in cloud environment, Li et al. presented a new approach with oblivious storage and computation, which is a common solution for such a problem [53].

Private Information Retrieval

Private Information Retrieval (PIR) is a scheme to transfer one out of many pieces of information in which the sender remains oblivious as to what piece has been transferred. It is a weaker form of Oblivious Transfer, which also requires that the receiver remains oblivious to other (than what he wants) pieces of information available with the sender. This scheme improves the privacy of the receiver by not letting the sender know which piece of information has actually been transferred to the receiver.

Chor et al. [54] introduced the notion of PIR and pro- posed the first construction using several separate databases which are not allowed to communicate with each other. Kushilevitz and Ostrovsky [55] presented a technique to construct a single database PIR. Subsequently, a number of papers [56, 57, 58] have continued this line of research to reduce the communication complexity. The most famous implementation of PIR is the oblivious transfer (OT) introduced by Rabin [59].

Secure Multi-Party Computation

Secure multi-party computation (MPC) is a set of schemes in which multiple participating parties jointly compute a function over the set of their respective inputs while keeping their inputs hidden from other parties. This model assures the privacy of participating entities from each other.

The theoretical and algorithmic foundations for SMC are well-researched and it has been shown that SMC has the potential to solve hard problems in application areas that require strong privacy. Various approaches based on compilers and domain-specific languages exist: The Fairplay system [60] implements two-party SMC, and the FairplayMP extension [61] implements multiparty SMC. SMCL [62] is a domain-specific language for SMC. One large scale real-world application of SMC was a sugar beet auction system in Denmark [63]. However, to the best of our knowledge, SMC for control or management of infrastructure has not been investigated. From its definition SMC framework can not only protects multiple users' privacy, but also enable complicated arithmetic and logic operations, therefore SMC shows great potential in building privacy preserving smart meter systems.

Zero-Knowledge Proof

Zero-knowledge proof (ZKP) is a method to prove ownership of certain knowledge without actually revealing the content of that knowledge. Using ZKP, one party can share certain fact without revealing that fact thereby creating the required trust to perform a secure communication. Although ZKP seems very powerful in improving privacy, designs of general-purpose ZKPs do not exit. Different solutions have to be designed for different scenarios and use cases. ZKP can be an interactive ZKP or non-interactive ZKP. In interactive ZKP, participating entities interact with each other while in non-interactive ZKP, they do not.

In 1985, Goldwasser et al. [64] first put forward the concept of interactive proof system and analysed the interactive proof system whose knowledge complexity is zero. Blum et al. [65, 66] first study the noninteractive zero knowledge (hereinafter referred to as NIZK) proof system and present the common reference string model that is generally applied at present. Noninteractive zero knowledge proof system contains only a message sent by a prover to verifier, which can be better used in the construction of cryptographic protocols. In recent years, Groth et al. suggest to turn the research of NIZK to specific problems [67, 68, 69] and construct NIZK proof systems based on different application scenarios. This idea greatly improves the efficiency and practicability of NIZK and created a new line of research on the applications of NIZK.

Quantum Cryptography

Many of the existing privacy enhancing technologies are based on traditional cryptographic primitives such as Public-Key Cryptography (PKC) algorithms which are vulnerable to possible attacks run by quantum computers. Post-Quantum Cryptography (PQC) offers solutions against such attacks. Hence, privacy enhancing technologies based on post-quantum cryptographic primitives are the natural evolution of privacy enhancing technologies in the future. The downside is that post-quantum technologies may introduce computational and memory constraints on host devices similar to what traditional PKC schemes have done earlier.

In recent past, researchers have proposed and developed many useful applications based on quantum cryptography. [70] proposed a quantum key distribution using EPON optical network. [71] proposed a privacy enhancing scheme for cloud computing using quantum cryptography. [72] proposed a scheme to encrypt data using quantum cryptography for big-data applications. [73] demonstrated encryption of Ethernet data using quantum keys and proposed that the quantum keys should be stored in smart card so that mobile phone users can communicate using quantum cryptography. Some of the challenges in this area are how to upgrade the existing environment to new environment and how to securely distribute the quantum keys to individual users. Even amidst the promising advantages of quantum cryptography over traditional cryptography, it may take some time for a developing country like India to migrate the existing PKI infrastructure to quantum-based infrastructure.

Though, quantum-based cryptography is an emerging technology and has a lot of potential, the scope of the thesis is kept within the present state of Aadhaar-based services such as eSign, DigiLocker, Registered Devices and toll payment which is still based on public key cryptography and is yet to be strengthened using quantum-based cryptography.

2.5 Access Control Models and Cryptographic Schemes

Access control refers to the methods to restrict, reject or accept access requests of subjects to an object. *Subject* may refer to any entity which seeks access to a protected resource such as a user, process, etc. *Object* may refer to any resource for which access needs to be controlled. Access control policies govern the rules of access control and are enforced by *reference monitor* which are assumed to have the

following properties.

- Unpassability. All access control requests pass through reference monitor and it is not possible to gain access to objects without passing through it.
- Tamperproofness. Reference monitor cannot be tampered without either raising alerts or shutting down the reference monitor.
- Verifiability. Reference monitor implementation can be verified to implement the desired functionality within a reasonable timeframe.

Reference monitor is implemented by a *security kernel*, which consists of both hardware and software. Reference monitor either grants or denies the access request and also provide necessary audit information. Some of the most commonly used access control models are Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

2.5.1 Mandatory Access Control

Mandatory Access Control (MAC) provides selective access control to subjects to perform a certain operation on an object. The access control policies are defined by a designated entity and users are not allowed to modify the policy. MAC is generally used in military or army systems.

2.5.2 Discretionary Access Control

Trusted Computer System Evaluation Criteria (TCSEC) defines Discretionary Access Control (DAC) as "*a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).*"

2.5.3 Role-based Access Control

Role-based Access Control (RBAC) was initially presented by Sandhu et al. in 2000 and standardized by NIST/ANSI later. In RBAC, each user is assumed to have roles and permissions are assigned to roles. A user, in turn, inherit all permissions assigned to roles to which it is associated. NIST/ANSI defines three levels of RBAC, namely, *core RBAC*, *hierarchical RBAC* which includes inheritance between roles and *constrained RBAC* which includes separation of duties.

2.5.4 Attribute-Based Access Control

NIST defines Attribute-Based Access Control (ABAC) [74] as "*an access control method, where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.*" The recommended architecture of ABAC consists of the following three entities.

- Policy Enforcement Point (PEP). An entity which intercepts user's access request takes access decision from PDP and either accepts or rejects access request based on the received decision.
- Policy Decision Point (PDP). An entity which evaluates access requests against access control policies and takes a decision to either accept or rejects the access request.
- Policy Information Point (PIP). An entity which provides values of attributes of subjects, objects and environment.
- Policy Administration Point (PAP). An entity which manages access authorization policies.

An attribute can be any system-wide agreed-upon characteristic of a subject, object, action or environment.

Conventional access models, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role Based Access Control(RBAC) [75, 76], are not designed to enforce privacy policies and barely meet privacy protection requirements [77], particularly, purpose binding (i.e. data collected for one purpose should not used for another purpose without user consent), conditions and obligations. Although [16, 78] introduced privacy aware access control frameworks in the context of traditional data management systems, privacy issues are somewhat more difficult to be addressed in within other contexts such as big data and e-governance systems.

2.5.5 Cryptographic Schemes

Attribute-based encryption (ABE) [79] is one of the cryptographic schemes which can be used to partially realize access control models. In this scheme, attributes of an entity are mapped to elements in the algebraic group used in the scheme. Although ABE schemes can realize most of the features of access control models, it

has difficulties realizing some features such as separation of duties, role hierarchies, obtaining environment attributes, etc [80].

ABE schemes are categorized into two types, Key-Policy ABE (KP-ABE) schemes [79] and Ciphertext-Policy ABE (CP-ABE) schemes [81]. In KP-ABE schemes, attributes are embedded in ciphertext, while access policies are associated with a secret key. In CP-ABE schemes, access policies are embedded in ciphertext, while attributes are associated with a secret key. Attribute-based signature (ABS) [82] facilitates a user to sign a message using his/her attributes rather than an identity. Hence, in ABS, a signature is an attestation by a set of attributes rather than by identity. Attribute-based Messaging (ABM) [83] facilitates messages to be encrypted using the recipient's attributes rather than a list of recipients.

2.6 Summary

This chapter presented the concept of privacy, privacy-related regulations across the world and in India. The chapter also presented the privacy-related practices used in three countries, Estonia, Austria and India. The chapter concludes with some of the cryptography mechanisms which can be useful in improving privacy such as fine-grained access control, secret sharing, attribute based authentication, attribute based encryption, attribute based signature, homomorphic encryption, functional encryption, searchable encryption, oblivious transfer, private information retrieval, secure multi-party computation and zero-knowledge proof.

This page intentionally left blank.

Chapter 3

Privacy Enhanced eSign Scheme 1

3.1 Introduction

eSign is an online electronic signature service in India which is being promoted by Government of India as part of its Digital India Initiative. As opposed to traditional dongle-based electronic signature, eSign provides benefits such as less cost, no manual authentication, no requirement of special hardware device and no requirement for the end-user to keep any key secret. With the passage of *Information Technology Act* (ITA-2000), an electronically signed digital document is considered equivalent to a handwritten signed paper document. In India, eSign is being regulated by *Controller of Certifying Authority* (CCA) and is being operated by certain designated empanelled agencies known as *eSign Service Providers* (ESP). ESP provides its services to application-specific agencies known as *Application Service Providers* (ASP). ASP provides eSign service to the end-users. eSign is governed by *Public Key Infrastructure* (PKI) which is further governed in legal matters by the national legislature of the country.

To avail eSign service, a resident needs to enrol with *Unique Identification Authority of India* (UIDAI) and receive a 12-digit identity number called *Aadhaar* [84] [85]. As part of the enrolment process, resident needs to provide information about his/her identity and address to UIDAI such as Name, Date of Birth, Address, Phone number, Email-id, Biometric (fingerprint-scan, iris-scan) etc. The process of obtaining this information from the end-user is known as *Know Your Customer* (KYC) and is initially introduced by *Reserve Bank of India* (RBI) for financial banks

[86]. Traditionally, this process involves the submission of a self-attested physical form along with necessary physical documents, followed by verification and approval by receiving organization. eKYC is an online service which facilitates completion of the KYC process electronically. eKYC has some significant benefits over traditional KYC, eKYC eliminates submission of physical documents by customer, is faster and is less error-prone. UIDAI's eKYC service facilitates a third entity to retrieve the resident's identity, address and other details after taking explicit consent and authorization from the resident.

With the increased adoption of Aadhaar based identification, many online services are now using Aadhaar based services and with its such wide adoption, the privacy of user data has become even more important. Although Aadhaar based eKYC service provides access to eKYC data only after taking an explicit consent from the resident, this way of taking consent from the resident has two shortcomings. First is that the consent is taken by a non-UIDAI entity and does not encode in itself a proof from the resident that the consent is indeed given by the resident. Second is that providing a boolean consent is too broad, either an unconditional access is given to the whole eKYC information or no access is given at all. A resident may wish to have a better privacy enhancing fine-grained access control to his/her eKYC data. The resident may wish to define a privacy and access control policy dictating the *scope* of information which can be provided, the *purpose* for which the information can be provided and *recipients* to whom the information can be provided. For example, a resident may wish to disclose only his/her name and address, only for the electronic signature purpose and only to a specific eSign Service Provider.

Some of the limitations and challenges of the present model of eSign are listed below.

- The first limitation is that the eKYC data access reflects a restrictive *self-only*, *full-resource* and *unlimited* access control. However, a resident may wish to have a better access control mechanism which allows third entities to access part of a resource which is to be used for a specific purpose and for a limited time period.

- The second limitation is that for each eSign request, the resident has to authenticate itself each time and to include the authentication proof in each such request. Moreover, if a resident needs to eSign multiple times, time taken by the initial authentication phase can be a major bottleneck.

- Performance of eSign should also be kept within acceptable limits if it is to be used at nationwide level. The amortized performance of eSign can be improved

using *digital access token* which encodes in itself the authentication proof and other information such as how many eSign requests can be made using this token and the expiry time of the token.

- Some other concerns are how and where the privacy policies of the participating entities should be encoded? What will be the overall scheme? Will it be secure enough to meet necessary security requirements?

In this chapter, a method to implement privacy aware eSign is introduced using *Privacy Enhancing and Fine-Grained Access Control* (PEaFGA) statements. A digital token is constructed to encode policy rules and to improve performance. A resident can encode PEaFGA statements in the digital access token for better access to his/her eKYC data. This token can be provided to third entities so that they can present this token for claiming protected resource from UIDAI. This chapter also presents a security analysis of the proposed scheme using *Burrows-Abadi-Needham (BAN)* logic. The analysis shows that in the proposed scheme, even if the network is unreliable, the exchanged information is reliable and is secured against eavesdropping.

The remainder of this chapter is organized as follows. Section 3.2 presents related work. Notations used in the chapter are listed in table 3.1. Section 3.3 presents Aadhaar based eKYC service. Section 3.4 presents eSign version 2.0 model. Section 3.5 introduces digital token to improve amortized performance of eSign. Section 3.6 presents proposed Privacy Aware eSign model using privacy enhancing and fine-grained access controlled eKYC. Section 3.6.4 presents formal security analysis of the proposed model using BAN logic and finally section 3.7 concludes the chapter.

3.2 Related Work

Digital tokens are increasingly being used in many cryptography related applications to achieve varied objectives.

U-Prove [87] is an identity management solution based on blind signatures [88] which uses digital tokens to achieve objectives of privacy and anonymity. U-Prove consists of two protocols, viz., issuance protocol and presentation protocol. In issuance protocol, identity provider issues a digital token to the subscriber which (s)he can later present to the verifier in presentation protocol so that the service provider can grant resource access to the subscriber. A U-Prove token consists of a unique token identifier, a public key of the token which aggregates information in the token, a token information field which encodes token specific information, a prover

information field which is opaque to the issuer, issuer signature on all the other token contents and a boolean value which indicates whether the token is protected by a device. U-Prove uses digital tokens effectively by encoding necessary information in it in a cryptographically secure way to achieve objectives such as privacy and anonymity.

OAuth2 [89] is an authorization framework which allows delegation of access to protected resources to a third party by using digital tokens referred to as access tokens. Access tokens are issued to Clients by *Authorization Server* after taking permission from *Resource Owner*. An access token can be of two types, viz., a bearer token and a MAC token. A bearer token is an opaque string which can be used to claim access to a resource by any entity who presents the token. A MAC token is essentially a shared symmetric key which is used to sign a challenge by the client to prove its possession of the token to authorization server. OAuth2 uses digital tokens effectively for access delegation and is used by many organizations for data sharing.

Bitcoin [90] is a decentralized digital currency which can be transacted over the peer-to-peer bitcoin network. A bitcoin network is composed of cryptographically secure linear chains of blocks with each block containing a header and a collection of transactions. A transaction is essentially a digital token that changes ownership of bitcoins from one entity to another. Each transaction in the bitcoin network is broadly composed of three parts, viz., input, output and amount. Input refers to the previous owner of the bitcoins, output refers to the new owner of the bitcoins and amount refers to the amount of bitcoin that is transacted. Bitcoins use cryptographically secure digital information containers (similar to digital tokens) effectively for the realization of digital currency.

Although Attribute Based Encryption (ABE) is also evolved to protect the privacy of user data, it is based on Identity Based Encryption (IBE). An agency may not shift from PKI to IBE framework for a number of reasons.

3.3 Aadhaar based e-KYC service

Aadhaar based eKYC service is available to general citizens only through certain empanelled agencies such as *eSign Service Provider* (ESP) and the infrastructure network is secured by certain designated agencies known as *Authentication Service Agency (ASA)* and *KYC User Agency* (KUA). eKYC service is hosted as a stateless REST-based web service over HTTPS and the details are sent as input data encoded in XML. Figure 3.1 depicts Aadhaar's eKYC webservice as specified in eKYC v2.1

Notation	Description
$\{X\}_Y$	X is signed by key of entity Y
SK_Y	Symmetric key of entity Y
SK_{Y_Z}	Symmetric key shared by entities Y and Z.
PR_Y	Private asymetric key of entity Y
PB_Y	Public asymetric key of entity Y
R_i	Resident
ASP_i	Application Service Provider
ESP_i	eSign Service Provider
UIDAI	Unique Identification Authority of India
ID_{R_i}, ID_{ASP_i}, ID_{ESP_i}	Identities of R_i, ASP_i and ESP_i
TID_{ESP_i}, TID_{ASP_i}	Unique transaction identifiers generated by ESP_i and ASP_i
PW_{R_i}	Password of R_i for login to ASP_i portal
$AadhaarNo_{R_i}$	Aadhaar No of R_i
C_{R_i}	Cookie associated with R_i's logged-in session, assigned by ASP
PR_{B_i}, PR_{ASP_i} PR_{ESP_i}, PR_{UIDAI}	Private keys of R_i browser, ASP_i, ESP_i and UIDAI
PB_{B_i}, PB_{ASP_i} PB_{ESP_i}, PB_{UIDAI}	Public keys of R_i browser, ASP_i, ESP_i and UIDAI
$n*_!$	nonces such as $n1_{ASP_i}$, where $*$ is any integer and ! can be R_i, ASP_i, ESP_i or UIDAI
$DataR_i(DataA_i,$ $DataE_i, DataU_i)$	Intermediate data in plaintext to be send by R_i (ASP_i, ESP_i, UIDAI)
$SignR_i(SignA_i,$ $SignE_i, SignU_i)$	$\{H(DataR_i)\}_{PR_{Ri}}$
$consent_{use\_ekyc}$	Consent from resident whether his/her eKYC can be used
$consent_{genuse\_at}$	Consent from resident whether a digital access token can be generated for later use
$License_{ASP_i}$ $License_{ESP_i}$	License for ASP_i (ESP_i) to use services from ESP (UIDAI)
M_i	Message (in plaintext) to be eSign
DSC_{Ri_Mi}	Digital Signature Certificate generated for message M_i for resident R_i
$\{M\}_{eSign\_R_i\_ESP_i}$	eSigned message (by R_i) through ESP_i
H()	One way cryptographically secure hash fn
$\|$	Concatenation operator
$\oplus$	XOR operator

Table 3.1: Notations used in this chapter

specification [91]. The specification provides following information about element *rc* which represents the resident consent.

"rc – (mandatory) Represents resident's explicit consent for accessing the res-

```
URL:
  https://<host>/kyc/<ver>/<ac>/<uid[0]>/<uid[1]>
         /<asalk>

Input Data:
  <Kyc ver="" ra="" rc="" lr="" de="" pfr="">
       <Rad>base64 encoded fully valid Auth XML for
            resident
       </Rad>
  </Kyc>

Response Data:
  <Resp status="" ko="" ret="" code="" txn="" ts=""
        err=""> encrypted and base64 encoded KycRes
        element
  </Resp>

  <KycRes ret="" code="" txn="" ts="" ttl="" actn=""
      err="">
      <Rar>base64 encoded fully valid Auth response
          XML for resident
      </Rar>
      <UidData uid="">
          <Poi name="" dob="" gender="" />
          <Poa co="" house="" street="" lm="" loc=""
               vtc="" subdist="" dist="" state=""
               country="" pc="" po=""/>
          <LData lang="" name="" co="" house=""
               street="" lm="" loc="" vtc=""
               subdist="" dist="" state=""
               country="" pc="" po=""/>
          <Pht> base64 encoded JPEG photo of the
                resident
          </Pht>
          <Prn type="pdf"> base64 encoded signed
               Aadhaar letter for printing
          </Prn>
      </UidData>
      <Signature/>
  </KycRes>
```

Figure 3.1: Aadhaar's eKYC 2.1 API

ident's identity and address data from Aadhaar system. Only valid value is "Y". Without explicit consent of the Aadhaar holder application should not call this API [91]."

As can be seen from the specification, *rc* is a boolean consent and assumes that it has been transferred from resident to UIDAI unaltered. Although intermediate communication channels between various entities from resident to UIDAI are well

secured and access to eKYC data is provided only after receiving explicit consent from the resident, this way of taking consent from a resident has two shortcomings. First is that the consent is taken by a non-UIDAI entity and does not encode in itself a proof from the resident that it is (s)he who provided the consent. This is because residents do not have any registered tamper-proof crypto device which can be used to encrypt user consent using resident specific PIN or password. Second is that providing a boolean consent is too broad, either an unconditional access is given to the whole eKYC information or no access is given at all. A resident may wish to have a better privacy enhancing fine-grained access control to his/her eKYC data indicating details on *scope*, *purpose* and *recipient*.

3.4 Present model of eSign in India

In eSign version 2.0 [92], a resident first registers itself with a front end application-specific agency viz. a viz., *Application Service Provider* (ASP). A resident can use either OTP based authentication or biometric-based authentication. In case of OTP based authentication, OTP generation request is forwarded to UIDAI via ASP and ESP. UIDAI generates an OTP and sends it to the resident's registered mobile number. In case of biometric-based authentication, the resident gets his fingerprint/iris scanned through a registered device. After the authentication phase, the resident now initiates an eSign request through ASP by providing it with the consent to use his/her eKYC, the document to be signed and his/her Aadhaar number. Figure 3.2 illustrates present model of eSign. ASP calculates the cryptographic hash of the document and sends it along with the resident's consent and resident's Aadhaar number to ESP. ESP takes authentication proof from the resident, creates a random symmetric key SK_{ESP_UIDAI} and a Personal Identity Data Object (PID). PID encodes in itself the resident's authentication proof and the cryptographic hash of the PID object (SHA256(PID)). ESP first encrypts PID with SK_{ESP_UIDAI}, second encrypts cryptographic hash of PID (SHA256(PID)) with SK_{ESP_UIDAI} and third encrypts SK_{ESP_UIDAI} with public key of UIDAI (PB_{UIDAI}). ESP now wraps them in a new object called "Auth" and sends it to UIDAI in eKYC request. UIDAI provides eKYC information to ESP. Using received eKYC information, ESP generates a Digital Signature Certificate (DSC) and provides it to ASP. ASP provides the digitally signed document to the resident.

In practice, the initial authentication phase in eSign request is the most time consuming since it involves either the manual text input (in case of OTP based authentication) or the physical scan of the fingerprint/iris (in case of biometric-based authentication). Other than that, in some use cases such as *Create Birth Certificate*,

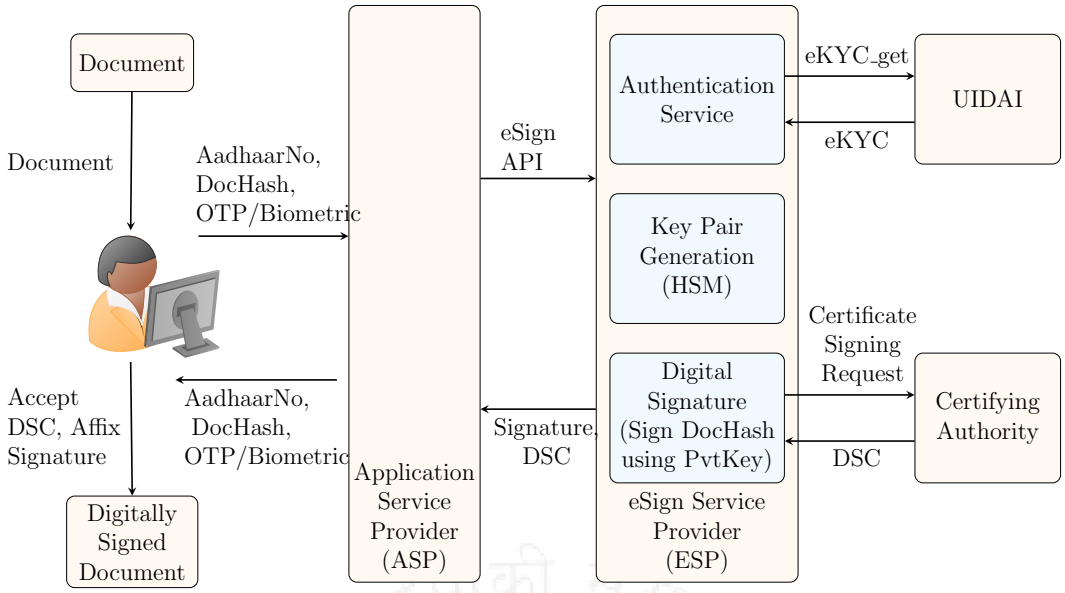


Figure 3.2: Present model of eSign

Create Death Certificate, *Student Enrolment*, etc., the application is most heavily used during a certain time period (nearing the end of a deadline) which puts a sudden nationwide load on UIDAI services.

3.5 Using digital tokens in eSign

The present model of eSign has few limitations. The first limitation is that in present model of eSign, eKYC data access reflects a restrictive *self-only*, *full-resource* and *unlimited* access control. A resident may wish to have a better access control mechanism reflecting *third-entity-also*, *partial resource*, *use-limited* and *time-limited*.

The second limitation is that a resident has to authenticate himself/herself for each eSign request and include the corresponding authentication proof in each eSign request.

If a resident wishes to eSign a large number of documents, the initial authentication phase consumes most of the overall eSign time. After taking necessary consent from the resident, his/her authentication proof be stored with ESP in the first request and is reused in rest of the requests.

A digital access token (refer figure 3.6) can be used to include claims from participating entities (ESP and UIDAI). A new service named *GenerateAccessToken* is proposed to be introduced by UIDAI.

In this proposed model of eSign (refer figures 3.7, 3.8), resident first authenti-

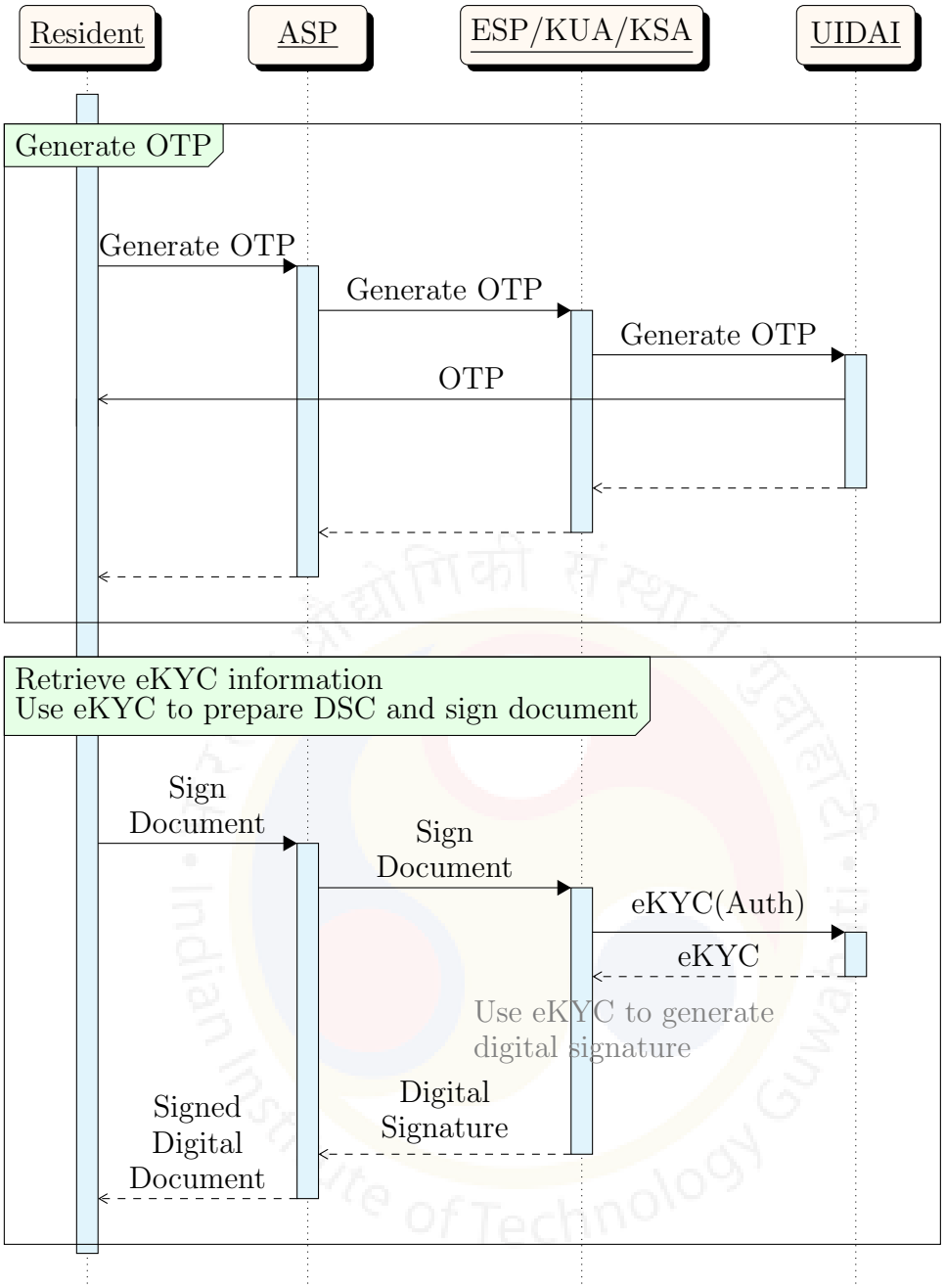


Figure 3.3: Sequence diagram of eSign 2.0

cates himself/herself using OTP or biometric-based authentication and sends eSign request to ASP. ASP forwards this eSign request to ESP. ESP takes OTP and permission to generate access token from resident and creates an "Auth" object. This "Auth" object is created as before but additionally including ESP claims as well. ESP sends *GenerateAccessToken* request to UIDAI including "Auth" object. After receiving this request, UIDAI creates an access token including its own claims as well as claims received from ESP. UIDAI sends this access token back to the ESP. Now, ESP sends eKYC request to UIDAI including this access token instead of the "Auth" object. After receiving eKYC information from UIDAI, ESP generates *Dig-*

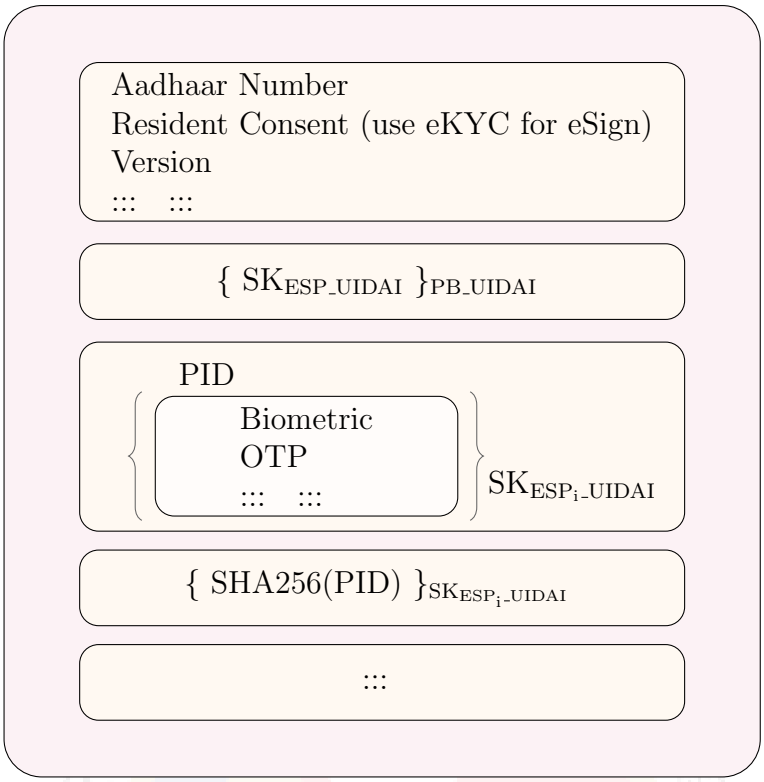


Figure 3.4: Auth Object (eSign 2.0)

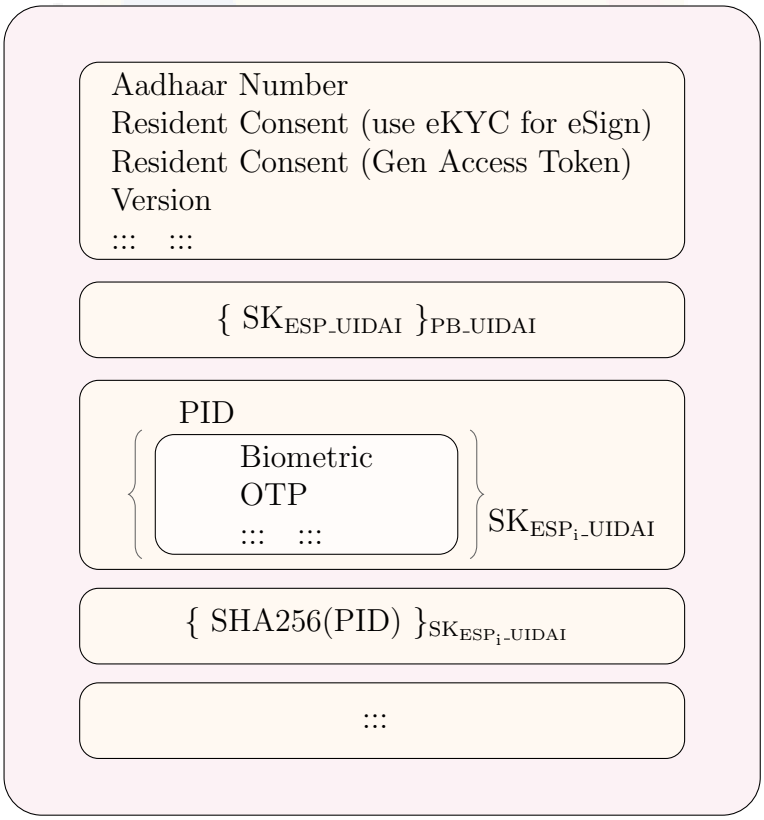


Figure 3.5: Proposed Auth Object

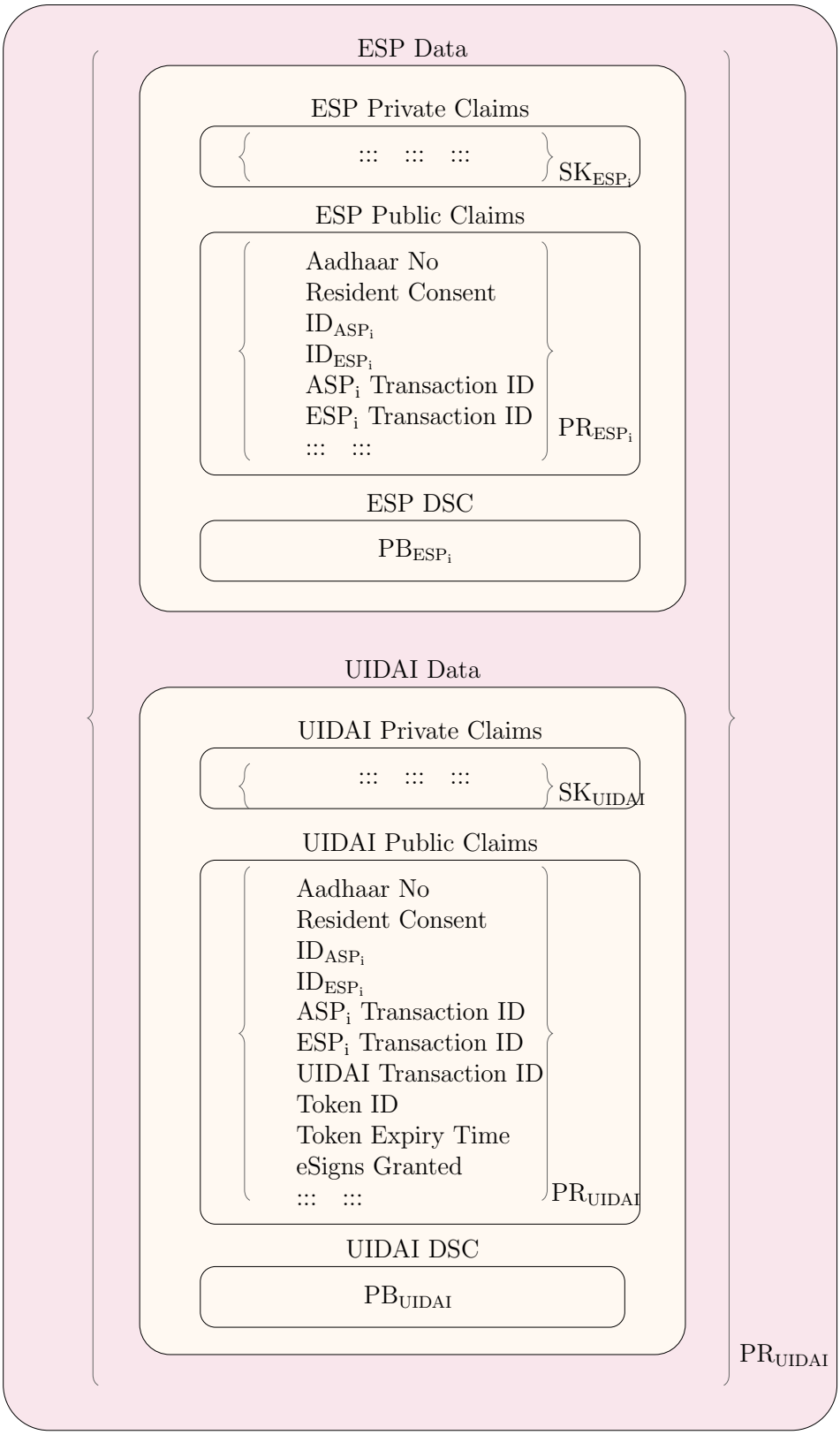


Figure 3.6: Proposed Access Token Structure - I

ital Signature Certificate (DSC) from it and provides the same to ASP. ASP embeds DSC in the document and sends the digitally signed document to the resident. For all rest of the eSign requests, ESP can reuse the same access token in eKYC requests

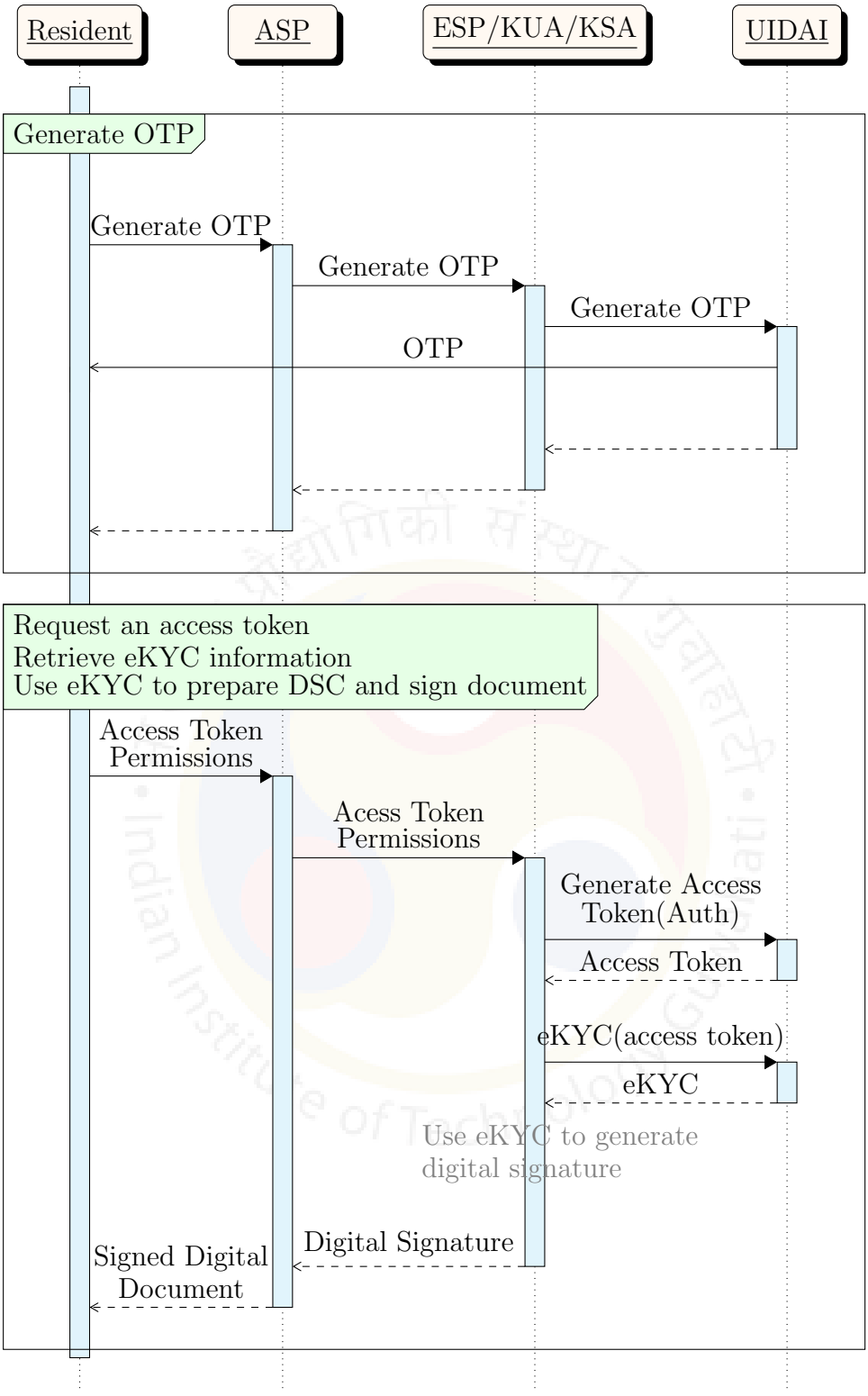


Figure 3.7: First call to eSign in eSign model (first iteration)

and avoid the initial authentication phase.

This chapter also presented two usability scenarios, based on whether the eKYC information can be cached by ESP or not. If ESP is permitted to reliably and securely store eKYC information of the resident, even the repeated eKYC requests

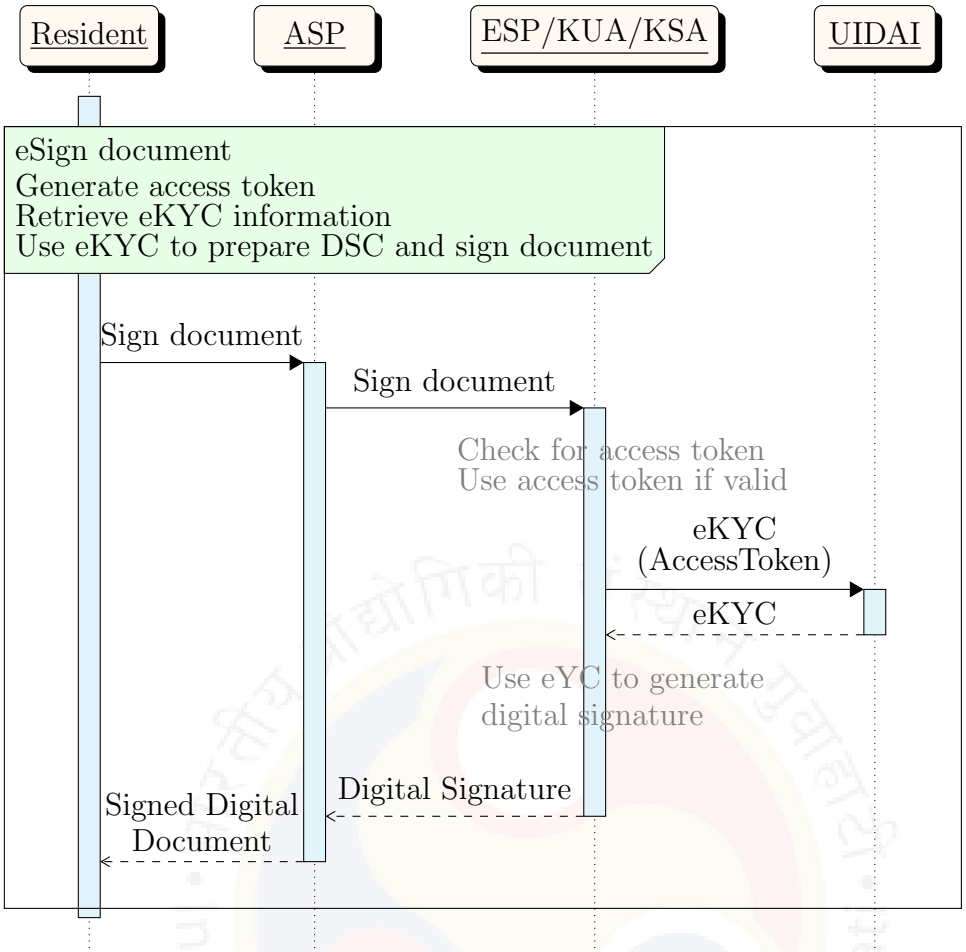


Figure 3.8: Second call to eSign in case eKYC needs to be fetched again

from ESP to UIDAI can be avoided.

This chapter also presented a performance comparison analysis of the proposed model with the present model and found substantial improvement in the amortized performance of eSign.

3.6 Proposed model of privacy aware eSign

The digital access token introduced in section 3.5 is used to increase the amortized performance of eSign by storing necessary claims from UIDAI and ESP. The same token can be enhanced to include claims from a resident as well. A resident can encode claims related to privacy and fine-grained access control of his/her eKYC data. A stricter PEaFGAC statement may be enforced centrally at UIDAI level and an overriding less strict rule can be supplied with each eKYC request to grant access to the requesting entity.

```
AadhaarNo
POI:
  name, dob
POA:
  co, house, street, lm, loc, vtc, subdist, dist,
  state, country, pc, po
LData:
  lang, name, co, house, street, lm, loc, vtc,
  subdist, dist, state, country, pc, po
Pht:
  <Base64 encoded JPEG photo of resident
Org:
  dep, desig
Other:
  email
```

Figure 3.9: eKYC information assumed to be available

3.6.1 Privacy aware attribute-based policy

A PEaFGAC statement encodes in itself the *scope* of information which can be provided, the *purpose* for which the information can be provided and attributes of *recipients* to whom the information can be provided. These statements are comprised of small sub-statements which are combined using relational operators. Each statement is identified by a numeric *id* and an alphanumeric *tag*.

An example of a PEaFGAC statement is presented in figure 3.10. This statement encodes in it that the purpose for seeking eKYC information should be eSign, seeking entity must either have the email in domain *finance.iitg.ac.in*, or must be working in *finance* department of *Indian Institute of Technology, Guwahati (IITG)*, or must have a designation of *director* or above. The statement is uniquely identified by a statement identifier (*ID*) and has a small alphanumeric representational string (*TAG*). Other than these, the statement also encodes in it the purpose for which eKYC can be accessed (*Purpose*), required (*eKYC*) attributes of information seeker (*AP*) and eKYC information which can be provided to the requester (*scope*). If required, a user can have multiple privacy statements for his/her eKYC data represented by different tags.

It is assumed that all entities which request eKYC data also have their eKYC information available with UIDAI. This includes not just the users but the organizations such as ESPs as well. To better understand an entity (both users and organizations), it is proposed that eKYC fields are expanded to include more details such as entity type (indicating whether the subject is a human or an organization), resident's organization, resident's department, resident's designation, etc. When an

```
PS.ID:
  5
PS.Tag:
  eSignDoc
PS.Purpose:
  eSign
PS.AP:
  (email = *@finance.iitg.ac.in)       OR
  (org = IITG AND org.dep = finance)   OR
  (desig >= director)
PS.Scope:
  poi.name, poi.dob, poa.country, Ldata.lang
```

Figure 3.10: Example of a PEaFGAC statement

entity attempts to access eKYC data of a resident, entity's eKYC data and purpose for which the eKYC data is sought are verified against PEaFGAC statement protecting eKYC data to decide whether the requisite access can be granted or not. Only if the access can be granted, the eKYC data be provided to the requesting entity. The eKYC data provided to the entity is limited in scope by PEaFGAC statement. For the rest of this chapter, eKYC data is assumed to consists of at least the information presented in figure 3.9.

3.6.2 Privacy aware attribute-based policy token

The digital token introduced earlier can be enhanced to include resident claims including PEaFGAC statement (refer figure 3.11). Before sending an eSign request, resident creates a PEaFGAC token by sending a token generation request to UIDAI through ASP and ESP. During the token generation process, the resident is redirected to UIDAI web page where (s)he provides OTP value for authentication and PEaFGAC statement for privacy and fine-grained access to his/her eKYC data. Subsequently, UIDAI verifies the OTP value and signs a cryptographic hash of the statement with its private key and stores the signed hash in resident's private claims and stores the statement in plaintext in resident's public claims section of PEaFGAC digital access token.

Tables 3.2-3.6 depicts sequence and details of communication messages among participating entities for generation of a token. First column indicates the message identifier, second column indicates the participating entities and the direction of communication and third column indicates what message is sent and how it is constructed.

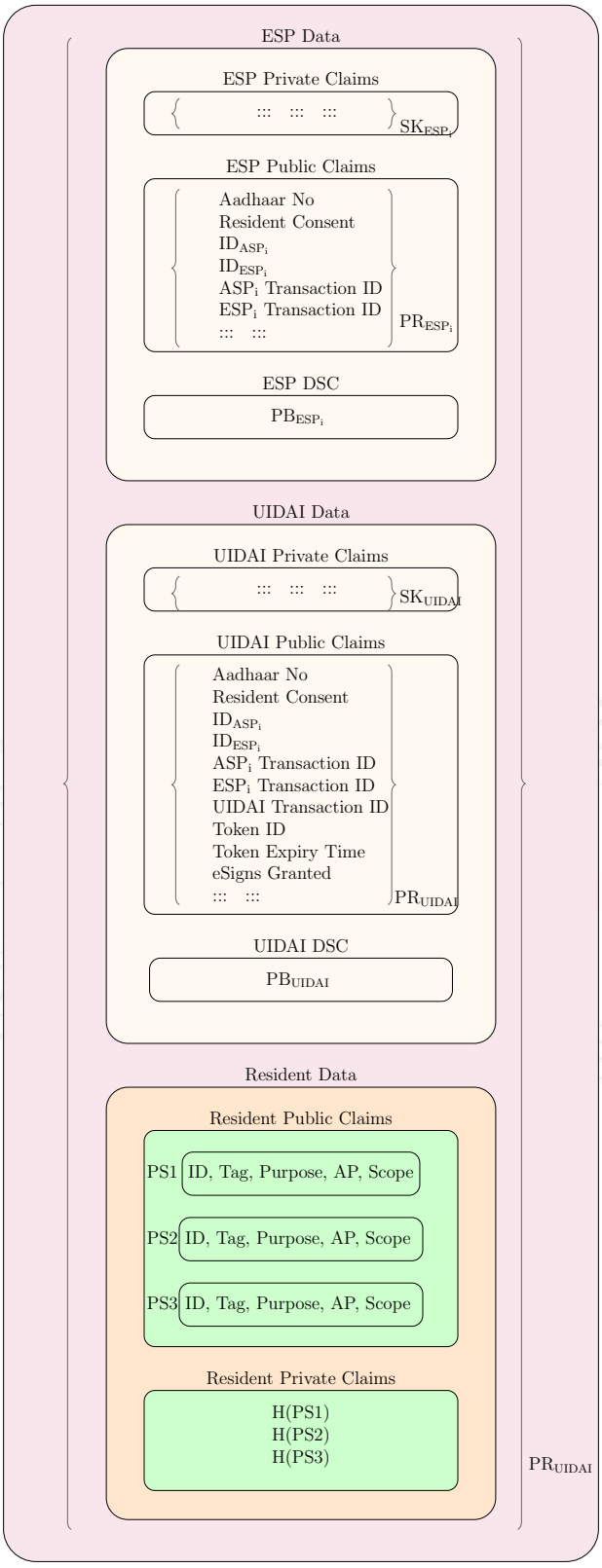


Figure 3.11: Proposed (PEaFGAC) Token Structure - II

3.6.3 Privacy aware attribute-based eSign

This section presents how PEaFGC statement for eKYC data and PEaFGAC token can be used to implement *Privacy Aware eSign*. It is assumed that PEaFGAC token

Login to ASP		
TGM1	R → ASP	Generate nonce $n1_{R_i}$ $DataR_1 = ID_{R_i} \| PW_{R_i} \| PB_{B_i} \| n1_{R_i}$ $SignR_1 = \{H(DataR_1)\}_{PR_{B_i}}$ $\{ \text{loginReq}(DataR_1, SignR_1) \}_{PB_{ASP_i}}$
TGM2	R ← ASP	$DataA_1 = C_{R_i} \oplus (n1_{R_i} + 1)$ $SignA_1 = \{H(DataA_1)\}_{PR_{ASP}}$ $\{ \text{loginRes}(DataA_1, SignA_1)\}_{PB_{B_i}}$

Table 3.2: Proposed PEaFGAC Token Generation protocol

has already been generated as explained in section 3.6.2. It is also assumed that the communication channel between resident and ASP is secured using SSL/TLS, between ASP and ESP is secured using SSL/TLS and between ESP and UIDAI is secured using dedicated secure leased lines.

Tables 3.7-3.8 depict sequence and details of communication messages transferred in eSign request in case eKYC needs to be fetched again.

3.6.4 Security Analysis

This section presents a formal security analysis of the proposed scheme using *Burrows-Abadi-Needham (BAN) logic* [93]. It is assumed that PEaFGAC token has already been generated securely. Analysis of the token generation request can be done similarly. BAN logic is a well-known model used to find beliefs of participants in a cryptographic protocol.

The security environment is assumed to be based on *Delev-Yao model* in which all messages are communicated over public channels and an attacker can see, modify, compose and replay messages but cannot break cryptographic principles. The security environment also assumes that an attacker can decipher messages if he has a valid decryption key. Some of the fundamental operators used in BAN logic are defined in table 3.9. An extension to BAN logic, defined in table 3.10 is required to analyse the proposed model.

Rules of Inference

[R1:] *Message meaning rules* concern the interpretation of messages. They all derive beliefs about the origin of messages.

Generate OTP		
TGM3	$R \rightarrow ASP$	Generate nonce $n2_{R_i}$ $DataR_2 = AadhaarNo_{R_i} \| C_{R_i} \| n2_{R_i}$ $SignR_2 = \{H(DataR_2)\}_{PR_{B_i}}$ $\{$ getotpASPReq$(DataR_2, SignR_2)$ $\}_{PB_{ASP_i}}$
TGM4	$ASP \rightarrow ESP$	Generate nonce $n1_{ASP_i}$ $DataA_1 = AadhaarNo_{R_i} \| ID_{ASP_i} \|$ $License_{ASP_i} \| TID_{ASP_i} \| n1_{ASP_i}$ $SignA_1 = \{H(DataA_1)\}_{PR_{ASP_i}}$ $\{$ getotpESPReq$(DataA_1, SignA_1)$ $\}_{PB_{ESP_i}}$
TGM5	$ESP \leftarrow UIDAI$	Generate nonce $n1_{ESP_i}$ $DataE_1 = AadhaarNo_{R_i} \| ID_{ESP_i} \|$ $License_{ESP_i} \| TID_{ESP_i} \| n1_{ESP_i}$ $SignE_1 = \{H(DataE_1)\}_{PR_{ESP_i}}$ $\{$ getotpReq$(DataE_1, SignE_1)$ $\}_{PB_{UIDAI}}$
TGM6	$R \leftarrow UIDAI$	$\{$ OTP $\}_{SecureCellularNetwork}$
TGM7	$ESP \leftarrow UIDAI$	$DataU_1 = returnStatus \| TID_{ESP_i} \|$ $MaskedMobileNo \| (n1_{ESP_i} + 1)$ $SignU_1 = \{H(DataU_1)\}_{PR_{UIDAI}}$ $\{$ getotpRes$(DataU_1, SignU_1)\}_{PB_{ESP_i}}$
TGM8	$ESP \leftarrow ASP$	$DataE_2 = returnStatus \| TID_{ASP_i} \|$ $MaskedMobileNo \| (n1_{ASP_i} + 1)$ $SignE_2 = \{H(DataE_2)\}_{PR_{ESP_i}}$ $\{$ getotpESPRes$(DataE_2, SignE_2)\}_{PB_{ASP_i}}$
TGM9	$ESP \leftarrow R$	$DataA_2 = returnStatus \|$ $MaskedMobileNo \| (n2_{R_i} + 1)$ $SignA_2 = \{H(DataA_2)\}_{PR_{ASP_i}}$ $\{$ getotpASPRes$(DataA_2, SignA_2)\}_{PB_{B_i}}$

Table 3.3: Proposed PEaFGAC Token Generation protocol

Generate Token		
TGM10	R $\rightarrow$ ASP	Generate nonce $n3_{R_i}$ $DataR_3 = C_{R_i} \| n3_{R_i}$ $SignR_3 = \{H(DataR_3)\}_{PR_{B_i}}$ $\{$ gentokASPReq$(DataR_3, SignR_3)$ $\}_{PB_{ASP_i}}$
TGM11	ASP $\rightarrow$ ESP	Generate nonce $n2_{ASP_i}$ $DataA_3 = AadhaarNo_{Ri} \| ID_{ASP_i} \| License_{ASP_i} \| TID_{ASP_i} \| n2_{ASP_i}$ $SignA_3 = \{H(DataA_3)\}_{PR_{ASP_i}}$ $\{$ gentokESPReq$(DataA_3, SignA_3)$ $\}_{PB_{ESP_i}}$
TGM12	ESP $\rightarrow$ UIDAI	Generate nonce $n3_{ESP_i}$ $DataE_3 = AadhaarNo_{Ri} \| ID_{ESP_i} \| License_{ESP_i} \| TID_{ESP_i} \| n3_{ESP_i}$ $SignE_3 = \{H(DataE_3)\}_{PR_{ESP_i}}$ $\{$ gentokUIDAIReq$(DataE_3, SignE_3)$ $\}_{PB_{UIDAI}}$
TGM13	UIDAI $\leftarrow$ ESP	Generate nonce $n1_{UIDAI}$ $DataU_1 =$ UIDAIRedirectURL (ForTakingPrivacyStatements)$\| PB_{UIDAI} \| TID_{ESP_i} \| n1_{UIDAI}$ $SignU_1 = \{H(DataU_1)\}_{PR_{UIDAI}}$ $\{$ genpsUIDAIReq$(DataU_1, SignU_1)$ $\}_{PB_{ESP_i}}$
TGM14	ESP $\leftarrow$ ASP	Generate nonce $n4_{ESP_i}$ $DataE_4 =$ UIDAIRedirectURL (ForTakingPrivacyStatements) $\| PB_{UIDAI} \| TID_{ASP_i} \| n4_{ESP_i}$ $SignE_4 = \{H(DataE_3)\}_{PR_{ESP_i}}$ $\{$ genpsESPReq$(DataE_4, SignE_4)$ $\}_{PB_{ASP_i}}$

Table 3.4: Proposed PEaFGAC Token Generation protocol

For shared secrets, the inference rule is

$$\frac{P \models Q \overset{Y}{\rightleftharpoons} P,\ P \lhd \langle X \rangle_Y}{P \models Q \rhd X} \tag{3.1}$$

TGM15	ASP $\leftarrow$ R	Generate nonce $n4_{R_i}$ $DataA_4$ = { Present UIDAIRedirectURL to Resident which requests him to provide OTP Value and Privacy statements$\|PB_{UIDAI}\|n4_{R_i}$} $SignA_4 = \{H(DataA_4)\}_{PR_{ASP_i}}$ { $genpsASPReq(DataA_4, SignA_4)$ }$_{PB_{B_i}}$
TGM16	R $\rightarrow$ UIDAI	{ PEaFGACPrivacyStatements }$_{PB_{UIDAI}}$

Table 3.5: Proposed PEaFGAC Token Generation protocol

That is, if P believes that the secret Y is shared with Q and sees $\langle X \rangle_Y$, then P believes that Q once said X.

[R2:] The *nonce-verification* rule expresses the check that a message is recent, and hence, that the sender still believes in it:

$$\frac{P \models \#(X),\ P \models Q \rhd X}{P \models Q \models X} \tag{3.2}$$

That is, if P believes that X could have been uttered only recently and that Q once said X, then P believes that Q believes X.

[R3:] The *jurisdiction* rule states that if P believes that Q has jurisdiction over X, then P trusts Q on the truth of X:

$$\frac{P \models Q \Rightarrow X,\ P \models Q \models X}{P \models X} \tag{3.3}$$

[R4:] The *seeing* rule states that if a principal sees a formula, then he also sees its components, provided he knows the necessary keys:

$$\frac{P \lhd (X, Y)}{P \lhd X}, \quad \frac{P \lhd \langle X \rangle_Y}{P \lhd X}, \quad \frac{P \models Q \overset{K}{\leftrightarrow} P(,)P \lhd \{X\}_K}{P \lhd X},$$

$$\frac{P \models \overset{K}{\mapsto} P,\ P \lhd \{X\}_K}{P \lhd X}, \quad \frac{P \models \overset{K}{\mapsto} P,\ P \lhd \{X\}_{K^{-1}}}{P \lhd X} \tag{3.4}$$

Note that if P sees X and P sees Y it does NOT follow that P sees (X, Y) since that means that X and Y were uttered at the same time.

PEaFGAC Token Generation Request		
TGM17	R $\rightarrow$ ASP	$\text{DataR}_4 = \text{C}_{\text{R}_i} \| (\text{n4}_{\text{R}_i} + 1)$ $\text{SignR}_4 = \{\text{H}(\text{DataA}_4)\}_{\text{PR}_{\text{B}_i}}$ $\{$ genpsASPRes$(\text{DataA}_4, \text{SignA}_4)$ $\}_{\text{PB}_{\text{B}_i}}$
TGM18	ASP $\leftarrow$ ESP	$\text{DataA}_5 = (\text{n4}_{\text{ESP}_i} + 1)$ $\text{SignA}_5 = \{\text{H}(\text{DataA}_4)\}_{\text{PR}_{\text{ASP}_i}}$ $\{$ genpsESPRes$(\text{DataA}_4, \text{SignA}_4)$ $\}_{\text{PB}_{\text{ESP}_i}}$
TGM19	ESP $\leftarrow$ UIDAI	$\text{DataE}_5 = (\text{n1}_{\text{UIDAI}} + 1)$ $\text{SignE}_5 = \{\text{H}(\text{DataE}_5)\}_{\text{PR}_{\text{ESP}_i}}$ $\{$ genpsUIDAIRes$(\text{DataE}_5, \text{SignE}_5)$ $\}_{\text{PB}_{\text{UIDAI}}}$
TGM20	ESP $\leftarrow$ UIDAI	Create $\text{PEaFGACTokenAT}_{\text{Ri}}$ $\text{DataU}_2 = \text{AT}_{\text{Ri}} \| (\text{n3}_{\text{ESP}_i} + 1)$ $\text{SignU}_2 = \{\text{H}(\text{DataE}_5)\}_{\text{PR}_{\text{ESP}_i}}$ $\{$ gentokUIDAIRes$(\text{DataE}_5, \text{SignE}_5)$ $\}_{\text{PB}_{\text{UIDAI}}}$
TGM21	ASP $\leftarrow$ ESP	$\text{DataE}_6 = (\text{n2}_{\text{ASP}_i} + 1)$ $\text{SignE}_6 = \{\text{H}(\text{DataE}_5)\}_{\text{PR}_{\text{ESP}_i}}$ $\{$ gentokESPRes$(\text{DataE}_6, \text{SignE}_6)$ $\}_{\text{PB}_{\text{ASP}_i}}$
TGM22	R $\leftarrow$ ASP	$\text{DataA}_5 = (\text{n3}_{\text{R}_i} + 1)$ $\text{SignA}_5 = \{\text{H}(\text{DataE}_5)\}_{\text{PR}_{\text{ASP}_i}}$ $\{$ gentokESPRes$(\text{DataA}_5, \text{SignA}_5)$ $\}_{\text{PB}_{\text{R}_i}}$

Table 3.6: Proposed PEaFGAC Token Generation protocol

[R5:] The *fresh* rule states that if one part of the formula is fresh, then the entire formula must be fresh.

$$\frac{\text{P} \models \#(\text{X})}{\text{P} \models \#(\text{X}, \text{Y})} \tag{3.5}$$

[R6:] The *belief* rule states that if P believes one part of the formula, then it also believe part of the formula.

$$\frac{\text{P} \models (\text{X}, \text{Y})}{\text{P} \models (\text{X})} \tag{3.6}$$

Login to ASP		
M1	R → ASP	Generate nonce $n1_{R_i}$ $DataR_1 = ID_{R_i} \| PW_{R_i} \| PB_{B_i} \| n1_{R_i}$ $SignR_1 = \{H(DataR_1)\}_{PR_{B_i}}$ $\{ \text{loginReq}(DataR_1, SignR_1) \}_{PB_{ASP_i}}$
M2	R ← ASP	$DataA_1 = C_{R_i} \oplus (n1_{R_i} + 1)$ $SignA_1 = \{H(DataA_1)\}_{PR_{ASP}}$ $\{ \text{loginRes}(DataA_1, SignA_1)\}_{PB_{B_i}}$
Initiate eSign request		
M3	R → ASP	Generate nonce $n2_{R_i}$ $DataR_2 = M_i \| consent_{use\_ekyc} \|$ $consent_{genuse\_at} \| C_{R_i} \| n2_{R_i}$ $SignR_2 = \{H(DataR_2)\}_{PR_{B_i}}$ $\{ \text{signdocASPReq}(DataR_2, SignR_2) \}_{PB_{ASP_i}}$
M4	ASP ← ESP	Generate nonce $n1_{ASP_i}$ $DataA_3 = H(M_i) \| AadhaarNo_{R_i} \| ID_{ASP_i} \|$ $License_{ASP_i} \| TID_{ASP_i} \|$ $consent_{use\_ekyc} \| consent_{genuse\_at} \|$ $n1_{ASP_i}$ $SignA_3 = \{H(DataA_3)\}_{PR_{ASP_i}}$ $\{ \text{signdocESPReq}(DataA_3, SignA_3) \}_{PB_{ESP_i}}$

Table 3.7: Proposed Privacy Aware eSign model

Extended Rules of Inference

[R7:] If receiver entity E_R believes that C_R is a cookie associated with a unique session from resident R, PB_B is public key with browser used by resident R, PB_{E_R} is public key of receiver entity E_R, n_R is a fresh nonce generated by R, E_R receives message of the form $\{\text{CommMsgReq}(X \| C_R \| n_R, \{H(X \| C_R \| n_R)\}_{PR_{B_i}})\}_{PB_{E_R}}$, then E_R believes that X is sent by entity R and communication channel from R to E_R is secure and no message is observed, modified or replayed by an intruder.

Retrieve eKYC (reusing access token) and sign document		
M5	ESP $\rightarrow$ UIDAI	Generate nonce $n1_{ESP_i}$ If AT_{R_i} is valid use it $DataE_5 = AT_{R_i} \| H(M_i) \| n1_{ESP_i}$ $SignE_5 = \{H(DataE_5)\}_{PR_{ESP_i}}$ $\{$ kycESPReq$(DataE_5, SignE_5)$ $\}_{PB_{UIDAI}}$
M6	ESP $\leftarrow$ UIDAI	Retrieve $eKYC_{ESP_i}$ Retrieve $AT_{R_i} \rightarrow UC \rightarrow AP$ Verify whether access can be granted based on above two parameters. $eKYC_{R_i}$ = eKYC of resident scoped by $AT_{R_i} \rightarrow UC \rightarrow$ scope $DataU_3 = eKYC_{R_i} \| (n1_{ESP_i} + 1)$ $SignU_3 = \{H(DataU_3)\}_{PR_{UIDAI}}$ $\{$ kycESPRes$(DataU_3, SignU_3)$ $\}_{PB_{ESP_i}}$
*M*7	ASP $\leftarrow$ ESP	Generate key pair PB_{R_i} PR_{R_i} using $eKYC_{R_i}$ $SignChain = \{ PB_{R_i} \}_{PR_{ESP_i}} \|$ $\{ PB_{ESP_i} \}_{PR_{CCA}}$ $DSC_{R_i\_M_i} = \{ eKYC_{R_i} \| H(M_i) \}_{PR_{R_i}} \|$ $PB_{R_i} \| SignChain$ Delete PR_{R_i} $DataU_2 = DSC_{R_i\_M_i} \| TID_{ASP_i} \| (n1_{ASP_i} + 1)$ $SignU_2 = \{H(DataU_2)\}_{PR_{ESP_i}}$ $\{$ signdocESPRes$(DataU_2, SignU_2)$ $\}_{PB_{ASP_i}}$
M8	R $\leftarrow$ ASP	$\{M_i\}_{eSign\_R_i\_ESP_i} = M_i \| DSC_{R_i\_M_i}$ $DataA_6 = \{M_i\}_{eSign\_R_i\_ESP_i} \| (n2_{R_i} + 1)$ $SignA_6 = \{H(DataA_6)\}_{PR_{ASP_i}}$ $\{$ signdocASPRes$(DataA_6, SignA_6)$ $\}_{PB_{B_i}}$
M9	R $\leftrightarrow$ R	Verify correctness of eKYC, H(M) and SignChain in $\{M_i\}_{eSign}$

Table 3.8: Proposed Privacy Aware eSign model

Operator Usage	**Description**
$P \models X$	P believes statement X
$P \lhd X$	P sees statement X
$P \longmapsto X$	P controls X
$\#(X)$	Message X is fresh
$P \overset{K}{\leftrightarrow} Q$	P and Q share key K
$\overset{K}{\mapsto} P$	P has K as its public key
$P \overset{X}{\rightleftharpoons} Q$	Formula X is a secret known only to P and Q
$\{X\}_K$	Formula X is encrypted using K
$\langle X \rangle_Y$	Formula X is combined with formula Y

Table 3.9: Fundamental BAN operators

Operator Usage	**Description**
$M_{eSign\_R\_ESP\_CCA}$	eSign of message M is done by Resident R through ESP approved by CCA $M_{eSign\_R\_ESP\_CCA}$ $= M \Vert DSC_{R\_M}$ $= M \Vert \{eKYC_R \Vert H(M)\}_{PR_R} \Vert PB_R \Vert SignChain$ $= M \Vert \{eKYC_R \Vert H(M)\}_{PR_R} \Vert PB_R \Vert \{PB_R\}_{PR_{ESP}} \Vert \{PB_{ESP}\}_{PR_{CCA}}$
$P \models E_i \xrightarrow{secure} E_j$	P believes that communication from entity E_i to E_j is secure
$P \models E_i \xleftarrow{secure} E_j$	P believes that communication from entity E_j to E_i is secure
$P \models E_i \xleftrightarrow{secure} E_j$	P believes that communication between entities E_i and E_j is secure in both directions
$P \models E_i \xleftrightarrow{ACTPerm} E_j$	P believes that entity E_i has given permission for action ACT to entity E_j
$P \models C_R \rightsquigarrow E_i$	P believes that cookie C_R is associated with logged-in entity E_i
$E_R \models E_R \xrightarrow{C_{E_R} \rightarrow ID_{E_R}} E_R$	E_R believes that it has securely communicated its identity ID_{E_R} to entity E_R through cookie C_{E_R}

Table 3.10: Extended BAN operators

$$\frac{\begin{array}{lcl} E_R & \models & \overset{PB_{E_R}}{\longmapsto} E_R, \\ E_R & \models & C_R \rightsquigarrow S, \\ E_R & \models & \#n_R, \\ E_R & \models & \{\{Y\}_{PR_R}\}_{PB_R} = Y \\ E_R & \lhd & \{\ \text{CommMsgReq}\ (X \parallel C_R \parallel n_R, \\ & & \quad \{H(X\|C_R\|n_R)\}_{PR_{R_i}})\ \}_{PB_{E_R}} \end{array}}{\begin{array}{lcl} E_R & \models & R \xrightarrow{\text{Secure}} E_R, \\ E_R & \models & R \rhd X \end{array}} \tag{3.7}$$

[R8:] If receiver entity E_R believes that PB_{E_R} is public key of receiver entity E_R, n_{E_R} is a fresh nonce generated by E_R, E_R receives message of the form $\{\ \text{CommMsgReq}\ (X\|n_{E_R}, \{H(X\|n_{E_R})\}_{PR_{E_R}})\ \}_{PB_{E_R}}$, then E_R believes that X is sent by entity E_R and communication channel from E_R to E_R is secure and no message is observed, modified or replayed by an intruder.

$$\frac{\begin{array}{lcl} E_R & \models & \overset{PB_{E_R}}{\longmapsto} E_R, \\ E_R & \models & \{\{Y\}_{PR_{E_R}}\}_{PB_{E_R}} = Y, \\ E_R & \models & \#n_{E_R} \\ E_R & \lhd & \{\ \text{CommMsgReq}\ (\ X \parallel n_{E_R}, \\ & & \quad \{H(X\|n_{E_R})\}_{PR_{E_R}})\ \}_{PB_{E_R}} \end{array}}{\begin{array}{lcl} E_R & \models & E_R \xrightarrow{\text{Secure}} E_R \\ E_R & \models & E_R \rhd X \end{array}} \tag{3.8}$$

[R9:] If receiver entity E_R believes that communication from all possible sender entities E_{R_i} to E_R ($\forall i = 1...n$) is secure, then E_R believes that communication channel to E_R is secure and no message is observed, modified or replayed by an intruder.

$$\frac{E_R \models E_{R_i} \xrightarrow{\text{secure}} E_R \quad (\forall i = 1...n)}{E_R \models \xrightarrow{\text{Secure}} E_R} \tag{3.9}$$

[R10:] If resident R believes that C_R is a cookie associated with a unique session from resident R, PB_{E_R} is the public key of entity E_R, n_R was a fresh nonce generated by R and used in a previous request call from R to E_R, R receives a message of the form $\{\text{CommMsgRes}(X\|(n_R+1), \{H(X\|(n_R+1)\}_{PR_{E_R}})\}_{PB_{E_R}}$, then E_R believes that X is sent by entity R and communication channel from R to E_R is secure and no message is observed, modified or replayed by an

intruder.

$$\frac{\begin{array}{lcl} R & \models & \overset{PB_{E_R}}{\longmapsto} E_R, \\ R & \models & C_R \rightsquigarrow S, \\ R & \models & \#(n_R - 1), \\ R & \lhd & \{\text{CommMsgRes } (X \parallel (n_R + 1), \\ & & \quad \{H(X \| (n_R + 1)\}_{PR_{E_R}})\}_{PB_{E_R}} \end{array}}{\begin{array}{lcl} R & \models & R \overset{\text{Secure}}{\longleftarrow} E_R, \\ RS & \models & X \lhd E_R \end{array}} \tag{3.10}$$

[R11:] If sender entity E_R believes that PR_{E_R} is private key of sender entity E_R, PB_{E_R} is public key of receiver entity E_R, n_{E_R} was a fresh nonce generated by R and used in a previous request call from E_R to E_R, E_R receives message of the form $\{\text{CommMsgRes } (X \| (n_{E_R} + 1), \{H(X \| (n_{E_R} + 1)\}_{PR_{E_R}})\}_{PB_{E_R}}$, then E_R believes that X is sent by entity E_R and communication channel from E_R to E_R is secure and no message is observed, modified or replayed by an intruder.

$$\frac{\begin{array}{lcl} E_R & \models & \overset{PB_{E_R}}{\longmapsto} E_R, \\ E_R & \models & \{\{X\}_{PR_{E_R}}\}_{PB_{E_R}} = X, \\ E_R & \models & \#(n_{E_R} - 1), \\ R & \lhd & \{\text{CommMsgRes } (X \parallel (n_{E_R} + 1), \\ & & \quad \{H(X \| (n_{E_R} + 1))\}_{PR_{E_R}})\}_{PB_{E_R}} \end{array}}{\begin{array}{lcl} E_R & \models & E_R \overset{\text{Secure}}{\longleftarrow} E_R, \\ E_R & \models & X \lhd E_R \end{array}} \tag{3.11}$$

[R12:] If sender entity E_R believes that communication from all possible receiver entities E_{R_i} ($\forall i = 1...n$) is secure, then E_R believes that communication channel to E_R is secure and no message is observed, modified or replayed by an intruder.

$$\frac{E_R \models E_R \overset{\text{secure}}{\longleftarrow} E_{R_i} \quad (\forall i = 1...n)}{E_R \models E_R \overset{\text{Secure}}{\longleftarrow}} \tag{3.12}$$

[R13:] An electronic signature (M_{ieSign}) is a valid signature only when resident verifies that three main parts in signature, viz., eKYC, H(M) and SignChain are as expected.

$$\begin{array}{lcll} R & \models & \text{geteKYC}(M_{\text{ieSign}}) & = & \text{KYC} \\ R & \models & \text{getHM}(M_{\text{ieSign}}) & = & \text{H(M)} \\ R & \models & \text{getSignChain}(M_{\text{ieSign}}) & = & \text{Valid} \\ \hline R & \models & M_{\text{ieSign}} & = & \text{Valid} \end{array} \quad (3.13)$$

Assumptions

The protocol makes several assumptions. The assumptions relevant for the discussion of this chapter are listed below.

[A1:] It is assumed that all sessions from all residents R_i keeps their cookie C_{R_i} secret.

[A2-A6:] The scheme makes several assumptions about public keys. For example, R_i believes that PB_{ASP_i} is public key of ASP_i. Similar to this, other entities also make similar assumptions. These assumptions are listed below.

$$\begin{array}{lcll} R_i & \models & \xmapsto{PB_{ASP_i}} & ASP_i \\ ESP_i & \models & \xmapsto{PB_{ASP_i}} & ASP_i \\ ASP_i & \models & \xmapsto{PB_{ESP_i}} & ESP_i \\ UIDAI & \models & \xmapsto{PB_{ESP_i}} & ESP_i \\ ESP_i & \models & \xmapsto{PB_{UIDAI}} & UIDAI \end{array} \quad (3.14)$$

[A7:] ASP_i assumes that all valid cookies C_{R_i} are associated with a valid ongoing session from a unique valid user R_i already logged in to ASP_i portal.

$$ASP_i \models C_{R_i} \rightsquigarrow ID_{R_i} \quad \forall i = 1..n \quad (3.15)$$

[A8-A15:] R_i and ASP_i assumes that all nonce $n*_{R_i}$ (where $*$ is any integer used in the scheme) are fresh. Similar to this, other entities also make similar

assumptions. These assumptions are listed below.

$$\begin{aligned} R_i &\models \#n*_{R_i} \\ ASP_i &\models \#n*_{R_i} \\ ASP_i &\models \#n*_{ASP_i} \\ ESP_i &\models \#n*_{ASP_i} \\ ESP_i &\models \#n*_{ESP_i} \\ UIDAi &\models \#n*_{ESP_i} \\ UIDAI &\models \#n*_{UIDAI} \\ ESP_i &\models \#n*_{UIDAI} \end{aligned} \tag{3.16}$$

[A16:] It is assumed that when ASP_i receives communication message of the form $CommMsg(DataA_j, SignA_j)_{PB_{ASP_i}}$ from ESP_i, it has verified the validity of data, i.e., $\{SignA_j\}_{PB_{ESP_j}} = H(DataA_j)$. The same assumption is made for all entities receiving messages of this form.

Goals to be achieved.

Following are the goals which are envisaged to be achieved by the proposed model.

[G1-G6:] Sender entity must be sure that the data received by receiver entity is same as what was sent by it and is not modified, observed or replayed by an intruder after it was sent by the sender entity. Similarly, receiver entity must be sure that the data received by it is same as what was sent by sender entity and is not modified, observed or replayed by an intruder after it was sent by the sender entity.

$$\begin{aligned} ASP_i &\models R_i \overset{secure}{\longleftrightarrow} ASP_i \\ R_i &\models R_i \overset{secure}{\longleftrightarrow} ASP_i \\ ASP_i &\models ASP_i \overset{secure}{\longleftrightarrow} ESP_i \\ ESP_i &\models ASP_i \overset{secure}{\longleftrightarrow} ESP_i \\ ESP_i &\models ESP_i \overset{secure}{\longleftrightarrow} UIDAI \\ UIDAI &\models ESP_i \overset{secure}{\longleftrightarrow} UIDAI \end{aligned} \tag{3.17}$$

[G7:] Resident R_i must be sure that at the end what he receives is indeed a digital signature on message M_i, signed by resident's private key and generated by the genuine ESP_i.

$$R_i \models M_{ieSign} = M_{eSign\_R_i\_ESP_i\_CCA} \tag{3.18}$$

Idealization

BAN idealization of communication messages in communication phase is shown in tables 3.11 and 3.12.

Analysis

[P1-P6:] Using messages M1, M3 and rule R7, it can be deduced that ASP_i believes that communication from R_i to ASP_i is secure. Using messages M2, M8 and rule R11, it can be deduced that ASP_i believes that communication from ASP_i to R_i is secure. From these two deductions, it can further be deduced that ASP_i believes that communication between R_i and ASP_i is secure in both directions.

Using M1, M3, R7, R8,

$$ASP_i \models R_i \xrightarrow{\text{secure}} ASP_i \quad \text{(I1)}$$

Using M2, M8, R11,

$$ASP_i \models R_i \xleftarrow{\text{secure}} ASP_i \quad \text{(I2)}$$

Using I1 and I2,

$$ASP_i \models R_i \xleftrightarrow{\text{secure}} ASP_i \quad \text{(G1 : Proved)}$$

Using M1, M3, R10, R11

$$ASP_i \models R_i \xrightarrow{\text{secure}} ASP_i \quad \text{(I3)}$$

Using M2, M8, R8,

$$ASP_i \models R_i \xleftarrow{\text{secure}} ASP_i \quad \text{(I4)}$$

Using I3 and I4,

$$ASP_i \models R_i \xleftrightarrow{\text{secure}} ASP_i \quad \text{(G2 : Proved)}$$

Using M4, R7,

$$ESP_i \models ASP_i \xrightarrow{\text{secure}} ESP_i \quad \text{(I5)}$$

Using M7, R11,

$$ESP_i \models ASP_i \xleftarrow{\text{secure}} ESP_i \quad \text{(I6)}$$

Using I5 and I6,

$$ESP_i \models ASP_i \xleftrightarrow{\text{secure}} ESP_i \quad \text{(G3 : Proved)}$$

M1	ASP_i	$\lhd$	$\{login\ (\ ID_{R_i} \| PW_{R_i} \| PB_{B_i} \| n1_{R_i}, \{H(ID_{R_i} \| PW_{R_i} \| PB_{B_i} \| n1_{R_i})\}_{PR_{B_i}}\ )\}_{PB_{ASP_i}}$
M2	R_i	$\lhd$	$\{loginRes\ (\ C_{R_i} \oplus (n1_{R_i}+1) \{H(C_{R_i} \oplus (n1_{R_i}+1))\}_{PR_{ASP_i}}\ )\}_{PB_{B_i}}$
M3	ASP_i	$\lhd$	$\{signdocASPReq\ (\ M_i \| consent_{use\_ekyc} \| consent_{genuse\_at} \| C_{R_i} \| n2_{R_i}), \{H(M_i \| consent_{use\_ekyc} \| consent_{genuse\_at} \| C_{R_i} \| n2_{R_i})\}_{PR_{B_i}}\ )\}_{PB_{ASP_i}}$
M4	ESP_i	$\lhd$	$\{signdocESPReq\ (\ H(M_i) \| AadhaarNo_{R_i} \| ID_{ASP_i} \| License_{ASP_i} \| TID_{ASP_i} \| consent_{use\_ekyc} \| consent_{genuse\_at} \| n1_{ASP_i}, \{\ H(H(M_i) \| AadhaarNo_{R_i} \| ID_{ASP_i} \| License_{ASP_i} \| TID_{ASP_i} \| consent_{use\_ekyc} \| consent_{genuse\_at} \| n1_{ASP_i})\ \}_{PR_{ASP_i}}\ )\}_{PB_{ESP_i}}$
M5	UIDAI	$\lhd$	$\{kycESPReq\ (\ AT_{R_i} \| H(M_i) \| n1_{ESP_i}, \{H(AT_{R_i} \| H(M_i) \| n1_{ESP_i})\}_{PR_{ESP_i}}\ )\}_{PB_{UIDAI}}$
M6	ESP_i	$\lhd$	$\{kycESPRes\ (\ eKYC_{R_i} \| (n1_{ESP_i}+1) \{H(eKYC_{R_i} \| (n1_{ESP_i}+1))\}_{PR_{UIDAI}}\ )\}_{PB_{ESP_i}}$
M7	ASP_i	$\lhd$	$\{signdocESPRes\ (\ \{eKYC_{R_i} \| H(M_i)\}_{PR_{R_i}} \| PB_{R_i} \| \{PB_{R_i}\}_{PR_{ESP_i}} \| \{PB_{ESP_i}\}_{PR_{CCA}} \| TID_{ASP_i} \| (n1_{ASP_i}+1), \{H(eKYC_{R_i} \| H(M_i)\}_{PR_{R_i}} \| PB_{R_i} \| \{PB_{R_i}\}_{PR_{ESP_i}} \| \{PB_{ESP_i}\}_{PR_{CCA}} \| TID_{ASP_i} \| (n1_{ASP_i}+1))\}_{PR_{ESP_i}}\ )\}_{PB_{ASP_i}}$

Table 3.11: BAN Idealization of Proposed Protocol (Part I)

M8	R_i	$\lhd$	$\{$signdocASPRes ($M_i \| \{eKYC_{R_i} \| H(M_i)\}_{PR_{R_i}} \| PB_{R_i} \| \{PB_{R_i}\}_{PR_{ESP_i}} \| \{PB_{ESP_i}\}_{PR_{CCA}} \| (n2_{R_i}+1)$ $\{H(M_i \| \{eKYC_{R_i} \| H(M_i)\}_{PR_{R_i}} \| PB_{R_i} \| \{PB_{R_i}\}_{PR_{ESP_i}} \| \{PB_{ESP_i}\}_{PR_{CCA}} \| (n2_{R_i}+1))\}_{ASP_i}$) $\}_{PB_{B_i}}$

Table 3.12: BAN Idealization of Proposed Protocol (Part II)

Using M4, R11,

$ASP_i \models ASP_i \xrightarrow{\text{secure}} ESP_i$ (I7)

Using M7, R8,

$ASP_i \models ASP_i \xleftarrow{\text{secure}} ESP_i$ (I8)

Using I5 and I6,

$ASP_i \models ASP_i \xleftrightarrow{\text{secure}} ESP_i$ (G4 : Proved)

Using M5, R7,

$UIDAI \models ESP_i \xrightarrow{\text{secure}} UIDAI$ (I7)

Using M6, R11,

$UIDAI \models ESP_i \xleftarrow{\text{secure}} UIDAI$ (I8)

Using I7 and I8,

$UIDAI \models ESP_i \xleftrightarrow{\text{secure}} UIDAI$

(G5 : Proved)

Using M5, R11,

$ESP_i \models ESP_i \xrightarrow{\text{secure}} UIDAI$ (I9)

Using M6, R8,

$ESP_i \models ESP_i \xleftarrow{\text{secure}} UIDAI$ (I0)

Using I9 and I10,

$ESP_i \models ESP_i \xleftrightarrow{\text{secure}} UIDAI$ (G6 : Proved)

[P7:] Using message M9 and rule R13, it can be deduced that R_i believes that $\{M_i\}_{eSign}$ is a valid electronic signature.

Using M9 and R13,

$R_i \models \{M_i\}_{eSign} = \{M_i\}_{eSign\_R_i\_ESP_i\_CCA}$

(G7 : Proved)

3.7 Summary

This chapter introduced a mechanism to implement privacy enhanced eSign using digital access token which can include claims from ESP, UIDAI and resident. Resident can include privacy and fine-grained access control statements for access to resident's eKYC data. This token can be used by third entities to access the protected eKYC data with better privacy and fine-grained access control rules enforced by the resident. A formal security analysis of the proposed model using BAN logic is also presented. Although the proposed scheme helps prevent unauthorized access to eKYC data, the identity of the signer is revealed to the receiver, which may not be desired. The next chapter addresses some of these concerns.

Chapter 4

Privacy Enhanced eSign Scheme 2

In recent years, the Government of India has introduced many Aadhaar based online services. Although these initiatives helped India compete in digital revolution across world and are acclaimed by many, they have also raised some concerns about security especially the privacy aspects. One of the initiatives in this direction is eSign which provides an online electronic signature service to its subscribers. Although most of the security aspects are addressed by eSign, some of the privacy aspects are yet to be addressed. Previous chapter introduced a mechanism to prevent unauthorized access to eKYC data of the user. This is achieved by facilitating participating entities to encode privacy related claims in digital tokens. However, the identity of the signer is revealed to the receiver. Revealing identify of the signer has at least two limitations. First is that this identity may not serve the intended purpose since it does not indicate the authority or the role of the signer and the second is that the signer may not wish to reveal his personal information. This chapter addresses some of these concerns.

4.1 Introduction

Although eSign is an encouraging initiative, some limitations and challenges of the present model of eSign are listed below.

- Because of inherent limitations of PKI, eSign has certain limitations such as it attests an identity and not the possession of attributes, to a claim. This is one of the barrier in achieving privacy and yet able to authenticate.

- Another challenge is that the present model does not permit the signer to remain indistinguishable among the set of people in possession of the same attributes. This limitation prevents maintaining the privacy of the subscriber.

- One more limitation is the assurance level of subscriber's consent which in most of the cases is taken in an HTML form.

- Performance of eSign should also be kept within acceptable limits if it is to be used at nationwide level. The amortized performance of eSign can be improved using *digital access token* described later in this chapter.

- Some other concerns are how and where the privacy policies of the participating entities should be encoded? What will be the overall scheme? Will it be secure enough to meet necessary security requirements?

Recent developments in cryptography have introduced Attribute Based Signature (ABS) [94], in which the signature attests the possession of attributes (and not identity) to a claim. Although ABS can address the limitations cited above, it is not deployed widely and the right and efficient implementation is still a major concern. Some other concerns are the performance of bulk signatures, assurance level of subscriber's consent and the overall workflow describing roles of each participant.

This chapter presents a mechanism for participating entities to collaborate in generating an attribute based token which can be reused in eSign requests to prevent initial time spent in authenticating the subscriber and generating the access tree. Other than that, this chapter also presents the overall scheme to implement privacy enhanced eSign using attribute based token.

Rest of this chapter is organized in the following sections. Section 4.2 presents related work. Section 4.3 presents some of the preliminaries which are required to understand the scheme. Section 4.4 presents the proposed scheme. Section 4.4.6 presents the security analysis of the proposed scheme. Section 4.4.7 presents the performance analysis of the proposed scheme. Section 4.5 presents summary of the work.

4.2 Related Work

A major percentage of secure systems (such as eSign) till date are built using PKI introduced by Diffie and Hellman [95]. In PKI, each subscriber has a *descriptive information* and is associated with a private key and the corresponding public key. A trusted entity referred to as *Certifying Authority* (CA) issues a DSC which attests

the public key with subscriber's descriptive information. One major limitation of PKI is the overhead of management and distribution of DSCs.

Further developments in cryptography introduced Identity based Encryption (IBE), which was introduced as a concept by Shamir in 1984 [96] but was realized later by Boneh and Franklin in 2001 [97] using pairing-based cryptography and by Cock using quadratic residues in 2001 [98]. In IBE, each subscriber has an identity and is associated with a private key and the corresponding public key. A trusted entity referred to as *Public Key Generator* (PKG) generates a private key for the subscriber and gives it to him. The corresponding public key can be derived using the subscriber's identity. Some major benefits of IBE over PKI are that public key of the subscriber can be derived from the subscriber's identity without any overhead of certificate management.

Later developments in cryptography introduced Attribute based Encryption (ABE) which facilitates encryption based on a set of attributes. ABE is classified in two types, viz. a viz., Key Policy ABE (KP-ABE) and Ciphertext Policy ABE (CP-ABE). KP-ABE was introduced by Sahai and Waters [79] as an extension to the Identity based encryption and CP-ABE was introduced by Bethencourt et al [81]. These two schemes differ mainly on what is encoded (access policy or set of attributes) and where (in ciphertext or private key). In KP-ABE, the access policy is encoded in subscriber's private key and a set of attributes are encoded in the ciphertext. Only if the access policy encoded in receiver's private key satisfies the set of attributes encoded in received ciphertext will the receiver be able to decrypt the ciphertext. In CP-ABE, the access policy is encoded in each ciphertext and a set of attributes are encoded in the subscriber's private key. Only if the set of attributes encoded in receiver's private key satisfies the access policy encoded in received ciphertext, will the receiver be able to decrypt the ciphertext.

Attribute based Signature (ABS) is another related development in which a signer can sign a document with the proof of possession of certain attributes without revealing those attributes and his identity. Several researchers have worked on realizing the ABS scheme. Guo et al. [94] presented the ABS scheme which was proven using strong extended Diffie Hellman assumption. Later Tan [99] et al. presented that Guo's scheme is vulnerable to partial key replacement attack. Maji et al. [100] presented an ABS scheme which supported strong predicates containing AND, OR and threshold gates.

4.3 Preliminaries

This section briefly describes some of the necessary backgrounds.

4.3.1 Bilinear pairings

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are multiplicative cyclic elliptic groups of order p, g_1 is a generator of $\mathbb{G}_1$, g_2 is a generator of $\mathbb{G}_2$, $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$, then a bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ that satisfies the following three properties.

1 Bilinearity: $e(P^a, Q^b) = e(P, Q)^{ab}$

2 Non-Degeneracy: $e(g_1, g_2) \neq 1$

3 Computability: $e(P, Q)$ can be computed efficiently.

4.3.2 Decisional Bilinear Diffie Hellman (DBDH) assumption

Let $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of prime order $p > 2^\lambda$ where $\lambda \in \mathbb{N}$, g is the generator of $\mathbb{G}$, $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an efficiently computable symmetric bilinear pairing map and $a, b, c, z \in \mathbb{Z}_p$ are random integers. The DBDH assumption states that no probabilistic polynomial time algorithm can distinguish between $\langle g, g^a, g^b, g^c, e(g, g)^{abc} \rangle$ and $\langle g, g^a, g^b, g^c, e(g, g)^z \rangle$ with more than a negligible advantage.

4.3.3 Strong Extended Diffie Hellman (S-EDH) assumption

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ are cyclic groups of prime order $p > 2^\lambda$ where $\lambda \in \mathbb{N}$, g_1 is the generator of $\mathbb{G}_1$, g_2 is the generator of $\mathbb{G}_2$, $\mathbb{O}_{x,y}(.)$ is an oracle that takes as input $m \in \mathbb{Z}_p^*$ and outputs $\langle g_1^r, g_2^{1/(x+r)}, g_2^{1/(m+r), g_2^{yr}} \rangle$ for a random $r \in \mathbb{Z}_p^*$. For all probabilistic polynomial-time adversaries $\mathbb{A}$, all $v, c \in \mathbb{Z}_p^*$ and all $a \in \mathbb{G}_1$ such that $a \neq 1$, $\Pr\left[x \xleftarrow{R} \mathbb{Z}_p : \mathbb{A}^{O_{xy}}(g, g^x, g_2, g_2^y) = (m, a, a^x, a^r, g_2^{1/(x+r)}, g_2^{1/(m+r)}, g^{yr}) | m \notin Q\right] \prec 1/\text{poly}(k)$ where Q is the set of queries adversaries A make to oracle $\mathbb{O}_{x,y}(.)$.

4.3.4 Access structure

Access structure [101] is defined as follows. Let $P_1, P_2, ..., P_n$ be the set of parties. A collection $A \subseteq 2^{P_1, P_2, ..., P_n}$ is monotone if $B \in A$ and $B \subseteq C$ implies $C \in A$. An access structure is monotone collection A of non empty subsets of $\{P_1, P_2, .., P_n\}$ (that is, $A \subseteq 2^{P_1, P_2, ..., P_n} \setminus \{\phi\}$). The sets in A are called the authorized sets and the sets not

in A are called the unauthorized sets. Access policy is generally represented by a monotone access structure implemented as an access tree.

Let $\mathcal{T}$ be an access tree representing an access structure. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. If num_x is the number of children of a node x and $\text{k}_\text{x} = 1$, the threshold gate is an OR gate and when $\text{k}_\text{x} = \text{num}_\text{x}$, it is an AND gate. Each leaf node x of the tree is described by an attribute and a threshold value $\text{k}_\text{x} = 1$, it is an AND gate. Each leaf node x of the tree is described by an attribute and a threshold value $\text{k}_\text{x} = 1$. To facilitate working with the tree access structure, three functions are defined. Parent of the node x in the tree is denoted by parent(x). The function attr(x) in defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. The tree access structure $\mathcal{T}$ also defines an ordering between the children of every node, that, the children oaf a node are numbered from 1 to num. The function index(x) returns such a number associated with the node x. Where the index values are uniquely assigned to nodes in the access structure for a viven key in an arbitrary manner.

Let $\mathcal{T}_x$ denotes the subtree rooted at node x. If a set of attributes λ satisfies the subtree $\mathcal{T}_x$, it is represented as $\mathcal{T}_x(\lambda) = 1$. $\mathcal{T}_x(\lambda)$ is computed recursively as follows. If x is a non-leaf node, evaluate $\mathcal{T}(y)$ for all children nodes y of node x. $\mathcal{T}_x(\lambda)$ returns 1 if and only if at least k_x children return 1. If x is a leaf node, then $\mathcal{T}_x(\lambda)$ returns 1 if and only if $\text{attr(x)} \in \lambda$.

4.4 Proposed model of privacy enhanced eSign

This section presents the proposed scheme of privacy enhanced token based eSign using attribute based signature.

4.4.1 Attribute Authority

An attribute can be any characteristic of a subscriber and is represented by a private key (an integer) and a corresponding public key (a point on the group). Two new entities are proposed to be introduced, namely, *Attribute Authority Manager* (AAM) and *Attribute Authority* (AA). AAM manages the universe of attributes and AA manages a set of attributes assigned to him by AAM. The scheme consists of a single AAM and multiple AAs. UIDAI can assume the role of the AAM and individual agencies such as ESP, RTO, etc. can assume the role of AAs. Each subscriber also

assumes the role of an AA since it also manages a small set of attributes representing his consent, purpose for which signature is taken, consumer of signature, etc.

When UIDAI starts as AAM, it executes setup(k) procedure, where k is a security parameter. In this procedure, UIDAI chose two cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of large prime order p on which discrete logarithm problem is assumed to be hard, a generator g_1 of $\mathbb{G}_1$, a generator g_2 of $\mathbb{G}_2$, a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ for which bilinear Diffie Hellman problem is assumed to be hard. Security parameter k defines the size of chosen groups. Now, AAM defines universe of attributes $\mathbb{U} = \{1, 2, ...n\}$ and designate specific subset for specific AAs such as attributes $\{001 - 100\}$ for itself, $\{101 - 200\}$ for ESPs, $\{201 - 225\}$ for subscribers, etc. These attributes are represented by $\mathbb{A}_A$, $\mathbb{A}_E$, and $\mathbb{A}_U$ respectively. Subscriber is given an ownership of only few of the attributes which facilitates him provide his consent, designate consumer of the signature, designate purpose for which the signature is taken, etc.

Now, to define a private key for itself (SK), the corresponding public key (PK) and a master public key (MPK), AAM chose a random number $\gamma \in_R \mathbb{Z}_p$, random numbers $t_i \in_r \mathbb{Z}_p$ for each attribute $i \in \mathbb{A}_A$ and defines them as below.

$$\begin{aligned} SK &= \{\gamma, \{t_i\}_{\forall i \in \mathbb{A}_A}\} \\ PK &= \{g^\gamma, \{T_i, \{T_i\}_{PVTA}\}_{\forall i \in \mathbb{A}_A}\} \\ MPK &= \{\mathbb{A}_U, \mathbb{A}_E, \mathbb{A}_A, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, p\} \end{aligned} \tag{4.1}$$

where $T_i = g^{t_i}$ and $\{T_i\}_{PVTA}$ is T_i signed by another private key PVTA of AAM.

Before subscribing as an AA, each subscriber is assumed to have a secure device such as a smart card or a mobile having Trusted Execution Environment (TEE) which already has MPK in it and is capable of establishing a secure communication channel between itself and UIDAI. When a subscriber (or an agency) wants to register itself as an AA, it calls RegisterAsAA() API of UIDAI. UIDAI authenticates the requester using his Aadhaar number (or requester id) and requests him to provide public keys for subscriber (or AA_i) specific attributes. Requester generates a random number $\alpha \in_R \mathbb{Z}_p$, random numbers $r_i \in_R \mathbb{Z}_p$ for each attribute $i \in \mathbb{A}_U$ (or $i \in \mathbb{A}_i$), generates public key $T_i = g^{t_i}$ for each of them and sends them to UIDAI. UIDAI digitally signs α and each of T_i and sends $\{g^\alpha\}_{PVTA}, \{T_i\}_{PVTA}$ $\forall i \in \mathbb{A}_U$ back to the subscriber (or AA). Subscriber (or AA_i)now has the private key $AASK_i$ and public key $AAPK_i$ as below.

$$\begin{aligned} AASK_i &= \{\alpha, \{t_i\}_{\forall i \in \mathbb{A}_U}\} \\ AAPK_i &= \{g^\alpha, \{g^\alpha\}_{PVTAA}, \{T_i, \{T_i\}_{PVTAA}\}_{\forall i \in \mathbb{A}_U}\} \end{aligned} \tag{4.2}$$

Requester (or AA_i) securely stores secret key USK in his secure device (or server).

4.4.2 Key Generation

An *Attribute based Private Key* (ABPvK) can be generated for a subscriber based on his associated attributes and an access tree. Since a subscriber can be associated with attributes from different AAs such as RTO, University, etc, an access tree can have access subtrees from different AAs. An example of access tree $\mathcal{T}$ comprising of three access subtrees $\mathcal{T}_S$, $\mathcal{T}_E$ and $\mathcal{T}_A$ is illustrated in figure 7.1. All attributes from single AA are assumed to be in one access subtree and only ESP is assumed to have permission to request ABPvK on behalf of subscriber.

Each *Attribute based Token* (ABT) is identified by a tuple $IDT_{ij} = \langle ID_i, \mathcal{T}_j \rangle$ where ID_i is subscriber's identifier and $\mathcal{T}_j$ is the access tree against which ABT is to be generated. Let $K \in \mathbb{G}_1$ and $r \in_R \mathbb{Z}_p$. Presence of some helper functions is assumed such as $GetAA(\mathcal{T})$ returns set of AAs whose attributes are present in $\mathcal{T}$, $L((T)) = leaves(T) \cap \mathbb{A}$, where $\mathbb{A}$ is the set of attributes manged by AA calling the function, $AASK(\mathcal{T})$ returns first component from all $AASK_i$ of all $AA_i \in GetAA(\mathcal{T})$.

A helper procedure $genParitalKey(IDT_{ij}, K, r)$ is proposed to be introduced which works as follows. AA prepares a set λ of attributes associated with ID_i. A polynomial q_x is chosen for each node x (including the leaves) in access tree $\mathcal{T}_j$. The nodes in the tree are chosen in a top-down manner, starting from the root node R. For each node x, degree d_x of the polynomial q_x is set to one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$. Now, for the root node R, set $q_R(0) = r$ and chose d other points randomly to define the polynomial q(x) completely. For any other node x, set $q_x(0) = q_{parent(x)}(index(x))$ and chose d_x other points randomly to completely define q_x. Once the polynomials are decided, for each leaf node x, set the secret value $D_x = K^{q_x(0)/t_i}$ where $i = att(x)$ and $x \in \lambda$.

One API $PullKey(IDT_{ij}, K)$ is proposed to be introduced by AA which is consumed by UIDAI and returns ABPvK. Second API $PullKeyAll(IDT_{ij}, K)$ is proposed to be introduced by UIDAI which is consumed by ESP and returns ABPvK from all participating AAs. Refer algorithms 4.1 and 4.2.

4.4.3 Token Generation

Since for bulk signatures, generation of ABPvK every time may be inefficient, an ABT is proposed to be introduced which contains ABPvK and associated token usage claims (such as expiry date) from all $AA \in GetAA(\mathcal{T})$. The ABT can be reused (till it expires) for every eSign request from the subscriber if those requests

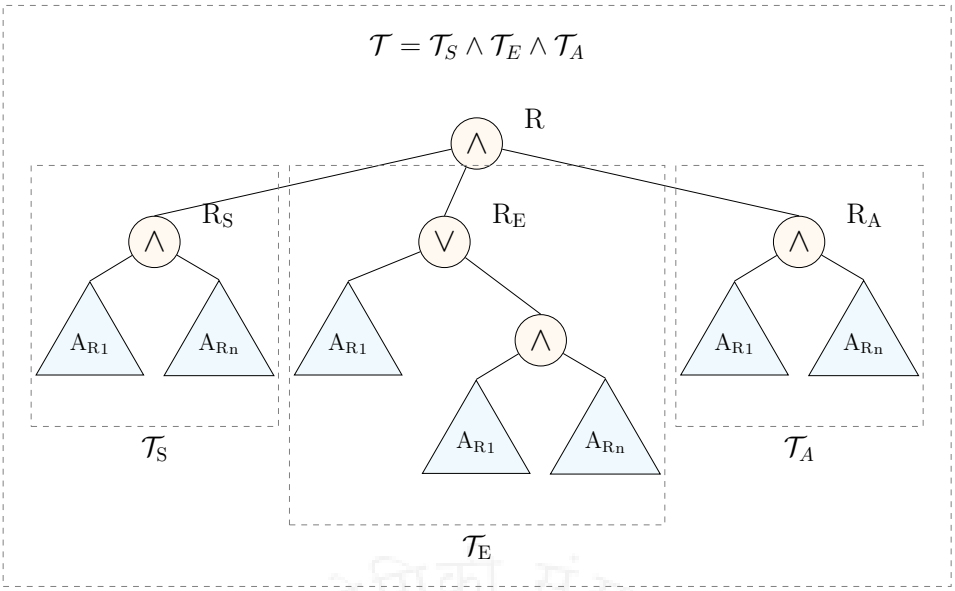


Figure 4.1: Example of an access policy tree

are against the same access tree.

To generate an ABT, all AA $\in$ GetAA($\mathcal{T}$) collaborate to arrive at a common group element K $\in \mathbb{G}_1$. For this, two APIs are proposed to be introduced by all AAs (including ESP), PullK(IDT_{ij}, K) to pull an updated value of K and PushK(IDT_{ij}, K) to let AA store updated value of K against IDT_{ij}. These APIs are consumed by UIDAI. One API GenTokPullAllK(IDT_{ij}, K) is proposed to be introduced by UIDAI in which it facilitates arriving at a common group element K. This API is consumed by ESP. One API GenTok(IDT_{ij}, K) is proposed to be introduced by ESP which is consumed by subscriber. Subscriber initiates this process by invoking its own procedure genTok(IDT_{ij}). Refer algorithms [4.3 - 4.7]. As seen in algorithm 4.6, ESP has created token ABT_{ij} which it keeps securely.

$$\text{ABT}_{ij} = \begin{cases} \text{IDT}_{ij} & = \text{ID}_i, \mathcal{T}_j \\ D_1 & = \bigcup_{\forall k} D_k \quad | \ \text{AA}_k \in \text{GetAA}(\mathcal{T}_j) \\ D_2 & = K^{\alpha}, K^{\beta}, K^{\gamma}, .. \mid \{\alpha, \beta, \gamma, ..\} \in \text{AASK}(\mathcal{T}_j) \end{cases} \tag{4.3}$$

4.4.4 eSign using token

A new version of eSign API eSign(ID_i, $\mathcal{T}_j$, H(m)) is proposed to be introduced by ESP where H(m) is one way secure hash of message to be signed. When ESP receives this request, it generates a random number $r_4 \in_R \mathbb{Z}_p$ and computes the signature σ

as below. The signature is then given back to the subscriber.

$$\sigma_{ij} = \left\{ \begin{array}{l} A = g^{r_4} \\ C = g^{\frac{1}{r_4 + H(m)}} \\ D = \{K^{\alpha}\}^{r_4} \cdot \{K^{\beta}\}^{r_4} \cdot \{K^{\gamma}\}^{r_4} \ldots \\ \quad = g^{r_4(\prod_{\forall k} r_k)(\sum_{\forall k} AASK_k)} \\ E_i = {D_k}^{r_4} = g^{r_4(\prod_{\forall k} r_k)(\frac{q_x(0)}{t_i})} \end{array} \right\} \mid AA_k \in \text{GetAA}(\mathcal{T}) \tag{4.4}$$

4.4.5 eSign Verification

To verify an eSigned document, an offline procedure Verify(M, σ, MPK) is proposed to be introduced. A recursive helper procedure VerN(T_i, E_i, i) is defined. For each leaf node x in $\mathcal{T}$, the helper procedure takes, three parameters, public key of the attribute, corresponding private key component from signature and i = attr(x). This is defined as below.

$$\text{VerN}(T_i, E_i, x) = \begin{cases} e(T_x, E_x) & \text{if } i \in \gamma \\ \perp & \text{otherwise} \end{cases} \tag{4.5}$$

For each non-leaf node x in access tree $\mathcal{T}$, the procedure is defined as follows. For all nodes z that are children of x, it calls VerN(T_z, E_z, z) and stores the output as F_z. Let S_x be an arbitrary $k_x -$ sized set of child nodes z such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$. Otherwise, F_x is computed as below.

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)} \qquad \text{where}\{i = \text{index}(z) \\ &\qquad\qquad S_x' = \{\text{index}(z) : z \in S_x\} \\ &= \prod_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)} \\ &= \prod_{z \in S_x} (e(g,g)^{r r_4 q_z(0)})^{\Delta_{i,S_x'}(0)} \\ &= \prod_{z \in S_x} (e(g,g)^{r r_4 q_{\text{parent}(z)}(\text{index}(z))})^{\Delta_{i,S_x'}(0)} \\ &= \prod_{z \in S_x} e(g,g)^{r r_4 q_x(i) \Delta_{i,S_x'}(0)} \\ &= e(g,g)^{r r_4 q_x(0)} \text{ using polynomial interpolation} \end{aligned} \tag{4.6}$$

It can be deduced that for the root node R, if the signature satisfies the access tree $\mathcal{T}_R$, VerN(E_R, T_R, R) returns $e(g,g)^{r_4(\prod_{\forall k} r_k)(\Sigma_{\forall k} AASK_k)}$.

Algorithm 4.1 AA : PullKey

Require: $\langle IDT_{ij}, K \rangle$
  $r \in_R \mathbb{Z}_p$
  $\langle D_1, D_2 \rangle \leftarrow$ genParitalKey(IDT_{ij}, K, α)
    $D_1 = K^{q_x(0)/t_i} \quad \forall i \in L(IDT_{ij} \rightarrow T)$
    $D_2 = K^{\alpha}$
  return $\langle D_1, D_2 \rangle$

Algorithm 4.2 UIDAI : PullKeyAll

Require: $\langle IDT_{ij}, K \rangle$
  $D_1 = D_2 = \phi$
  $AA \leftarrow$ GetAA$(IDT_{ij} \rightarrow T)$
  while AA $\neq$ empty **do**
    $AA_i \leftarrow$ DEQUEUE(AA)
    Call API of AA_i API :
      $\langle D_1', D_2' \rangle \leftarrow$ PullKey(IDT_{ij}, K)
    $D_1 = D \cup D_1'$
    $D_2 = D, D_2'$
  end while
  return $\langle D_1, D_2 \rangle$

Algorithm 4.3 AA : PullK

Require: $\langle IDT_{ij}, K \rangle$
  $r \in_R \mathbb{Z}_p$
  Store mapping : $IDT_{ij} \leftrightarrow r$
  return K^r

Algorithm 4.4 AA : PushK

Require: $\langle IDT_{ij}, K \rangle$
  $r \in_R \mathbb{Z}_p$
  Update mapping : $IDT_{ij} \leftrightarrow K$
  return

Algorithm 4.5 UIDAI : GenTokPullAllK

Require: $\langle IDT_{ij}, K \rangle$
  $AA \leftarrow$ GetAA$(IDT_{ij} \rightarrow T)$
  while AA $\neq$ empty **do**
    $AA_i \leftarrow$ DEQUEUE(AA)
    Call AA_i API : $K \leftarrow$ PullK(IDT_{ij}, K)
  end while
  $AA \leftarrow$ GetAA$(IDT_{ij} \rightarrow T)$
  while AA $\neq$ empty **do**
    $AA_i \leftarrow$ DEQUEUE(AA)
    Call AA_i API : PushK(IDT_{ij}, K)
  end while
  return K

Algorithm 4.6 ESP : GenTok

Require: $\langle IDT_{ij}, K \rangle$
  $r \in_R \mathbb{Z}_p$
  $K \leftarrow K^r$
  $K \leftarrow$ UIDAI : GenTokPullAllK(IDT_{ij}, K)
  Store mapping : $IDT_{ij} \leftrightarrow K$
  $\langle D_1, D_2 \rangle \leftarrow$ UIDAI : PullKeyAll(IDT_{ij}, K)
  $IDT_{ij} =$
    $ID_{ij} : ID_i, \mathcal{T}_j$
    $D_1 : D_U \cup D_{AA_1} \cup D_{AA_2} \cup ...$
    $D_2 : K^{\alpha}, K^{\beta}, K^{\gamma}, ...$
  return

Algorithm 4.7 Subscriber : genTok

Require: $\langle IDT_{ij} \rangle$
  $r \in_R \mathbb{Z}_p$
  $K \leftarrow g^r$
  $K \leftarrow$ ESP : GenTok$(IDT_{ij}, K, \mathcal{T})$
  Store mapping : $IDT_{ij} \leftrightarrow K$
  return

Now, the signature verifier verifies following equalities.

$$\begin{aligned} e(g, D) &\stackrel{?}{=} F_R \\ e(g^m.A, C) &\stackrel{?}{=} e(g, g) \end{aligned} \tag{4.7}$$

Only if these equalities hold true, the verifier accepts the signature.

4.4.6 Security Analysis

This section presents the security analysis of the proposed scheme based on intuitive reasoning. To keep the focus on the objective of this chapter, it is assumed that the communication channel between different entities is secure and before communicating any message, both entities authenticate each other. This will ensure confidentiality, data integrity and mutual authentication.

The signed document and the signature on it do not reveal any information about the identity of the user. The signature is done using attributes of the user and does not include the identity of the user. The signature verifier also does not need to know the identity of the user to verify the signature. Hence, the privacy of the user is maintained.

The proposed scheme is existentially unforgeable under chosen-message attack under the strong extended Diffie Hellman assumption. This is true since it is not the case, and the scheme is forgeable with a non-negligible probability ϵ, then the strong extended Diffie Hellman assumption can also be broken with the same non-negligible probability ϵ. Moreover, since the user's key is never given to the user himself and ESP is a trusted entity, partial key replacement attack will not be possible.

Our goal is to show that for every adversary $\mathcal{A}$ and environment $\mathcal{Z}$, there exists a simulator $\mathcal{S}$ such that $\mathcal{Z}$ cannot distinguish whether it is interacting in the real world with $\mathcal{A}$ or the ideal world with $\mathcal{S}$. $\mathcal{S}$ is given a black-box access to $\mathcal{A}$. In our description, $\mathcal{S}$ will use $\mathcal{A}$ to simulate conversations with $\mathcal{Z}$. Specifically, $\mathcal{S}$ will

directly forward all messages from $\mathcal{A}$ to $\mathcal{Z}$ and from $\mathcal{Z}$ to $\mathcal{A}$.

Adversary $\mathcal{A}$ produces signature σ and message m such that verification succeeds and yet simulator $\mathcal{S}$ never gave $\mathcal{A}$ this user's signature on m. This scenario occurs with only negligible probability under the EDH assumption.

Recall that EDH takes as input $(g, g^x, \bar{g}, \bar{g}^x)$ together with access to oracle $O_x(.)$ that takes input $c \in \mathbb{Z}^*$ and produces output $(g^x, \bar{g}^{\frac{1}{x+v}}, \bar{g}^{\frac{1}{v+c}})$ for any $v, \in_R \mathbb{Z}^*{}_p$. The goal is to produce a tuple $(c, a, a^v, \bar{g}^{\frac{1}{x+v}}, \bar{g}^{\frac{1}{v+c}})$ for any $a \in \mathbb{G}_1$ and any $v, c \in \mathbb{Z}^*$ such that c was not queried to the oracle. When adversary $\mathcal{A}$ succeeds with probability ϵ, then $\mathcal{S}$ solves the EDH problem with probability ϵ. $\mathcal{S}$ proceeds as follows.

- **Setup**: $\mathcal{S}$ establishes the global parameters and the key generation.

  [a] Setup public parameters such as $(g, \bar{g})$.

  [b] Guess which honest user $\mathcal{A}$ will attack. Give this user, the public key $pk^* = (g, \bar{g}, g^x, \bar{g}^x, g^r, g^{t_1}, g^{t_2}, ..., g^{t_u}, g^c)$, for random $r \in_R \mathbb{Z}_p$. (Logically this assigns user, the secret key, $sk^* = (t_1, t_2, ..., t_u, c)$).

- **Signing:** When $\mathcal{A}$ is asked for a signature on $m \in \mathbb{Z}_p^*$ from the honest user associated with secret key sk^*:

  [a] Query oracle $O_x(m)$ to get output $(g^v, \bar{g}^{\frac{1}{x+v}}, \bar{g}^{\frac{1}{c+v}})$.

  [b] $\mathcal{A}$ responds with signature $S = g^r, \bar{g}^{\frac{1}{y+r}}, \bar{g}^{\frac{1}{m+r}}, \bar{g}^{wr}, \{\bar{g}^{(r\frac{q_x(0)}{t_i})}\}_{\forall i \in \gamma}$

- **Verification**: $\mathcal{S}$ verifies the sinagure produced by $\mathcal{A}$

- **Output**: Suppose $\mathcal{A}$ produces a valid signature σ' for a new message $m' \in \mathbb{Z}_p^*$ for the user with key sk^*. Then $\mathcal{S}$ outputs (m', σ) to solve the EDH problem.

It is easy to observe that $\mathcal{S}$ perfectly simulates the signature world for $\mathcal{A}$. When $\mathcal{A}$ succeeds with probability ϵ, then $\mathcal{S}$ solves the EDH problem with probability ϵ. Hence, the proposed scheme is existentially unforgeable under chosen-message attack

under the strong extended Diffie Hellman assumption.

4.4.7 Performance Analysis

This section presents the performance analysis of the proposed scheme. However, since the present model of eSign is based on PKI, the results of this analysis cannot be compared directly with the present model of eSign. This section assumes the presence of two procedures, viz. a viz., L($\mathcal{T}$) and NL($\mathcal{T}$) which returns the set of leaves and non-leaves in access tree $\mathcal{T}$. Table 7.1 depicts various costs of each phase (in terms of the number of operations) for each participating entity. Three columns of this table indicate the number of signing operations, exponent operations and the pairing operations.

The major procedures in this scheme are setup(), userRegistrationAA(ID_{U_i}), esp RegistrationAA(), tokenGeneration(), eSign(H(m), $\mathcal{T}$) and eVerification(σ, H(m)). For analysis, we will consider two helper procedures, genPartialKey() and mutually ArriveAtK(). The setup procedure is executed by attribute authority at the very beginning to set up its private key ASK, the corresponding public key APK and the master public key MPK. ASK consists of a set of integers chosen for attributes in $\mathbb{A}_A$. In APK, corresponding public key for each attribute is arrived by raising g to the power of the respective private chosen integer. In addition to this, the APK component is also arrived by raising g to the power of secret random number γ. Hence, this procedure involves $|\mathbb{A}_A| + 1$ exponentiation and $|\mathbb{A}_A|$ signatures by attribute authority.

In user registration procedure, g^{α} involves one exponentiation and user attribute based public key UPK is arrived by raising g the corresponding components in USK. This involves $(\mathbb{A}_{U_i} + 1)$ exponentiations, $(\mathbb{A}_{U_i} + 1)$ signatures by attribute authority and 1 Aadhaar based authentication. ESP registration procedure is also similar to user registration procedure and will involve $(\mathbb{A}_{E_i} + 1)$ exponentiation, $(\mathbb{A}_{E_i} + 1)$ signatures by attribute authority and 1 authentication. In helper func-

		Signing	Exponent	Pairing
Setup	User			
	ESP			
	AA	$\|\mathcal{A}_{\mathrm{A}}\|+1$	$\|\mathcal{A}_{\mathrm{A}}\|+1$	
User/ESP Registration	User	$\|\mathcal{A}_{\mathrm{U_i}}\|+1$	$\|\mathcal{A}_{\mathrm{U_i}}\|+1$	
	ESP	$\|\mathcal{A}_{\mathrm{E_i}}\|+1$	$\|\mathcal{A}_{\mathrm{E_i}}\|+1$	
	AA			
Token Generation	User		$\|\mathrm{L}(\mathcal{T}_{\mathrm{U_i}})\|+2$	
	ESP	1	$\|\mathrm{L}(\mathcal{T}_{\mathrm{E_i}})\|+2$	
	AA	1	$\|\mathrm{L}(\mathcal{T}_{\mathrm{A}})\|+2$	
eSign	User			
	ESP		$\|\mathrm{L}(\mathcal{T})\|+5$	
	AA			
eSign Verification	User		$\|\mathrm{NL}(\mathcal{T})\|$	$\|\mathrm{L}(\mathcal{T})\|+2$
	ESP			
	AA			

Table 4.1: Cryptographic cost

tion genKey($\mathcal{T}_{\mathrm{i}}, \mathrm{ID}, \mathrm{K}$), a polynomial is created for every node (including the leaf nodes) and for each leaf node representing an attribute, K is raised to the power of $\mathrm{q_x}(0)/\mathrm{t_i}$. Ignoring the polynomial creation cost, this will involve $|\mathrm{L}(\mathcal{T}_{\mathrm{i}}\mathrm{i})|$ exponentiation. In helper procedure mutuallyArriveAtK(), K, K_α, K_β and K_γ are arrived by using 6 exponentiation. Procedure genToken() involves three invocations of genKey($\mathcal{T}_{\mathrm{i}}, \mathrm{ID}, \mathrm{K}$) for $\mathcal{T}_{\mathrm{U_i}}$, $\mathcal{T}_{\mathrm{E_i}}$ and $\mathcal{T}_{\mathrm{A}}$ which will involve $|\mathrm{L}(\mathcal{T})|$ exponentiation, one mutuallyArriveAtK() invocation, which will involve 6 exponentiation. Other than that, σ_{E_i} and σ_A contributes two signatures, one by $\mathrm{E_i}$ and one by AA.

In procedure, eSign($\mathcal{T}_{\mathrm{q}}, \mathrm{H(m)}$), D is computed using 3 exponentiation, A is computed using 1 exponentiation, C is computed using 1 exponentiation and 1 hash and $\mathrm{E_i}$ is computed using $|\mathrm{L}(\mathcal{T})|$ exponentiation. This involves a total of $|\mathrm{L}(\mathcal{T})|+5$ exponentiation and 1 hash. In eSignVerification() procedure, for each leaf node of $\mathcal{T}$, a paring is computed, for each internal node of $\mathcal{T}$ the values obtained from child are raised to lagrange's coefficient and then multiplied. Further to this, 2 pairings are computed for final verification. This involves $|\mathrm{L}(\mathcal{T})|+2$ pairings and $|\mathrm{NL}(\mathcal{T})|$ exponentiation. Table 7.1 depicts the cryptographic cost of various entities in various phases with respect to signing, exponent and pairing operations.

Setup, UserRegistration and ESPRegistraion are one-time operations. Based on regulatory guidelines, ESP can keep the token and if possible, reuse the same later for multiple eSign requests. For bulk eSign operations TokenGeneration is also a one time operation. The recurring cost is only for eSign which is $|(\mathrm{L}(\mathcal{T}))| + 5$ exponents and which is born by ESP. Thus, the amortized cost of eSign grows linear to the number of attributes in terms of exponents.

$$\mathrm{AmortizedCost}_{\mathrm{eSign}} = \mathcal{O}(\mathrm{L(T)})\mathrm{Cost}_{\mathrm{exponent}} \tag{4.8}$$

4.5 Summary

In the traditional eSign model, the identity of the signer is revealed to the receiver, which may neither be sufficient nor be required. This chapter introduced a mechanism to implement privacy-enhanced eSign in which the identity of the signer is not revealed to the receiver. The receiver, on the other hand, is assured that the signer holds the required set of attributes. The next chapter explores privacy improvement in another Aadhaar-based service, named, DigiLocker.

This page intentionally left blank.

Chapter 5

Privacy Enhanced DigiLocker

Previous two chapters introduced mechanisms to improve privacy in Aadhaar-based eSign service. This chapter explores privacy related improvements in another Aadhaar -based service, namely, DigiLocker, which provides shareable private storage space on public cloud to its subscribers. Although DigiLocker ensures traditional security such as data integrity and secure data access, the privacy of e-documents is yet to be addressed. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) can improve data privacy but the right implementation of it has always been a challenge. This chapter presents a scheme to implement privacy enhanced DigiLocker using CP-ABE.

5.1 Introduction

In last decade, Government of India has taken several e-Governance initiatives such as a unique digital identity (referred to as Aadhaar [102]) for every resident, online Aadhaar based authentication and several online citizen-centric services such as eKYC, eSign, and DigiLocker. At present, most of these services are built using traditional Public Key Infrastructure (PKI) with limited data privacy in which specifying authorized entities beforehand which are permitted to access data may

not be possible and even if possible, the solution may not scale.

In DigiLocker [89], documents of subscribers are hosted on public cloud which is assumed to be a trusted entity. However, cloud storage may not be trustworthy and may be susceptible to insider attacks. Moreover, instead of providing a *reactive access authorization to a single requester*, a subscriber may want to provide a *proactive access authorization to multiple requesters* meeting certain criteria of attributes.

5.2 Related Work

Recent developments in cryptography have introduced Attribute-Based Encryption (ABE) [79] in which encryption is done under a set of attributes. ABE is classified in Key-Policy ABE (KP-ABE) [79] and CP-ABE. In KP-ABE, the access policy is encoded in the subscriber's private key and a set of attributes are encoded in the ciphertext. In CP-ABE, the access policy is encoded in the ciphertext and a set of attributes are encoded in the subscriber's private key. In CP-ABE, only if the set of required attributes encoded in receiver's private key satisfies the access policy encoded in received ciphertext, the receiver is able to decrypt the ciphertext. Since the introduction of CP-ABE, researchers have proposed innovative mechanisms to use it to improve data privacy [103], [104].

5.3 Present model of DigiLocker in India

DigiLocker is an Aadhaar based online service which facilitates *subscribers* to store e-documents, *issuer* agencies to provide e-documents and *requester* applications to get access to e-documents. An *e-document* is a digitally signed electronic document. *Repositories* are provided by issuers to host collection of e-documents. *Digital Locker* is a storage space provided to each subscriber to store e-documents. *Requester* is an application which seeks access to some e-document. All participating entities must

adhere to *Digital Locker Technology Specification (DLTS)* [105].

An e-document is uniquely identified by a *Unique Resource Identifier (URI)* which is a triplet of the form ⟨IssuerID :: DocType :: DocID⟩, where $IssuerID$ is a unique identifier of the issuer, e.g., CBSE, for Central Board of Secondary Education. *DocType* is a classification of e-documents as defined by the issuer. For example, CBSE may classify certificates into MSTN for 10th mark sheet and KVYP for certificates issued to KVPY scholarship fellow. *DocType* also helps issuers to use different repositories for different types of e-documents. $DocID$ is an issuer defined unique identifier (an alphanumeric string) of the e-document within a document type. Some hypothetical examples of e-document URI are ⟨CBSE :: MSTN :: 22636726⟩, ⟨DLSSB :: HSMS :: GJSGEJXS⟩. DigiLocker ensures data integrity of e-documents by mandating that all e-documents are digitally signed by issuers.

When an issuer is registered, it provides two APIs, namely, PullDoc to pull an e-document based on a given URI and PullUri to pull all URIs meeting a given search criteria. When a requester application is registered, it is given a unique requester identifier, a secret key which is shared between DigiLocker and requester application and a FetchDoc API is given to access e-documents based on URI. Based on the URI, FetchDoc forwards the request to appropriate issuers to retrieve the e-document. DigiLocker ensures secure data access of e-documents by API license keys, secure transport, an explicit authentication (if required by *DocType*) and all requests and responses to be digitally signed.

5.4 Security Model

The security model of the proposed scheme is based on the following IND-sAtt-CPA game [106] between a challenger and an adversary $\mathcal{A}$.

Init Phase: Adversary $\mathcal{A}$ chooses a challenge access tree $\mathcal{T}^*$ and gives it to the challenger.

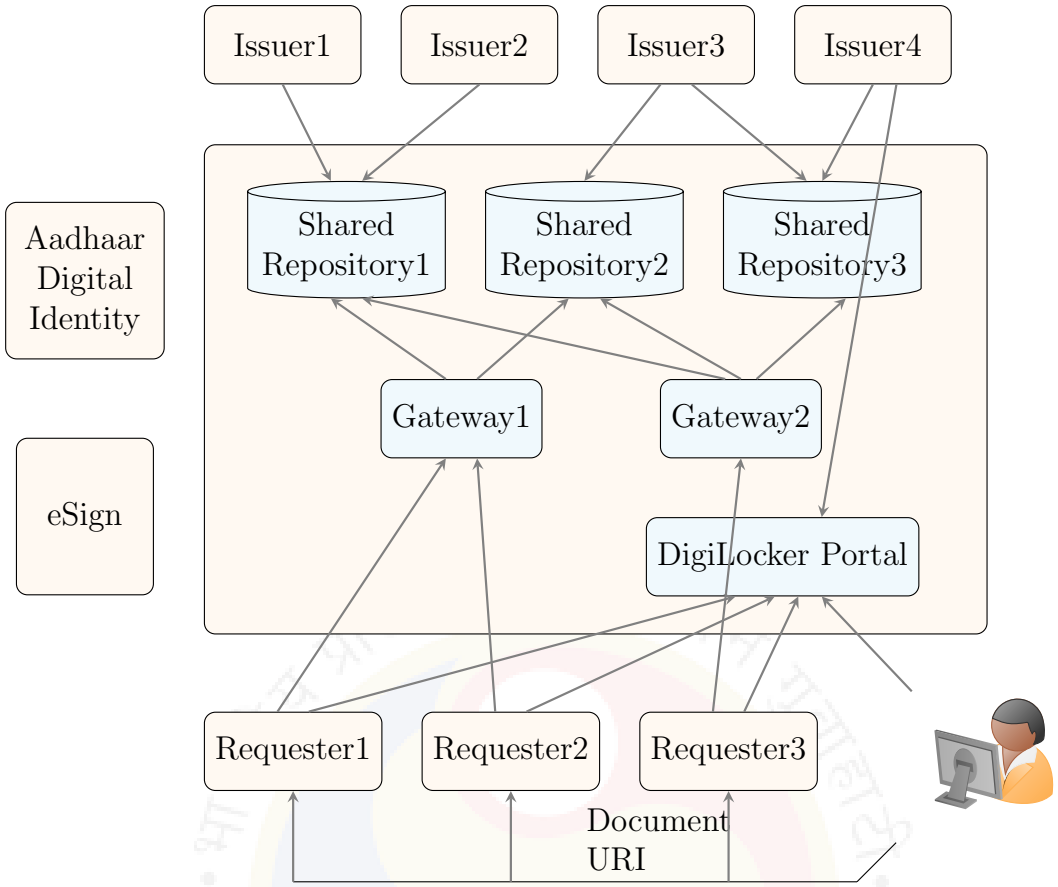


Figure 5.1: Present model of DigiLocker

Setup Phase: Challenger runs a *setup* procedure to generate $\langle \text{ASK}, \text{APK} \rangle$ and gives the public key APK to adversary $\mathcal{A}$.

Phase I: Adversary $\mathcal{A}$ makes an attribute-based private key request to the key generation oracle for any attribute set with the restriction that the attribute set should not include any attribute which is part of $\mathcal{T}^*$. Challenger generates the key as described in section 5.5.4 and returns the same to adversary $\mathcal{A}$.

Challenge Phase: Adversary $\mathcal{A}$ sends two equal length messages m_0 and m_1 to challenger. Challenger chooses a random number $b \in_R \{0, 1\}$, encrypts m_b using $\mathcal{T}^*$ and APK as is described in section 5.5.3.

Phase II: Adversary $\mathcal{A}$ can send multiple requests to generate an attribute-based private key with the same restriction as in Phase I.

Guess Phase: Adversary $\mathcal{A}$ outputs a guess $b\prime \in \{0, 1\}$.

The advantage of adversary $\mathcal{A}$ in this game is defined to be $\epsilon = |\Pr[b\prime = b] - \frac{1}{2}|$. Only if any polynomial time adversary $\mathcal{A}$ has a negligible advantage, the scheme is considered secure against an adaptive chosen plaintext attack (CPA).

5.5 Proposed model of privacy enhanced DigiLocker

The proposed scheme introduces two new roles, namely, *Attribute Authority Manager* (AAM) and *Attribute Authority* (AA). AAM is an entity which manages the universe of attributes and AA is an entity which manages a set of attributes (as assigned by AAM). DigiLocker is proposed to assume the role of AAM and individual issuers are proposed to assume the role of AA. A subscriber is assigned a set of attributes from each issuer which holds at least one e-document of the subscriber. Each requester application is assigned a set of attributes from DigiLocker based on certain criteria such as the purpose of access, for how long the data is going to be used, etc. To create a privacy enhanced e-document for a subscriber, issuer and subscriber mutually creates an attribute-based token (which will be used later in encryption) for an access policy, generates a symmetric key, encrypts the document with the symmetric key, encrypts the symmetric key with the attribute-based token, creates an e-document enclosing both the encrypted symmetric key and the encrypted document, creates a URI for this e-document and pushes it to subscriber's digital locker using PushURI API. When this e-document is shared with a requester application, the requester will be able to decrypt the encrypted symmetric key only if the requester is associated with a set of attributes which satisfies the access policy used to encrypt the symmetric key. Only when the requester obtains the symmetric key, he is able to decrypt and retrieve the document.

In *Setup(κ)* procedure, AAM chose a cyclic group $\mathbb{G}_0$ of large prime order p (κ defines the size of group) on which discrete logarithm problem is assumed to be hard, generator g, a bilinear map e : $\mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ for which bilinear Diffie

Hellman problem is assumed to be hard, a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_0$ which maps a binary string encoded attribute to a group element, chose random numbers $\alpha, \beta \in_R \mathbb{Z}_p$ and set its private key ASK and public key APK as below.

$$\begin{aligned} \text{ASK} &= \{\beta, g^{\alpha}\} \\ \text{APK} &= \{g^{\beta}, e(g,g)^{\alpha}, \mathbb{G}_0, g\} \end{aligned} \tag{5.1}$$

5.5.1 Attribute Assignment

An attribute can be any characteristic of a subscriber or requester and is represented by a binary string $\{0,1\}^*$. Attribute assignment to both subscribers and requesters is proposed to be done lazily in the background with the aim to keep the list of associated attributes in DigiLocker up to date.

For subscriber's attribute assignment and modification, two APIs are proposed to be introduced. First is $mathrmPullAttrs(ID_i)$ which is provided by issuers and is consumed by DigiLocker to pull the updated list of attributes of the subscriber with Aadhaar number ID_i. Second is PushAttrs(ID_i, NewAttrs) which is provided by DigiLocker and is consumed by the issuer to push any change in attributes of the subscriber with Aadhaar number ID_i. For requester applications, attributes are assigned and updated by DigiLocker.

It is important to take appropriate measures to handle load of a voluminous country like India. One such measure could be to prepone part of the encryption process. This preponed encryption process generates a token with mutual cooperation between subscriber and issuer. This token can be reused every time for a given subscriber and for a given access policy.

A helper procedure encPartial($\mathcal{T}$, r) is assumed to be present which works as follows. It chooses a polynomial q_x for each node x (including the leaves) in the tree $\mathcal{T}$. These polynomials are chosen in the following way in a top-down manner,

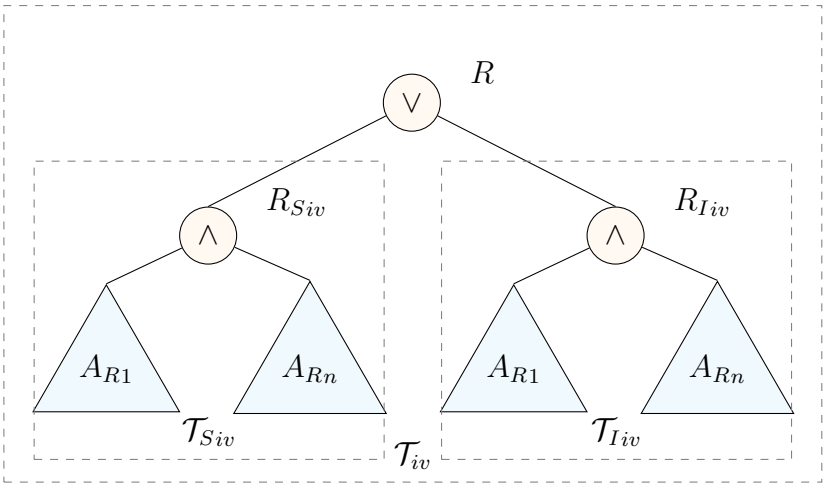


Figure 5.2: Example of an access policy tree

starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$. Starting with the root node R the procedure chooses a random $r \in_R \mathbb{Z}_p$ and sets $q_r(0) = r$. Then, it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses d_x other points randomly to completely define q_x.

5.5.2 Token Generation

An access tree $\mathcal{T}_{iv}$ is comprised of access subtree $\mathcal{T}_{S_{iv}}$ from subscriber S_i and access subtree $\mathcal{T}_{I_{iv}}$ from issuer I_v (refer figure 7.1). If issuer I_v needs to generate its part of token for subscriber S_i, for access tree $\mathcal{T}_{iv}$, it generates a random number $r_i \in_R \mathbb{Z}_p$, and generates following partial-token using APK and encPartial($\mathcal{T}_{I_{iv}}, r_i$). Let Y_I is the set of leaf nodes in $\mathcal{T}_{I_{iv}}$.

$$\text{CTtok}_{I_{iv}} = \begin{cases} \mathcal{T}_{I_{iv}} \\ C1_I = e(g,g)^{\alpha r_i} \\ C2_I = g^{\beta r_i} \\ \left.\begin{array}{l} C3_{I_y} = g^{q_y(0)} \\ C4_{I_y} = H(attr(y))^{q_y(0)} \end{array}\right\} \forall\ y \in Y_I \end{cases} \tag{5.2}$$

Issuer notifies subscriber to provide its part of the token. Subscriber S_i generates a random number $r_s \in_R \mathbb{Z}_p$ and generates following partial-token using APK and encPartial($\mathcal{T}_{S_{iv}}$). Let Y_S is the set of leaf nodes in $\mathcal{T}_{S_{iv}}$.

$$\text{CTtok}_{S_{iv}} = \begin{cases} \mathcal{T}_{S_{iv}} \\ C1_S = e(g,g)^{\alpha r_s} \\ C2_S = g^{\beta r_s} \\ \left.\begin{array}{l} C3_{S_y} = g^{q_y(0)} \\ C4_{S_y} = H(attr(y))^{q_y(0)} \end{array}\right\} \forall\ y \in Y_S \end{cases} \tag{5.3}$$

The subscriber provides its part of partial-token to the issuer. The issuer creates the final token by combining the two partial-tokens and keeps it securely with it.

$$\text{CTtok}_{iv} = \begin{cases} \mathcal{T}_{iv} = \mathcal{T}_{S_{iv}} \cup \mathcal{T}_{I_{iv}} \\ C1 = C1_S.C1_I \\ \quad = e(g,g)^{\alpha r_s} e(g,g)^{\alpha r_i} \\ C2 = C2_S.C2_I = g^{\beta r_s} g^{\beta r_i} \\ \left.\begin{array}{l} C3 = C3_{S_y} \cup C3_{I_y} \\ \quad = g^{q_y(0)} \\ C4 = C4_{S_y} \cup C4_{I_y} \\ \quad = H(attr(y))^{q_y(0)} \end{array}\right\} \forall\ y \in Y_S \cup Y_I \end{cases} \tag{5.4}$$

5.5.3 Encryption

A new *DocType* PRIV is proposed to be introduced for privacy enhanced e-documents. To create a privacy enhanced e-document, issuer creates a URI $\langle I_v :: PRIV :: D_w \rangle$ where I_v is the issuer identifier and D_w is the document identifier within the doc-

ument type PRIV. Now, issuer generates a random number $r_{ie} \in_R \mathbb{Z}_p$, generates a symmetric key SK_{ivw}, encrypts e-document m with SK_{ivw}, encrypts SK_{ivw} with $CTtok_{I_{iv}}$ and produces the following ciphertext.

$$CT_{ivw} = \begin{cases} \mathcal{T}_{iv} = \mathcal{T}_{S_{iv}} \cup \mathcal{T}_{I_{iv}} \\ C1 = e(g,g)^{\alpha r_s r_{ie}} e(g,g)^{\alpha r_i r_{ie}} SK_{ivw} \\ C2 = g^{\beta r_s r_{ie}} g^{\beta r_i r_{ie}} \\ \left.\begin{array}{l} C3_y = g^{r_{ie}(q_y(0))} \\ C4_y = H(attr(y))^{q_y(0)} \end{array}\right\} \forall\ y \in Y_{iv} \\ C5 = \{m\}_{SK_{ivw}} \end{cases} \tag{5.5}$$

5.5.4 Key Generation

A new API $GenABPvtKey(ID_i, IS_j)$ is proposed to be provided by DigiLocker to generate an attribute-based private key for a subscriber with Aadhaar identifier ID_i and with attributes from issuers in the set IS_j. Let S_{ij} is the set of all attributes assigned to S_i by all issuers in set IS_j. DigiLocker generates random numbers $r \in_R \mathbb{Z}_p$, $r_j \in_R \mathbb{Z}_p$ for each attribute $j \in_R S_{ij}$, computes attribute-based private key $ASK_{ID_i IS_j}$ as below and keeps this key securely with it.

$$ASK_{ID_i IS_j} = \left\{ \begin{array}{l} D = g^{(\alpha + r)/\beta} \\ \left.\begin{array}{l} D_j = g^r . H(j)^{r_j} \\ D_j\prime = g^{r_j} \end{array}\right\} \forall\ j \in S_{ij} \end{array} \right. \tag{5.6}$$

Note that multiple attribute-based private keys can exist for a subscriber for a different set of attributes. If anyone issuer set IS_i is a proper subset of another issuer set IS_j, the key corresponding to IS_i is redundant and can be removed.

5.5.5 Decryption

A new API FetchPrivDocURI is proposed to be provided by DigiLocker for decryption purpose. This API facilitates a requester with identifier ID_R to retrieve ciphertext CT_{ivw} of e-document from URI $\langle I_v :: PRIV :: D_W \rangle$ of subscriber S_i. DigiLocker extracts the set of attribute issuers IS_k from $CT_{ivw} \rightarrow \mathcal{T}_{iv}$, retrieves $ASK_{ID_R IS_k}$ and calls $Decrypt(CT_{ivw}, ASK_{ID_R IS_k})$. A helper procedure $DecryptNode(CT_{ivw}, ASK_{ID_R IS_K})$ is defined as below. Let S_k is the set of all attributes from issuers in set IS_k. If x is a leaf node and if $attr(x) \notin S_k$, then $DecryptNode(CT_{ivw}, ASK_{ID_R IS_k}, x) = \perp$ else if $attr(x) \in S_k$, then the procedure is defined as below.

$$\begin{aligned} &DecryptNode(CT_{ivw}, ASK_{ID_R IS_k}, x) \\ &= \frac{e(D_x, C4_y)}{e(D_x\prime, C5_y)} \\ &= \frac{e(g^r.H(attr(x))^{r_j}, g^{r_{ie} q_y(0)})}{e(g^{r_j}, H(attr(x))^{q_x(0)})} \\ &= e(g,g)^{r r_{ie} q_x(0)} \end{aligned} \tag{5.7}$$

If x is a non-leaf node, the recursive procedure is defined as follows. For all children nodes z of x, $DecryptNode(CT_{ivw}, ASK_i, x)$ is called and their output is stored in F_z. Let S_x be an arbitrary k_x sized set of child nodes z such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$. Otherwise, F_x is computed as below.

$$
\begin{aligned}
F_x &= \prod_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)} \qquad \begin{matrix} \text{where}\{i = \text{index}(z) \\ S_x' = \{\text{index}(z) : z \in S_x\} \end{matrix} \\
&= \prod_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} (e(g,g)^{r.r_{ie}.q_z(0)})^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} (e(g,g)^{r.r_{ie}.q_{\text{parent}(z)}(\text{index}(z))})^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} e(g,g)^{r.r_{ie}.q_x(i)\Delta_{i,S_x'}(0)} \\
&= e(g,g)^{rr_{ie}q_x(0)} \text{ (using polynomial interpolation)} \qquad (5.8)
\end{aligned}
$$

Decrypt$(CT_{ivw}, ASK_{ID_R IS_k})$ calls DecryptNode($CT_{ivw}, ASK_{ID_R IS_k}, R$) where R is root node of T_{iv}. If the access tree is satisfied by attributes in S_k, set A = DecryptNode$(CT_{ivw}, ASK_{ID_R IS_k}, R) = e(g,g)^{r.r_{ie}.(r_s+r_i)}$. Now the procedure obtains symmetric key SK_{ivw} by computing

$$
\begin{aligned}
\frac{C1}{\frac{e(C2,D)}{A}} &= \frac{e(g,g)^{\alpha r_s r_{ie}} e(g,g)^{\alpha r_i r_{ie}} SK_{ivw}}{\frac{e(g^{\beta r_s r_{ie}} g^{\beta r_i r_{ie}}, g^{(\alpha+r)/\beta})}{e(g,g)^{rr_{ie}(r_s+r_i))}}} \\
&= \frac{e(g,g)^{\alpha r_s r_{ie}} e(g,g)^{\alpha r_i r_{ie}} SK_{ivw}}{\frac{e(g^{\beta r_{ie}(r_s+r_i)}, g^{(\alpha+r)/\beta})}{e(g,g)^{rr_{ie}(r_s+r_i))}}} \\
&= \frac{e(g,g)^{\alpha r_{ie}(r_s+r_i)} SK_{ivw}}{\frac{e(g,g)^{r_{ie}(r_s+r_i)(\alpha+r)}}{e(g,g)^{rr_{ie}(r_s+r_i))}}} \\
&= SK_{ivw} \qquad (5.9)
\end{aligned}
$$

Symmetric key SK_{ivw} is now used to decrypt the encrypted e-document.

$$
m = \{CT_{ivw} \rightarrow C5\}_{SK_{ivw}} \qquad (5.10)
$$

DigiLocker returns the decrypted document m to requester.

5.5.6 Security Analysis

If the proposed scheme is not secure than an adversary $\mathcal{A}$ can win IND-sAtt-CPA game and solve the DBDH assumption with advantage $\epsilon/2$. If the DBDG assumption is solved by adversary $\mathcal{A}$, a simulator β can be built which can solve DBDH assumption with advantage $\epsilon/2$. Challenger chose a group $\mathbb{G}_0$, a generator g, a bilinear map e and chose random numbers $\mathrm{a}, \mathrm{b}, \mathrm{c}, \theta \in_{\mathrm{R}} \mathbb{Z}_p^*$. The challenger selects at random $\mu \in_{\mathrm{R}} 0, 1$ and sets Z_μ as below.

$$\mathrm{Z}_\mu = \begin{cases} (\mathrm{g}, \mathrm{g})^{\mathrm{abc}}, & \text{if } \mu = 0 \\ \mathrm{e}(\mathrm{g}, \mathrm{g})^{\theta}, & \text{if } \mu = 1 \end{cases} \tag{5.11}$$

Challenger provides DBDB challenge to the simulator: $\langle \mathrm{g}, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{Z}_\mu \rangle$ $\langle \mathrm{g}, \mathrm{g}^{\mathrm{a}}, \mathrm{g}^{\mathrm{b}}, \mathrm{g}^{\mathrm{c}}, \mathrm{Z}_\mu \rangle$. In IND-sAtt-CPA game, simulator β plays the role of challenger for adversary $\mathcal{A}$.

Init Phase: The adversary chose the challenge access tree $\mathcal{T}^*$ and gives it to simulator.

Setup Phase: The challenger chose a random number $\mathrm{x}\prime \in \mathbb{Z}_p$, sets $\alpha = \mathrm{ab} + \mathrm{x}\prime$ and computes y as below.

$$\mathrm{y} = \mathrm{e}(\mathrm{g}, \mathrm{g})^{\alpha} = \mathrm{e}(\mathrm{g}, \mathrm{g})^{\mathrm{ab}} \mathrm{e}(\mathrm{g}, \mathrm{g})^{\mathrm{x}\prime} \tag{5.12}$$

Now, challenger chose a random numbers $\mathrm{r} \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$ and $\mathrm{r_i} \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$ for $(1 \leq \mathrm{i} \leq |\mathrm{U}|)$ and for all $\mathrm{a_j} \in \mathbb{U}$, computes $\mathrm{d_j}$ and $\mathrm{d_j}\prime$ as below.

$$\left.\begin{aligned} \mathrm{d_j} &= \begin{cases} \mathrm{g}^{\mathrm{r}/\mathrm{b}} \mathrm{H}(\mathrm{j})^{\mathrm{r_j}} & \text{...if } \mathrm{a_j} \notin \mathcal{T}^* \\ \mathrm{g}^{\mathrm{r}} \mathrm{H}(\mathrm{j})^{\mathrm{r_j}} & \text{...if } \mathrm{a_j} \in \mathcal{T}^* \end{cases} \\ \mathrm{d_j}\prime &= \mathrm{g}^{\mathrm{r_j}} \end{aligned}\right\} (1 \leq \mathrm{j} \leq |\mathrm{U}|) \tag{5.13}$$

Now, challenger sends public parameters $\text{APK} = \{g^{\beta}, e(g,g)^{\alpha}, \mathbb{G}, g\}$ to adversary $\mathcal{A}$.

Phase 1: In this phase, adversary $\mathcal{A}$ sends requests for private key for any set of attributes w_j which does not contain any attribute in $\mathcal{T}^*$.

$$w_j = \{a_j \mid (a_j \in \mathbb{U} \wedge a_j \notin \mathcal{T}^*)\} \tag{5.14}$$

For each query from adversary $\mathcal{A}$, challenger chose a random number $r\prime \in_R \mathbb{Z}_p$, sets $r = -b(r\prime + a)$ and computes D as below.

$$\begin{aligned} D &= g^{(\alpha+r)/\beta} = (g^{(\alpha+r)})^{1/\beta} = (g^{((ab+x\prime)-b(r\prime+a))})^{1/\beta} \\ &= (g^{x\prime-br\prime})^{1/\beta} = (g^{x\prime}.(g^{b})^{-r\prime})^{1/\beta} \end{aligned} \tag{5.15}$$

Because of restriction $a_j \notin \mathcal{T}^*$ in this phase, D_j can be computed as below.

$$\begin{aligned} D_j &= g^{r/b}H(j)^{r_j} = g^{r/b}H(j)^{r_j} = g^{-(r\prime+a)}H(j)^{r_j} \\ &= (g^{a})^{-1}g^{-r\prime}H(j)^{r_j} \end{aligned} \tag{5.16}$$

Now, challenger sends private key $\text{ASK}_{w_j} = D, (D_j, D_j\prime) \mid \forall a_j \in w_j$ to adversary $\mathcal{A}$

Challenge Phase: In this phase, adversary $\mathcal{A}$ submits two plaintext messages m_0 and m_1 to the challenger. Challenger selects a random plaintext message m_b from the two messages where $b \in_R \{0,1\}$, sets $r_{ie} = 1$, chose random variables r_i and r_s such that $c = r_i + r_c$. Now, set value of root node $\mathcal{T}^*$ to c and assign values to leaf nodes of $\mathcal{T}^*$ as described in section on *access tree* to arrive at $C3_y$ and $C4_y$. The final ciphertext $\text{CT}_{\mathcal{T}^*}$ is computed as below. The ciphertext is returned to adversary $\mathcal{A}$.

$$CT_{\mathcal{T}^*} = \begin{cases} \mathcal{T}_{iv} = \mathcal{T}^* \\ \mathrm{C1} = \mathrm{e(g,g)}^{\alpha \mathrm{r_s}} \mathrm{e(g,g)}^{\alpha \mathrm{r_i}} \mathrm{m_b} \\ \quad = \mathrm{e(g,g)}^{\alpha(\mathrm{r_s}+\mathrm{r_i})} \mathrm{m_b} \\ \quad = \mathrm{e(g,g)}^{\mathrm{c}} \mathrm{m_b} \\ \mathrm{C2} = \mathrm{g}^{\beta \mathrm{r_s}} \mathrm{g}^{\beta \mathrm{r_i}} = \mathrm{g}^{\beta(\mathrm{r_s}+\mathrm{r_i})} \\ \quad = \mathrm{g}^{\beta} \mathrm{g}^{\mathrm{c}} \\ \left.\begin{array}{l} \mathrm{C3_y} = \mathrm{g}^{(\mathrm{q_y}(0))} \\ \mathrm{C4_y} = \mathrm{H(attr(y))}^{\mathrm{q_y}(0)} \end{array}\right\} \forall\ \mathrm{y} \in \mathrm{Y_{iv}} \end{cases} \tag{5.17}$$

Phase 2: In this phase, adversary $\mathcal{A}$ can continue to send secret key generation requests with the same restriction as in *Phase*1, i.e., $\mathrm{a_j} \notin \mathcal{T}^*$.

Guess Phase: In this phase, adversary $\mathcal{A}$ outputs a guess $\mathrm{b\prime} \in \{0, 1\}$. If $\mathrm{b\prime} = \mathrm{b}$, the simulator β will guess that $\mu = 0$ and $\mathrm{Z}_\mu = \mathrm{e(g,g)}^{\mathrm{abc}}$, otherwise will guess that $\mu = 1$ and $\mathrm{Z}_\mu = \mathrm{e(g,g)}^{\theta}$. When $\mathrm{Z}_u = \mathrm{e(g,g)}^{\mathrm{abc}}$ the simulator β gives the perfect simulation and $\mathrm{c}_{\mathcal{T}^*}$ is a valid ciphertext. Therefore, the advantage of the adversary is

$$\Pr[\mathrm{b\prime} = \mathrm{b} \mid \mathrm{Z}_\mu = \mathrm{e(g,g)}^{\mathrm{abc}}] = \frac{1}{2} + \epsilon \tag{5.18}$$

If $\mu = 1$ then $\mathrm{Z}_\mu = \mathrm{e(g,g)}^{\theta}$ and $\mathrm{c}_{\mathcal{T}^*}$ is random ciphertext for the adversary, and the adversary does not gain information about $\mathrm{m_b}$. Hence, we have

$$\Pr[\mathrm{b\prime} \neq \mathrm{b} \mid \mathrm{Z}_\mu = \mathrm{e(g,g)}^{\theta}] = \frac{1}{2} \tag{5.19}$$

Since the simulator β guesses $\mu\prime = 0$ when $\mathrm{b\prime} = \mathrm{b}$ and $\mu\prime = 1$ when $\mathrm{b\prime} \neq \mathrm{b}$, the overall advantage of β to solve DBDH assumption is

$$\frac{1}{2}\Pr[\mu\prime = \mu \mid \mu = 0] + \frac{1}{2}\Pr[\mu\prime = \mu \mid \mu = 1] - \frac{1}{2} = \frac{\epsilon}{2} \tag{5.20}$$

If the adversary $\mathcal{A}$ has the above advantage ϵ to win the IND-sAtt-CPA game, the challenger can solve the DBDH assumption problem with $\epsilon/2$ advantage with the help of adversary $\mathcal{A}$. However, there are no effective polynomial algorithms which can solve the DBDH assumption problem with non-negligible advantage according to the DBDH assumption. Hence, the adversary cannot win the IND-sAtt-CPA game with the above advantage ϵ, namely the adversary having no advantage to break through the proposed scheme.

5.6 Summary

This chapter presents a mechanism to improve data privacy in DigiLocker, in which subscriber can encrypt his documents using a privacy policy and only the requesters whose attributes satisfy the policy can decrypt and retrieve the document. The proposed scheme prepones part of the encryption process to increase performance. This preponed process creates a digital token that can be reused later. The proposed scheme is proved to be secure against IND-sAtt-CPA game. The next chapter explores privacy requirements and possible improvement in toll payment service.

This page intentionally left blank.

Chapter 6

Privacy Enhanced Toll Payment

Previous chapter presented a mechanism to improve privacy in Aadhaar-based DigiLocker service, which provides a sharable private storage space on public cloud to its subscribers. With the introduction of IoT and VANET based systems, number of devices and inter-device communication has increased substantially and is expected to increase even further. With this information outgrowth, Privacy and Anonymity are two important security goals which are getting more and more attention. This chapter presents a mechanism to ensure privacy of data and anonymity of entities while communicating for payment of toll tax in a VANET based system.

6.1 Introduction

Recent developments in Information and Communication Technology (ICT) have enabled new opportunities in information technology. This has led to the emergence of new concepts such as Internet of Things (IoT), Intelligent Transport Systems (ITS), Vehicular Adhoc NETworks (VANETs), etc. VANET is generally classified as vehicle to vehicle communication which is also referred to as Inter-Vehicle Communication (IVC) and vehicle to infrastructure communication which is also referred to as Vehicle-to-Roadside Communication (VRC). IoT and VANET have

led to the information outgrowth and *Privacy* and *Anonymity* are two security goals which are gaining more and more attention. Although these two goals are

Notation	**Description**
U_i	End User
UID_{Ui}	User Identification Device for user U_i
RTO	Regional Transport Office
IB_i	Issuer Bank
AS	Authentication Server
TS_i	Toll Station
VM_{Ui}	Vehicle Manufacturer
sPC_{Ui}	Smart Payment Card of U_i (Received from IB_i)
sRC_{Vi}	Smart Vehicle Registration Certificate Card of user U_i (Received from RTO)
ID_AS_{Ui}	Identities of user U_i in AS, user U_i in IB_i,
ID_IB_{Ui}	Vehicle Manufacturer VM_i in RTO and Toll
ID_RTO_{VMi}	Station TS_i in RTO
ID_RTO_{TSi}	
PW_AS_{Ui}	Passwords for user U_i in AS, user U_i in IB_i,
PW_IB_{Ui}	Vehicle Manufacturer VM_i in RTO and Toll
PW_RTO_{VMi}	Station TS_i in RTO
PW_RTO_{TSi}	
SK_{Ui_AS}	Symmetric key shared between U_i and AS.
SK_{Ui_IBi}	Symmetric key shared between U_i and IB_i
SK_{VMi_RTO}	Symmetric key shared between VM_i and RTO
SK_{TSi_RTO}	Symmetric key shared between TS_i and RTO
SK_{Vi_RTO}	Symmetric key shared between V_i and RTO
SK_{sPC_sRC}	Symmetric key shared between sPC_{Ui} and sRC_{Vi}
N_i, (i = 1...n)	Nonces generated by different entities.
NX_i, (i = 1...n)	Data generated by combining nonces and other terms.
S_{RTO_TS}	Secret kept with *RTO* used when interacting
R_{RTO_TS}	with TS_i
S_{RTO_V}	Secret kept with *RTO* used when interacting
R_{RTO_V}	with Vehicle's sRC_i
$Data_i$, (i = 1...n)	Data (in plaintext) to be communicated
$PData_i$, (i = 1...n)	Data (in ciphertext) to be communicated

Table 6.1: Notations used in this chapter

often used interchangeably they have subtle differences. Privacy implies *freedom of actions* and anonymity implies *freedom of expressions*. Privacy hides *what one does* and anonymity hides *who one is*. Since one of the distinguished characteristic of VANET and IoT is the usage of low power devices, traditional asymmetric

cryptographic based operations cannot be used in such cases. Secure Socket Layer (SSL)/Transport Layer Security (TLS) provides protection for all data in communication but it needs pre-configuration and involves heavy asymmetric cryptographic operations which may not be feasible for resource constraint devices. This chapter presents a mechanism to ensure security, privacy and anonymity in vehicle to infrastructure communication in automated collection of toll tax payment using lightweight operations such as one-way cryptographic hash, XOR and concatenation. The chapter uses notations mentioned in figure 6.1.

6.2 Related Work

The use of sensitive and personal data during traffic communication should be secured from disclosure and possible misuse. In vehicular network, privacy related issues can arise at multiple stages such as aggregation, processing, collection, evaluation and visualization. Preserving privacy of personal data in these stages is an essential requirement [107]. Many of the researchers have proposed their schemes in this area. Some of the relevant work is presented below.

[108] proposed a scheme emphasising on the message recovery certificateless signature to enhance conditional privacy of the system. The proposed scheme also ensures unlinkability since the vehicle is not associated with the message it sends. The scheme however does not provide unobservability. [109] proposed a certificateless scheme based on elliptic curve to achieve conditional privacy. However, this scheme also does not provide unobservability. [110] proposed a privacy enhanced scheme based on HMACs. Instead of the certificate revocation list, the scheme proposed to use the revocation of vehicles. The scheme also provides anonymity. This scheme, however, ignores contextual privacy. [111] proposed a scheme which provides location privacy and in which neighbour vehicles can authenticate the safety related messages. The scheme also provides traceability features. This scheme, however, does not provide unlinkability and unobservability. [112] proposed a scheme based

on K-anonymity and hash-based messages. This scheme provides a mechanism for an RSU to provide optimal communication cost and a mechanism to ensure privacy of the vehicle. The scheme also ensures that the communication messages are safe from any possible attack in the vehicle. However, the scheme does not provide contextual privacy. [113] proposed a scheme based on group communication to achieve privacy preserving properties. A group of vehicles does an initial handshake to recognize each other and can later authenticate each other without any support from the RSUs. During the handshake, the group of vehicles agrees upon a shared secret, which is used by members to securely communicate among themselves. Although the scheme provides unlinkability of communication messages, it ignores the contextual privacy. [114] proposed a scheme which uses CPAS, a vehicle-to-infrastructure framework to achieve some of the privacy properties. The proposed provided privacy, traceability and anonymity but not unlinkability and hence could not satisfy the unobservability and conditional privacy. [115] proposed a scheme based on elliptic curves to provide content privacy. The scheme uses a pseudonym rather than the real identity to achieve anonymity. However, the scheme could not provide contextual privacy. [116] proposed a privacy enhanced scheme in which RSUs store their master keys in a tamper proof device. The scheme ensures privacy of the drivers from other drivers and also provides unlinkability by not linking the vehicle with the communication messages. The scheme however does not provide unobservability privacy.

In [117], the proposed system assumes the presence of an RFID based smart card for automatic authentication and payment. The system identifies the RFID tag, authenticates it and makes the necessary payment. Once the payment is made successfully, the barrier is lifted. In [118], the toll collection process is analyzed in multiple phases such as association, authentication, payment and verification. The scheme has four participants, namely, the vehicle, the RSU, the bank and the toll operator. The scheme has three protocols. In the first protocol, the vehicle is registered to obtain a unique identity. In the second protocol, the vehicle purchases

an e-toll from the bank. In the third protocol, the vehicle presents the e-toll to the toll operator. The scheme has a large number of messages which may introduce a potential delay in the whole process.

In some other researches, the authors proposed systems which assign prices to individual pathways and the final fee is calculated by summing prices of all the pathways travelled.

[119] and [120] were two of the earliest papers on enhancing privacy in maintaining traffic rules toll collection. [119] proposed a traffic enforcement system such as for red-light violations and uses a private-set intersection protocol to achieve the same. [120] proposed a toll tax collection system and uses a general evaluation of a secure function. [121] proposed a trusted tamper-resistant hardware in each vehicle which calculates the amount to be paid and which also facilitates the functioning of the hardware to be monitored by the owner of the vehicle. [122] proposed a privacy enhanced toll system which takes path commitment from the driver which he drove without revealing every pathways he drove. Hash functions were used to make commitments which made the system very efficient. The system ensured that the right fee is computed by revealing essentially one path from one leaf in Merkele hash tree to the root of the tree. The system also used intermittent checks to ensure that the reported pathways were indeed reported genuinely. [123] proposed a privacy preserving toll system which uses the homomorphic commitments in which the drivers commit to the prices for each pathway and the sum of those prices. The product of the commitments made is actually the commitment of the sum of the prices of individual pathways. This helps in verifying that the final sum of the price is computed correctly. Similar to the earlier systems, this system also used intermittent checks to ensure that the reported pathways were indeed reported genuinely. However, in this scheme, the driver is required to provide the individual road segments he drove and to avoid disclosure of IP addresses, they are supposed to use networks (such as Tor) which conceal user location. [124] proposed some of the shortcomings by not

requiring the driver to disclose individual pathways he drove and hence not requiring him to use networks such as Tor. The scheme proposed to commit to a pathway (and hence to the corresponding fee) homomorphically. In the audit protocol, the commitments are opened

Several safety and convenience applications have been introduced in VANET and IoT domain [120], [125], [126], [127]. This includes better and smarter ITS which can facilitate to avoid collision, to find quickest path to a destination, automated fare collection, smart parking, etc. Most of the proposed protocols use asymmetric and elliptic curve cryptography which are not very suitable for fast-moving vehicles or tiny devices. Moreover, privacy and anonymity are often ignored by these works.

Based on communication limitations among user, merchant and payment gateway payment mode can be envisaged in following different ways [128].

- Kiosk-Centric. In this model, users cannot directly interact with the issuer. Merchant acts as a proxy to facilitate communication between user and issuer.
- User-Centric. In this model, merchants cannot directly interact with the acquirer. User acts as a proxy to facilitate communication between merchant and acquirer.
- Server-Centric. In this model, user and merchant cannot communicate with each other. Payment gateway acts as an intermediary to facilitate communication between user and merchant.

Most of the studies are based on the assumption that user and merchant can both talk to each other as well as to the payment gateway. [129] proposed a mobile payment protocol for VANET but that is based on user-centric payment model which is not suitable for payments such as toll tax since in such scenarios, the restriction is with the user and not the merchant. Moreover, the work does not aim to achieve

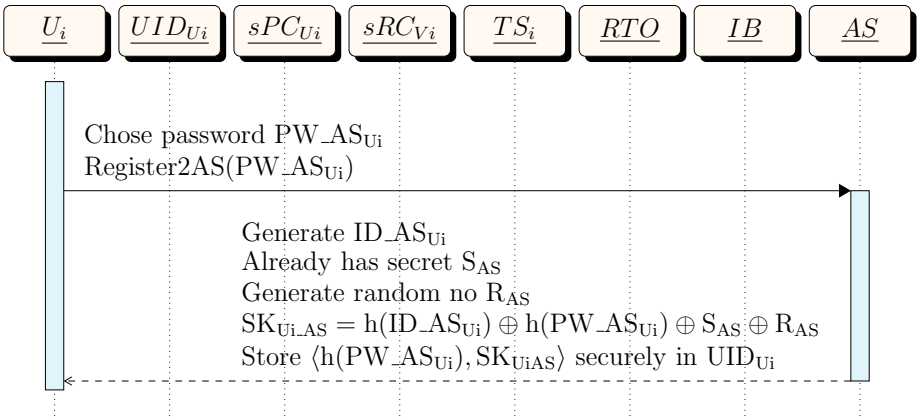


Figure 6.1: User Registration at Authentication Server

privacy and anonymity in its model.

As discussed in the review above, content privacy and anonymity property is not or partially provided by many of the earlier proposed schemes. This chapter proposes a privacy enhancing scheme which addresses some of the weaknesses in these schemes. The proposed scheme addresses privacy requirements such as content privacy, anonymity and unobservability. In addition, the proposed scheme also uses BAN logic and ProVerif to ensure that the scheme is secure against various types of attacks such as replay, impersonation, modification and man-in-the-middle.

6.3 Proposed Model of privacy enhanced toll payment

The proposed model ensures that the vehicle does not disclose its identity to the toll station and yet the vehicle is issued a toll ticket generated directly from the RTO. This enables transparency of actions, privacy of information and anonymity of identity and still achieving the desired level of functionality.

The proposed model consists of registration phase of participating entities and the payment phase in which participating entities interact with each other for the payment of toll tax.

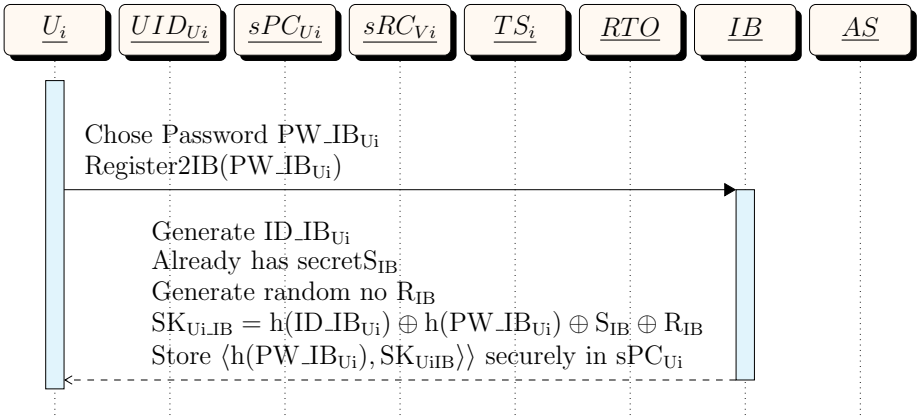
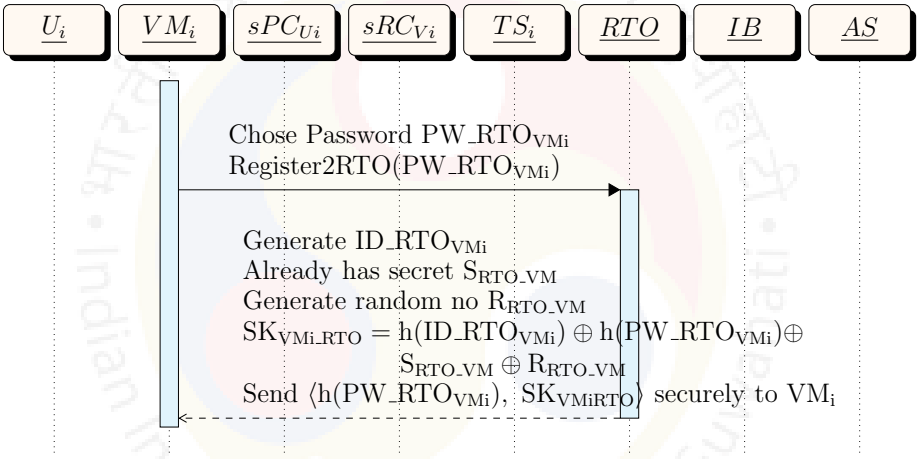


Figure 6.2: User Registration at Issuer Bank



=

Figure 6.3: Manufacturer Registration at RTO

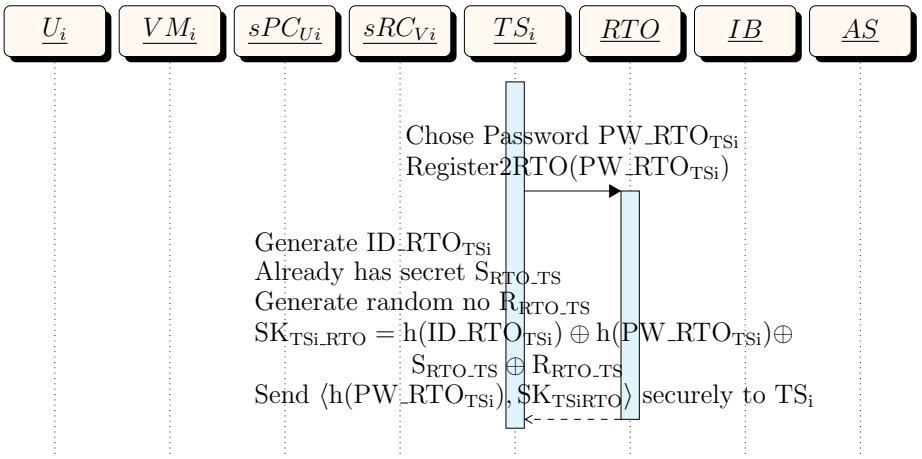


Figure 6.4: Toll Station Registration at RTO

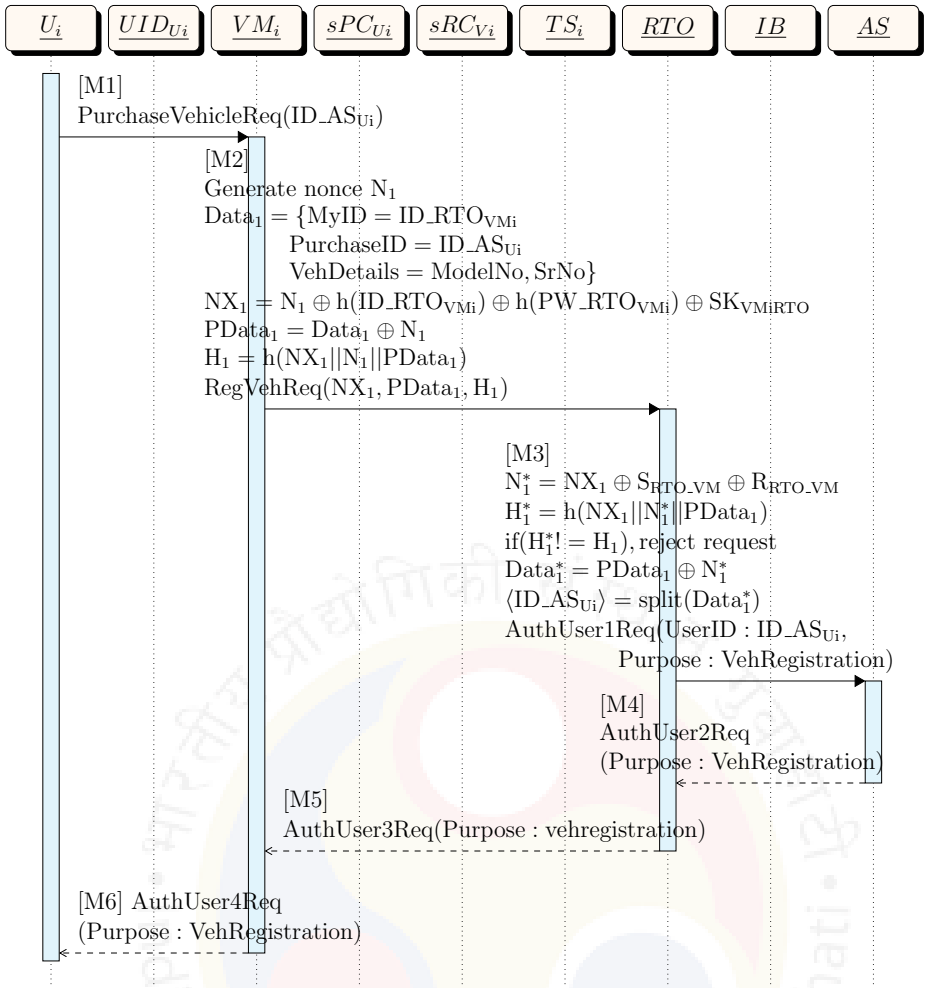


Figure 6.5: Vehicle Registration at RTO - Part 1

6.3.1 Registration Phase

Registration phase consists of *User Registration at Authentication Server*, User Registration at Issuer Bank, Vehicle Manufacturer Registration at RTO, Toll Station Registration at RTO, Vehicle Registration at RTO and Payment Card Registration with Vehicle. Registration of user with authentication server is illustrated in figure 6.1, registration of user with issuer bank is illustrated in figure 6.2, registration of manufacturer with RTO is illustrated in figure 6.3, registration of toll station at RTO is illustrated in figure 6.4, vehicle registration is illustrated in figures 6.5, 6.6 - registration of payment card with vehicle is illustrated in figures 6.7 - 6.8.

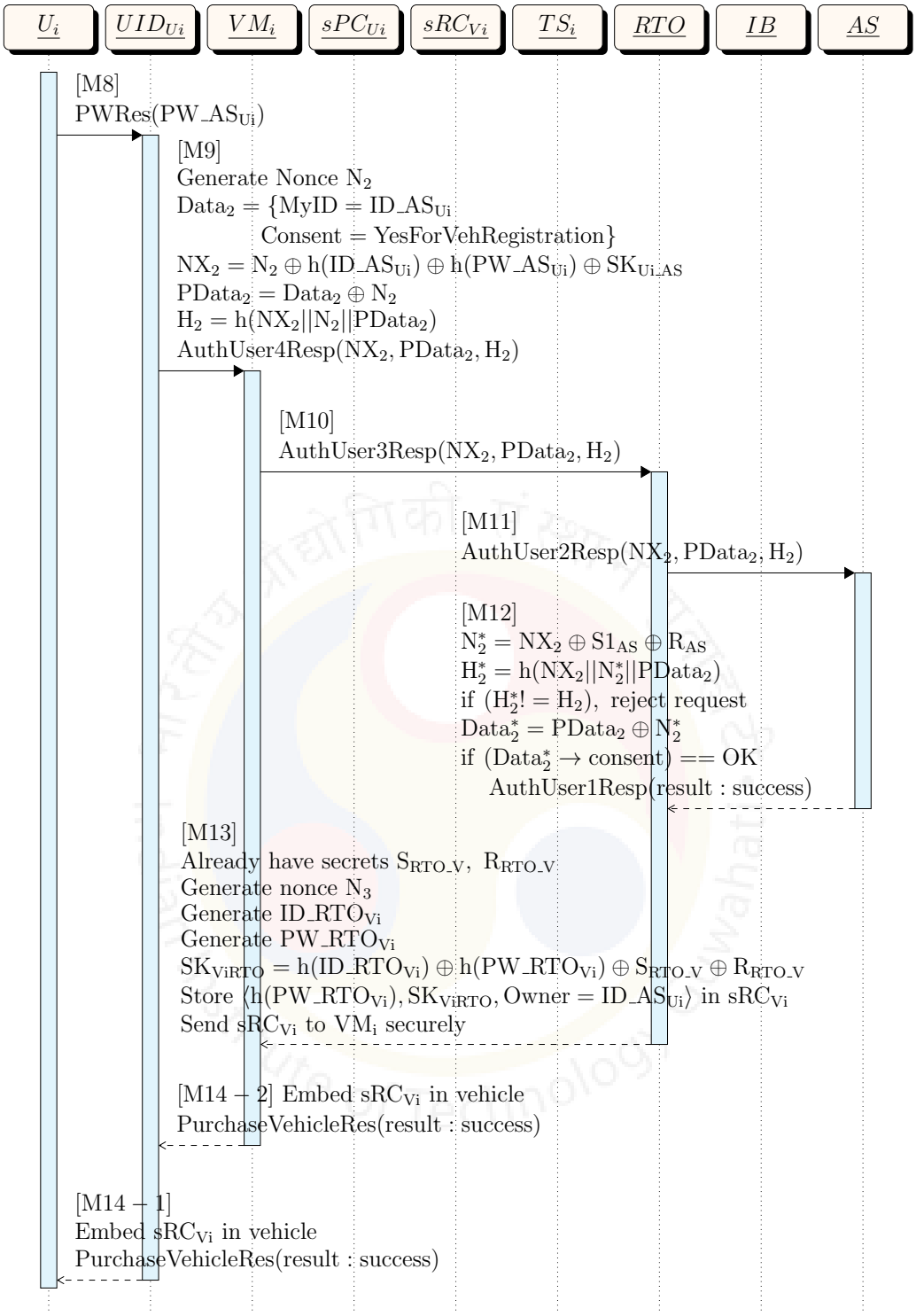


Figure 6.6: Vehicle Registration at RTO - Part 2

6.3.2 Payment Phase

Steps for initializing the payment phase at start of the vehicle are explained in figure 6.9. Steps for payment phase when the vehicle approaches a toll station are explained in figures 6.11 - 6.15.

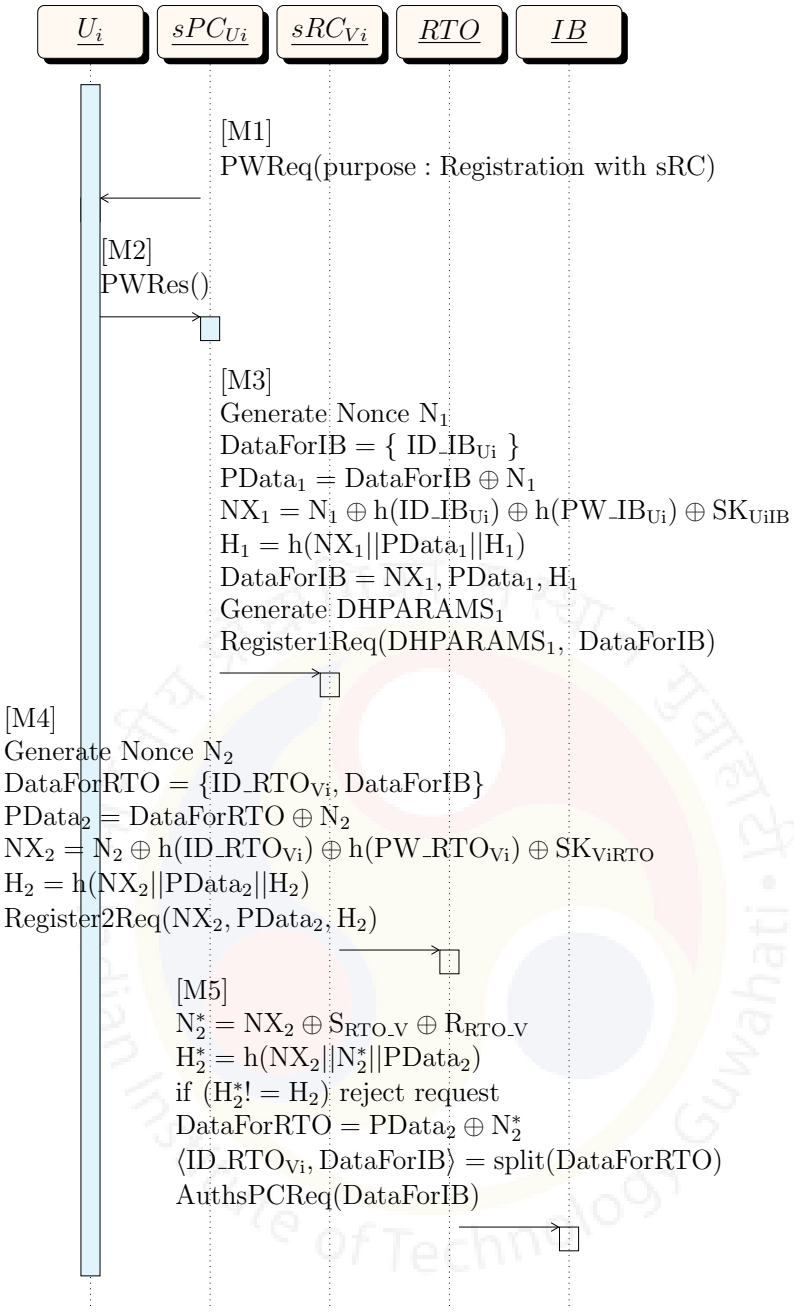


Figure 6.7: sPC_i Registration with sRC_i (Part - I)

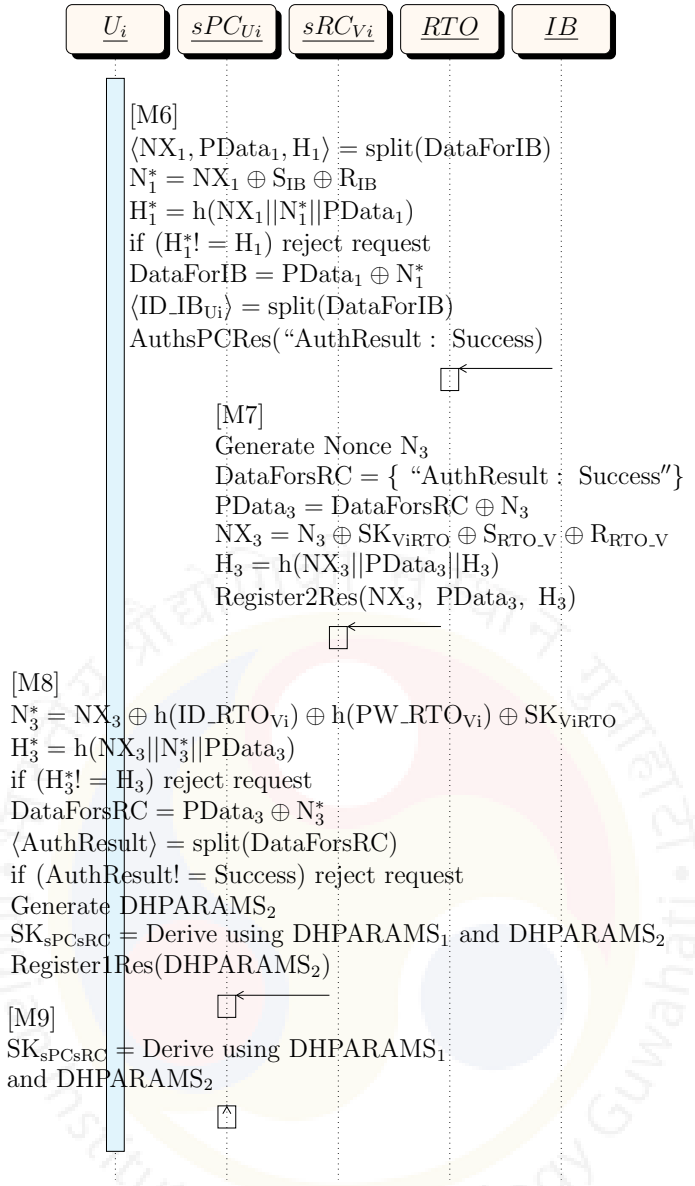


Figure 6.8: sPC_i Registration with sRC_i (Part - II)

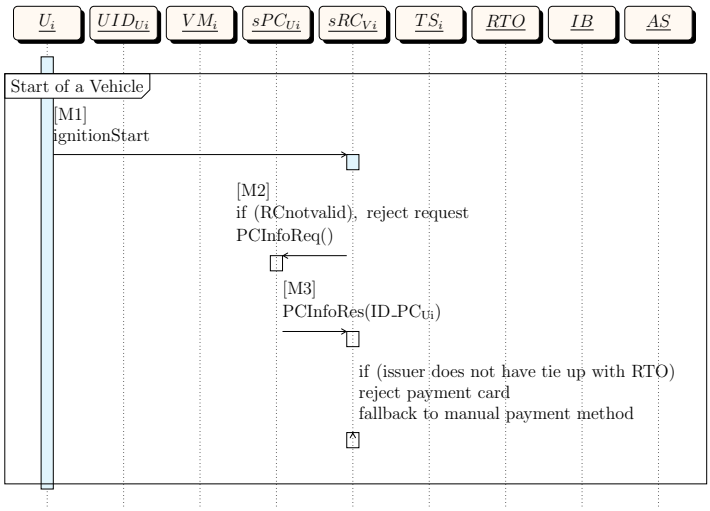


Figure 6.9: Start of a Vehicle

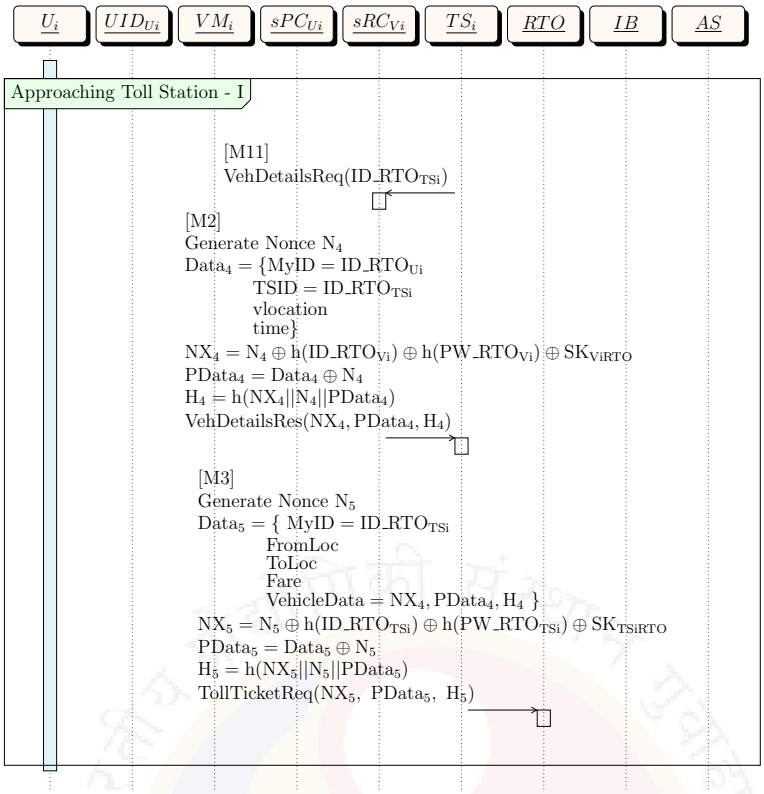


Figure 6.10: Payment Phase (Part - I.I)

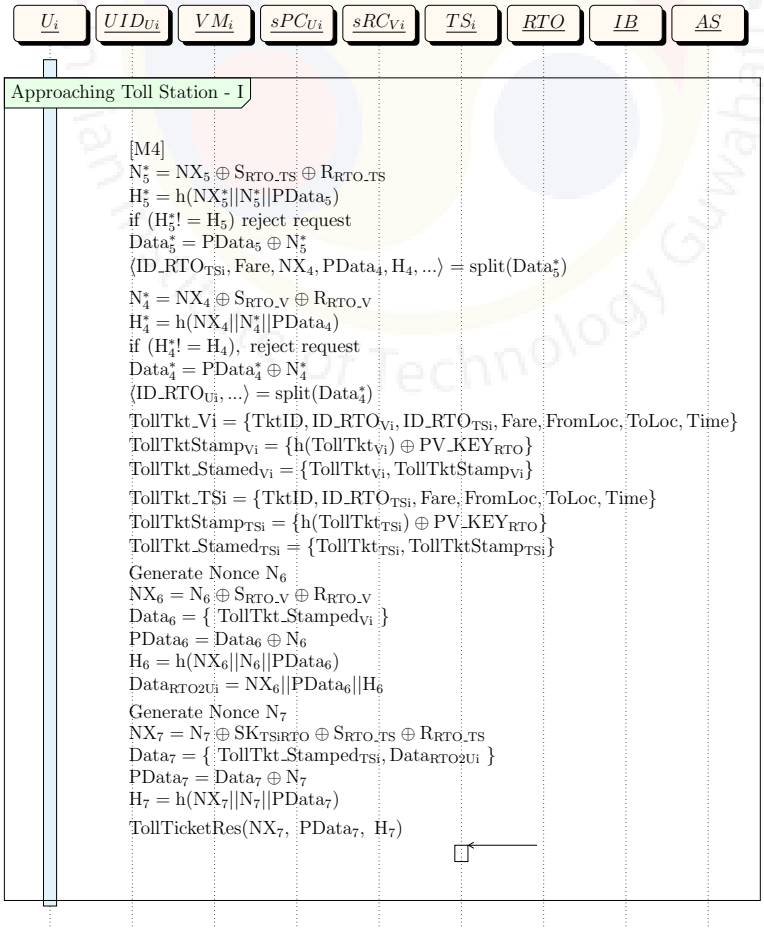


Figure 6.11: Payment Phase (Part - I.II)

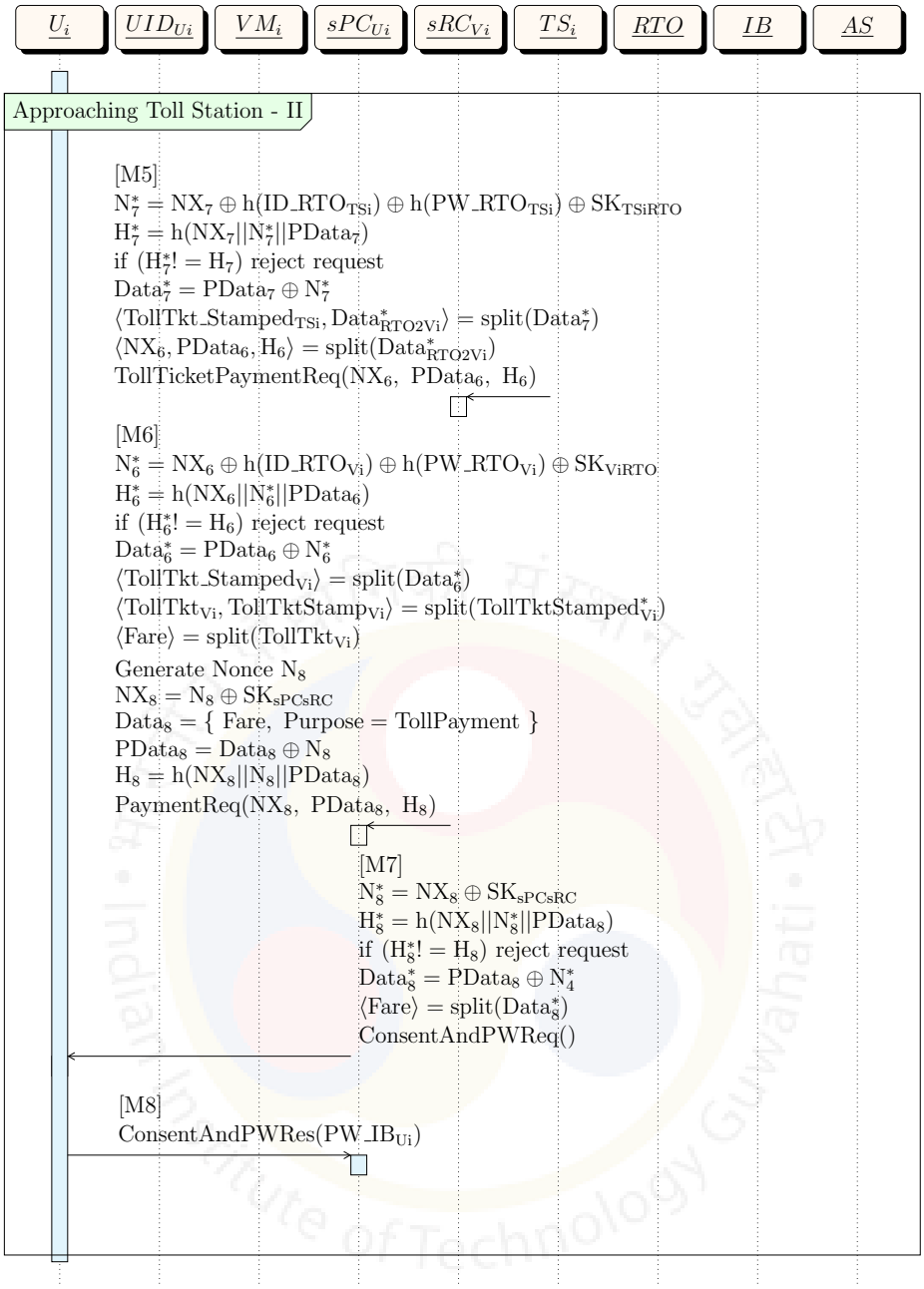


Figure 6.12: Payment Phase (Part - II.I)

6.3.3 Security Analysis

This section will demonstrate that the proposed scheme holds several key security requirements, which are essential in IoT environment.

Sender and Data Authentication

In communication phase, when one entity E1 wants to send some data to another entity E2, it creates a nonce N_E and builds three parameters NX_E, $PData_E$ and

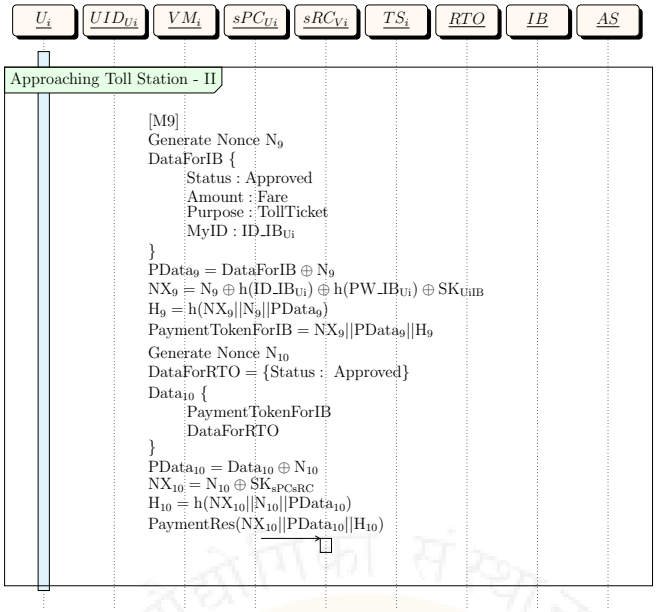


Figure 6.13: Payment Phase (Part - II.II)

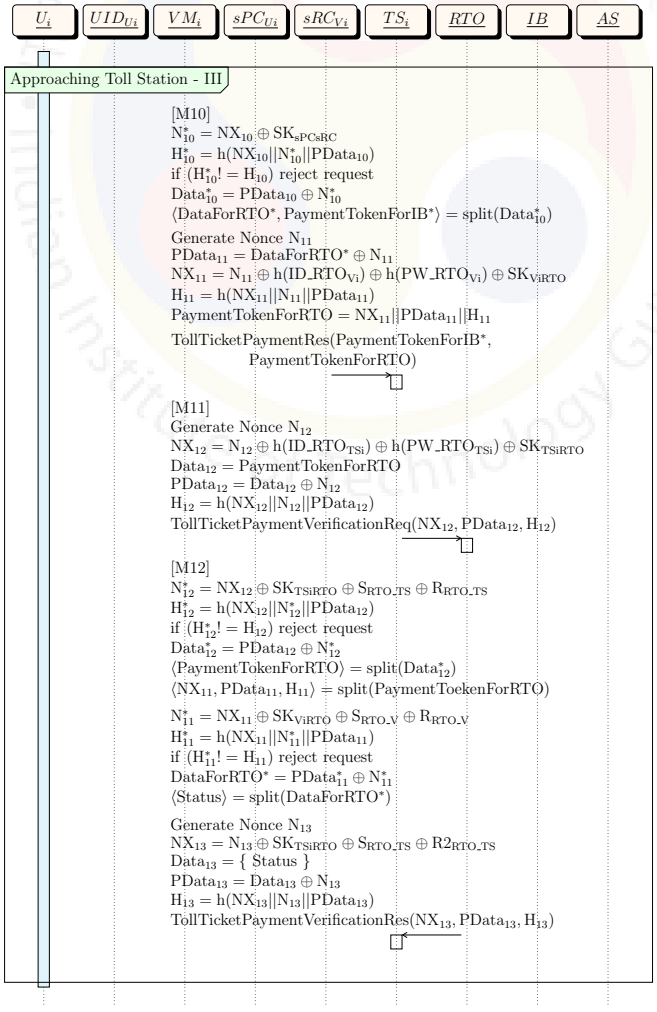


Figure 6.14: Payment Phase (Part - III.I)

Figure 6.15: Payment Phase (Part - III.II)

H_E using the nonce, N_E and a secret symmetric key SK_{E1_E2} shared between E1 and E2, hash of identifier $h(ID_{E1})$ and hash of password $h(PW_{E1})$. These three parameters are built in such a way that even if these three parameters are known to an attacker, he cannot derive session key, password or nonce out of it. These three parameters are transferred to receiver entity. When receiving entity receives these parameters, it computes H^*_E using received parameters and two secrets S_{E2} and R_{E2}.

Only if received H_E and recomputed H_E^* matches, the request is taken forward. This ensures that the data is send by one of the trusted entity and hence can be trusted. Further to this, each data object $Data_E$ contains in it the name of its sender entity which ensures sender authentication. In this way, all participants of the proposed scheme ensures that data is coming from some trusted entity and the trusted data received contains in it the identity of the sender. Sender is sure that only a genuine entity (having a valid session key) can decipher the data and receiver is sure that only a genuine entity (having a valid session key) can encipher the data. Moreover, the data transferred contains in it the information about its sender. Hence this ensures sender (or receiver) that it is communicating with a genuine entity.

Anonymity

When an entity wants to send data to another entity, it never sends its identity in plaintext. Identity of the sender is retrieved by deciphering $PData_E$. Moreover, since $PData_E$ is enciphered using a nonce, even if same data is to be send again, a different $PData_{E_i}$ is send for that data. Hence even if an attacker intercepts messages transferred between entities, he cannot deduce identity of the sender or the receiver.

Privacy

Since data object is enciphered using the nonce and nonce itself is enciphered using the session key and password, even if an attacker intercepts messages transferred between entities, he cannot deduce the content and the intention of the message. Hence the proposed scheme ensures privacy also.

Resistance to Impersonating Attacks

In impersonating attacks, an attacker impersonates as a genuine entity and tries to invade the system. In the proposed scheme, only an entity having both valid session key and valid password can create valid NX_{E_i} which is used by receiver entity along

with its own session key and password to recompute the nonce. To impersonate a genuine entity, an attacker needs to know both the session key and the password of some genuine entity which are never transferred across the network. Hence the proposed scheme is also resistance to impersonating attacks.

Resistance to Replay Attacks

In replay attack, an attacker intercepts previous communication messages and replays the same to pass the verification process of the receiver entity. Since nonce is used to populate all three parameters (NX_{E_i}, $PData_{E_i}$ and H_{E_i}) in communication messages, none of the message can be replayed by an attacker. Hence the proposed scheme is resistance to replay attack as well.

Resistance to Man-In-The-Middle Attacks

In man-in-the-middle attack, an attacker intercepts communication message and copy or modify it in such a way that he appears as a genuine entity to the receiver entity. In the proposed scheme, any change in the communication message will fail verification process at the receiver entity. Moreover, without a valid session key and password, none of the parameter can be deciphered. Hence the proposed scheme is also resistant to man-in-the-middle attack.

6.3.4 Formal Security Analysis Using BAN Logic

This section presents formal security analysis of the proposed protocol using Burrows-Abadi-Needham (BAN) logic [93]. BAN logic is a well-known model used to find beliefs of participants in a cryptographic protocol. The model assumes that all messages are communicated over public channels and an attacker can see, modify, compose and replay messages. The model also assumes that an attacker can decipher messages if he has a valid decryption key. Some of the fundamental operators used in BAN logic are defined in Table 6.2. An extension to BAN logic is required to analyse the proposed model 6.3.

Operator Usage	Description
$P \models X$	P believes statement X
$P \lhd X$	P sees statement X
$P \longmapsto X$	P controls X
$\#(X)$	Message X is fresh
$P \overset{K}{\leftrightarrow} Q$	P and Q share key K
$\overset{K}{\mapsto} P$	P has K as its public key
$P \overset{X}{\rightleftharpoons} Q$	Formula X is a secret known only to P and Q
$\{X\}_K$	Formula X is encrypted using K
$\langle X \rangle_Y$	Formula X is combined with formula Y

Table 6.2: Fundamental BAN operators

Operator Usage	Description
$P \models X \Longleftrightarrow Y$	P believes statement X is same as Y
$P \models P \overset{Y_K}{\longleftarrow} Q$	P believes that P has transferred statement Y to Q securely by combining secret K shared between P and Q

Table 6.3: Extended BAN operators

Rules of Inference

[R1:] *Message meaning rules* concern the interpretation of messages. They all derive beliefs about the origin of messages.

For shared secrets, the inference rule is

$$\frac{P \models Q \overset{Y}{\rightleftharpoons} P,\ P \lhd \langle X \rangle_Y}{P \models Q \rhd X} \tag{6.1}$$

That is, if P believes that the secret Y is shared with Q and sees $\langle X \rangle_Y$, then P believes that Q once said X.

[R2:] The *nonce-verification* rule expresses the check that a message is recent, and hence, that the sender still believes in it:

$$\frac{P \models \#(X),\ P \models Q \rhd X}{P \models Q \models X} \tag{6.2}$$

That is, if P believes that X could have been uttered only recently and that Q once said X, then P believes that Q believes X.

[R3:] The *jurisdiction* rule states that if P believes that Q has jurisdiction over X, then P trusts Q on the truth of X:

$$\frac{\mathrm{P} \models \mathrm{Q} \Rightarrow \mathrm{X}, \mathrm{P} \models \mathrm{Q} \models \mathrm{X}}{\mathrm{P} \models \mathrm{X}} \tag{6.3}$$

[R4:] The *seeing* rule states that if a principal sees a formula, then he also sees its components, provided he knows the necessary keys:

$$\frac{\mathrm{P} \lhd (\mathrm{X}, \mathrm{Y})}{\mathrm{P} \lhd \mathrm{X}}, \quad \frac{\mathrm{P} \lhd \langle \mathrm{X} \rangle_{\mathrm{Y}}}{\mathrm{P} \lhd \mathrm{X}}, \quad \frac{\mathrm{P} \models \mathrm{Q} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{P}(,)\mathrm{P} \lhd \{\mathrm{X}\}_{\mathrm{K}}}{\mathrm{P} \lhd \mathrm{X}},$$

$$\frac{\mathrm{P} \models \overset{\mathrm{K}}{\mapsto} \mathrm{P}, \mathrm{P} \lhd \{\mathrm{X}\}_{\mathrm{K}}}{\mathrm{P} \lhd \mathrm{X}}, \quad \frac{\mathrm{P} \models \overset{\mathrm{K}}{\mapsto} \mathrm{P}, \mathrm{P} \lhd \{\mathrm{X}\}_{\mathrm{K}^{-1}}}{\mathrm{P} \lhd \mathrm{X}}. \tag{6.4}$$

Note that if P sees X and P sees Y it does NOT follow that P sees (X, Y) since that means that X and Y were uttered at the same time.

[R5:] The *fresh* rule states that if one part of the formula is fresh, then the entire formula must be fresh.

$$\frac{\mathrm{P} \models \#(\mathrm{X})}{\mathrm{P} \models \#(\mathrm{X}, \mathrm{Y})}. \tag{6.5}$$

[R6:] The *belief* rule states that if P believes one part of the formula, then it also believe part of the formula.

$$\frac{\mathrm{P} \models (\mathrm{X}, \mathrm{Y})}{\mathrm{P} \models (\mathrm{X})}. \tag{6.6}$$

Extended Rules of Inference

[R7:] If P believes that K is a shared secret between P and Q, P sees a nonce N encrypted using K, P sees a hash H, P sees X, P finds N to be fresh and P finds H is same as $h(\{N\}_K||\{\{N\}_K\}||X)$, then P believes that N and X are sent by Q and N is shared only between P and Q.

$$\frac{\begin{array}{llllll} \mathrm{P} & \models & \mathrm{P} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{Q}, & \mathrm{P} & \lhd & \langle \mathrm{N} \rangle_{\mathrm{K}}, \quad \mathrm{P} \lhd \mathrm{H}, \\ \mathrm{P} & \lhd & \mathrm{X}, & \mathrm{P} & \models & \#\mathrm{N}, \\ \mathrm{P} & \models & \mathrm{H} \iff \mathrm{h}(\langle \mathrm{N} \rangle_{\mathrm{K}} \,||\, \langle \langle \mathrm{N} \rangle_{\mathrm{K}} \rangle_{\mathrm{K}} \,||\, \mathrm{X}) & & & \end{array}}{\mathrm{P} \models \mathrm{Q} \rhd \mathrm{N}, \quad \mathrm{P} \models \mathrm{Q} \rhd \mathrm{X}, \quad \mathrm{P} \models \mathrm{P} \overset{\mathrm{N}}{\leftrightarrow} \mathrm{Q}} \tag{6.7}$$

[R8:] If P believes that K is a shared secret between P and Q, believes that K is fresh, sees Y combined with K, then it believes that Q has sent Y and Y is secured from intruder with the help of K, which essentially means that Y is not modified, observed or replayed by an attacker after it was sent by Q.

$$\frac{\mathrm{P} \models \mathrm{P} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{Q}, \quad \mathrm{P} \models \#\mathrm{K}, \quad \mathrm{P} \lhd \langle \mathrm{Y} \rangle_{\mathrm{K}},}{\mathrm{P} \models \mathrm{Q} \rhd \mathrm{Y}, \quad \mathrm{P} \models \mathrm{Q} \overset{\mathrm{Y_K}}{\longleftarrow} \mathrm{P},} \tag{6.8}$$

Assumptions

The protocol makes several assumptions. The assumptions relevant for the discussion of this chapter are listed below.

[A1-A8:] The protocol makes several assumptions about symmetric keys. For example, $\mathrm{V_i}$ belives that $\mathrm{SK_{ViRTO}}$ is a secret shared only between $\mathrm{V_i}$ and RTO (A1). Similar to this, other entities also make assumptions. These assumptions are indicated below.

$$
\begin{array}{llll}
\mathrm{sRC_{Vi}} & \models & \mathrm{sRC_{Vi}} & \mathrm{P} \overset{\mathrm{SK_{ViRTO}}}{\rightleftharpoons} \mathrm{RTO} \\
\mathrm{RTO} & \models & \mathrm{sRC_{Vi}} & \overset{\mathrm{SK_{ViRTO}}}{\rightleftharpoons} \mathrm{RTO} \\
\mathrm{TS_i} & \models & \mathrm{TS_i} & \overset{\mathrm{SK_{TSiRTO}}}{\rightleftharpoons} \mathrm{RTO} \\
\mathrm{RTO} & \models & \mathrm{TS_i} & \overset{\mathrm{SK_{TSiRTO}}}{\rightleftharpoons} \mathrm{RTO} \\
\mathrm{sPC_i} & \models & \mathrm{sPC_i} & \overset{\mathrm{SK_{sPCsRC}}}{\rightleftharpoons} \mathrm{sRC_i} \\
\mathrm{sRC_i} & \models & \mathrm{sPC_i} & \overset{\mathrm{SK_{sPCsRC}}}{\rightleftharpoons} \mathrm{sRC_i} \\
\mathrm{sPC_i} & \models & \mathrm{sPC_i} & \overset{\mathrm{SK_{UiIB}}}{\rightleftharpoons} \mathrm{IB_i} \\
\mathrm{IB_i} & \models & \mathrm{sPC_i} & \overset{\mathrm{SK_{UiIB}}}{\rightleftharpoons} \mathrm{IB_i}
\end{array} \tag{6.9}
$$

[A9:] It is assumed that receiving parties have verified the validity of H_i.

$$
\begin{array}{llll}
\mathrm{RTO} & \models & \mathrm{H_5} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_5} \rangle_{\mathrm{SK_{TSiRTO}}} || \langle \langle \mathrm{N_5} \rangle_{\mathrm{SK_{TSiRTO}}} \rangle_{\mathrm{SK_{TSiRTO}}} || \mathrm{PData_5}) \\
\mathrm{TS_i} & \models & \mathrm{H_7} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_7} \rangle_{\mathrm{SK_{TSiRTO}}} || \langle \langle \mathrm{N_7} \rangle_{\mathrm{SK_{TSiRTO}}} \rangle_{\mathrm{SK_{TSiRTO}}} || \mathrm{PData_7}) \\
\mathrm{sRC_{Vi}} & \models & \mathrm{H_4} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_4} \rangle_{\mathrm{SK_{ViRTO}}} || \langle \langle \mathrm{N_4} \rangle_{\mathrm{SK_{ViRTO}}} \rangle_{\mathrm{SK_{ViRTO}}} || \mathrm{PData_4}) \\
\mathrm{sPC_{Ui}} & \models & \mathrm{H_8} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_8} \rangle_{\mathrm{SK_{sPCsRC}}} || \langle \langle \mathrm{N_8} \rangle_{\mathrm{SK_{sPCsRC}}} \rangle_{\mathrm{SK_{sPCsRC}}} || \mathrm{PData_8}) \\
\mathrm{sRC_{Vi}} & \models & \mathrm{H_{10}} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_{10}} \rangle_{\mathrm{SK_{sPCsRC}}} || \langle \langle \mathrm{N_{10}} \rangle_{\mathrm{SK_{sPCsRC}}} \rangle_{\mathrm{SK_{sPCsRC}}} || \mathrm{PData_{10}}) \\
\mathrm{RTO} & \models & \mathrm{H_{12}} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_{12}} \rangle_{\mathrm{SK_{TSiRTO}}} || \langle \langle \mathrm{N_{12}} \rangle_{\mathrm{SK_{TSiRTO}}} \rangle_{\mathrm{SK_{TSiRTO}}} || \mathrm{PData_{12}}) \\
\mathrm{RTO} & \models & \mathrm{H_{11}} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_{11}} \rangle_{\mathrm{SK_{ViRTO}}} || \langle \langle \mathrm{N_{11}} \rangle_{\mathrm{SK_{ViRTO}}} \rangle_{\mathrm{SK_{ViRTO}}} || \mathrm{PData_{11}}) \\
\mathrm{RTO} & \models & \mathrm{H_9} & \Longleftrightarrow \mathrm{h}(\langle \mathrm{N_9} \rangle_{\mathrm{SK_{ViIB}}} || \langle \langle \mathrm{N_9} \rangle_{\mathrm{SK_{ViIB}}} \rangle_{\mathrm{SK_{ViIB}}} || \mathrm{PData_9})
\end{array}
$$

[A10:] It is assumed that the receiving parties have decipherd NX_i and found respective N_i to be fresh.

Goals to be achieved.

Following are the goals which are envisaged to be achieved by the proposed model.

[G1-G8:] One of the goal statement is that RTO should establish that $\mathrm{Data_5}$ is indeed sent by $\mathrm{TS_i}$. Similar to this other goal statements can also be listed.

[G9-G16:] One of the goal statement is that RTO should establish that $\mathrm{Data_5}$ sent by $\mathrm{TS_i}$ to RTO is secured (using $\mathrm{N_5}$) and is not modified, observed or

$$
\begin{array}{llllll}
\mathrm{RTO} & \models & \#\mathrm{N_5}, & \mathrm{TS_i} & \models & \#\mathrm{N_7}, \\
\mathrm{sRC_{Vi}} & \models & \#\mathrm{N_4}, & \mathrm{sPC_{Vi}} & \models & \#\mathrm{N_8}, \\
\mathrm{sRC_{Vi}} & \models & \#\mathrm{N_{10}}, & \mathrm{RTO} & \models & \#\mathrm{N_{12}}, \\
\mathrm{RTO} & \models & \mathrm{N_{11}}, & \mathrm{IB_i} & \models & \#\mathrm{N_9}
\end{array}
$$

$$\begin{array}{lllll}
RTO & \models & TS_i & \lhd & Data_5, \\
TS_i & \models & RTO & \lhd & Data_7, \\
sRC_{Vi} & \models & RTO & \lhd & Data_4, \\
sPC_{Ui} & \models & sRC_{Vi} & \lhd & Data_8, \\
sRC_{Vi} & \models & sPC_{Ui} & \lhd & Data_{10}, \\
RTO & \models & TS_i & \lhd & Data_{12}, \\
RTO & \models & sRC_{Vi} & \lhd & Data_{11}, \\
IB_i & \models & sPC_{Ui} & \lhd & Data_9
\end{array} \tag{6.10}$$

$$\begin{array}{lllll}
RTO & \models & TS_i & \overset{\langle Data_5 \rangle_{N_5}}{\longrightarrow} & RTO \\
TS_i & \models & RTO & \overset{\langle Data_7 \rangle_{N_7}}{\longrightarrow} & TS_i \\
sRC_{Vi} & \models & RTO & \overset{\langle Data_4 \rangle_{N_4}}{\longrightarrow} & sRC_{Vi} \\
sPC_{Ui} & \models & sRC_{Vi} & \overset{\langle Data_8 \rangle_{N_8}}{\longrightarrow} & sPC_{Ui} \\
sRC_{Vi} & \models & sPC_{Ui} & \overset{\langle Data_{10} \rangle_{N_{10}}}{\longrightarrow} & sRC_{Vi} \\
RTO & \models & TS_i & \overset{\langle Data_{12} \rangle_{N_{12}}}{\longrightarrow} & RTO \\
RTO & \models & sRC_{Vi} & \overset{\langle Data_{11} \rangle_{N_{11}}}{\longrightarrow} & RTO \\
IB_i & \models & sPC_{Ui} & \overset{\langle Data_9 \rangle_{N_9}}{\longrightarrow} & IB_i
\end{array} \tag{6.11}$$

replayed by an intruder after it was sent by TS_i. Similar to this other goal statements can also be listed.

Idealization

BAN idealization of communication messages in communication phase is shown in table 6.4.

Analysis

[P1:] Using message M1, assumptions A1, A5, and rules R7, R8, it can be deduced that A_i believes S_i has send data $Data_{S_i}$.

Using M3,

M1	sRC_{Vi}	$\lhd$	ID_RTO_{TSi}
M2	TS_i	$\lhd$	$NX_4, PData_4, H_4$
M3	RTO	$\lhd$	$NX_5, PData_5, H_5$
M4	TS_i	$\lhd$	$NX_7, PData_7, H_7$
M5	sRC_{Vi}	$\lhd$	$NX_4, PData_4, H_4$
M6	sPC_{Ui}	$\lhd$	$NX_8, PData_8, H_8$
M7	U_i	$\lhd$	"Consent_And_PW_Request"
M8	sPC_{Ui}	$\lhd$	PW
M9	sRC_{Vi}	$\lhd$	$NX_{10}, PData_{10}, H_{10}$
M10	TS_i	$\lhd$	PaymentTokenForIB,
		$\lhd$	PaymentTokenForRTO
M11	RTO	$\lhd$	$NX_{12}, PData_{12}, H_{12}$
M12	TS_i	$\lhd$	$NX_{13}, PData_{13}, H_{13}$
M13	TS_i	$\lhd$	PaymentTokenForIB

Table 6.4: BAN Idealization

$$\begin{aligned} RTO \quad &\lhd \quad NX_5, PData_5, H_5 \\ &\lhd \quad \langle N_5 \rangle_{SK_{TSiRTO}}, \ Data_5, \\ &\quad h(\ \langle N_5 \rangle_{SK_{TSiRTO}} || \\ &\qquad \langle \langle N_5 \rangle_{SK_{TSiRTO}} \rangle_{SK_{TSiRTO}}) \end{aligned}$$

Using A10, A11 and R7,

$$RTO \quad \models \quad TS_i \rhd N_5 \tag{I1}$$

$$RTO \quad \models \quad TS_i \rhd \langle Data_5 \rangle_{N_5} \tag{I2}$$

$$RTO \quad \models \quad TS_i \overset{N_5}{\leftrightarrow} RTO \tag{I3}$$

Using M3, I3, A11, I2 and R8,

$$RTO \quad \models \quad TS_i \rhd Data_5 \tag{G1 : Proved}$$

This proves that goal G1 holds true.

[P2-P8:] Goals G2 to *G*8 can be proven similar to proof P1 for G1. (G2 − G8 : Proved)

[P9:]

$$\text{RTO} \models \text{TS}_\text{i} \overset{\text{N}_5}{\leftrightarrow} \text{RTO}$$

$$\text{RTO} \models \#\text{N}_5$$

$$\text{RTO} \models \text{TS}_\text{i} \triangleright \langle \text{Data}_5 \rangle_{\text{N}_5}$$

Using R8,

$$\text{RTO} \models \text{TS}_\text{i} \overset{\langle \text{Data}_5 \rangle_{\text{N}_5}}{\longrightarrow} \text{RTO} \qquad \text{(G9 : Proved)}$$

This proves that goal G9 holds true.

[P10-P16:] Goals G10 to G16 can be proven similar to proof P9 for G9.

6.3.5 Formal Security Analysis Using ProVerif

This section presents formal analysis of proposed protocol using ProVerif [130]. ProVerif is a protocol verifier tool based on applied pi calculus [131]. This tool can be used to prove secrecy and authenticity properties of cryptographic protocols. In ProVerif, an attacker is assumed to have "Dolev-Yao" capabilities which means an attacker has complete control of public communication channels and can read, modify, delete and inject messages but cannot break cryptography.

The protocol is modelled parallel execution of nine processes, *user* indicating U_i, *uid* indicating UID_{Ui}, *vm* indicating vehicle manufacturer VM_i, *spc* indicating smart payment card sPC_{Ui}, *src* indicating sRC_{Vi}, *ts* indicating TS_i, *rto* indicating RTO, *ib* indicating IB_i, and *as* indicating AS. Security of shared secret symmetric keys, passwords and identities is formalized by the following queries. ProVerif version 2.00 is used to run the model and all queries were proved to hold true. Authentication of entities is formalized by following queries.

6.4 Summary

This chapter presents a mechanism to improve privacy in an automated toll tax collection service by ensuring security, privacy and anonymity in vehicle to infras-

query attacker (id_as_ui).
query attacker (pw_as_ui).
query attacker (id_ib_ui).
query attacker (pw_ib_ui).
query attacker (id_rto_vmi).
query attacker (pw_rto_vmi).
query attacker (pw_rto_tsi).
query attacker (s_as).
query attacker (r_as).
query attacker (sk_ui_as).
query attacker (s_ib).
query attacker (r_ib).
query attacker (sk_ui_ib).
query attacker (s_ib).
query attacker (r_ib).
query attacker (sk_ui_ib).
query attacker (s1_rto).
query attacker (r1_rto).
query attacker (sk_vmi_rto).
query attacker (s2_rto).
query attacker (r2_rto).
query attacker (sk_tsi_rto).
query attacker ($sk_s pc_s rc$).

$$\text{inj-event}(\text{user\_end}(\text{id\_as\_ui})) \Longrightarrow \text{inj} - \text{event}(\text{user\_begin}(\text{id\_as\_ui})).$$
$$\text{inj-event}(\text{uid\_end}(\text{id\_as\_ui})) \Longrightarrow \text{inj} - \text{event}(\text{uid\_begin}(\text{id\_as\_ui})).$$
$$\text{inj-event}(\text{vm\_end}(\text{id\_rto\_vmi})) \Longrightarrow \text{inj} - \text{event}(\text{vm\_begin}(\text{id\_rto\_vmi})).$$
$$\text{inj-event}(\text{spc\_end}(\text{id\_ib\_ui})) \Longrightarrow \text{inj} - \text{event}(\text{spc\_begin}(\text{id\_ib\_ui})).$$
$$\text{inj-event}(\text{src\_end}(\text{id\_rto\_vmi}) \Longrightarrow \text{inj} - \text{event}(\text{src\_begin}(\text{id\_rto\_vmi})).$$
$$\text{inj-event}(\text{ts\_end}(\text{id\_rto\_tsi})) \Longrightarrow \text{inj} - \text{event}(\text{ts\_begin}(\text{id\_rto\_tsi})).$$
$$\text{inj-event}(\text{rto\_end}(\text{id\_rto\_tsi})) \Longrightarrow \text{inj} - \text{event}(\text{rto\_begin}(\text{id\_rto\_tsi})).$$
$$\text{inj-event}(\text{ib\_end}(\text{id\_ib\_ui})) \Longrightarrow \text{inj} - \text{event}(\text{ib\_begin}(\text{id\_ib\_ui})).$$
$$\text{inj-event}(\text{as\_end}(\text{id\_as\_ui})) \Longrightarrow \text{inj} - \text{event}(\text{as\_begin}(\text{id\_as\_ui})).$$

tructure communication. In the proposed scheme, the vehicle does not disclose its identity to the toll station and yet the vehicle is issued a toll ticket generated directly from the RTO. This enables transparency of actions, privacy of information and anonymity of identity and still achieves the desired level of functionality. The next chapter explores privacy-related requirements and improvement in another Aadhaar-based system for registered devices. Registered devices are special devices used to capture and store biometric.

Chapter 7

Privacy Enhanced Registered Devices

The previous chapter presents a mechanism to improve privacy in an automated toll tax collection service. This chapter explores privacy-related requirements and improvement in Aadhaar-based system for registered devices. Registered devices are devices used to capture and store biometric.

7.1 Introduction

Each time a resident needs to use an Aadhaar-based service, he needs to authenticate himself by providing his biometric (or a One Time Password (OTP) for low risk activity). Biometric is a sensitive data and an utmost care should be taken to ensure security of devices used to store and transmit biometric. UIDAI introduced *Registered Devices* [132] with three major requirements. First is that every device must have a unique identifier for traceability, analytics and fraud management. Second is that the device uses its private key to sign biometric within the device. This is to eliminate the use of stored biometrics. Third is that the service provided by

the device provider must be certified by UIDAI. UIDAI acknowledges *public devices* also but mandates that necessary security measures must be taken to ensure security of devices. Registered devices are categorized in two levels (L0 and L1) based on their compliance level. In L0 compliance devices, signing and encryption of biometric is done within the software in host operating system. In this case, software should ensure the security of private keys from other users and applications in the system. In L1 compliance devices, signing and encryption of biometric is done within the secure device storage area. In this case, the key is secured from other users and applications. An L0 device is identified by idHash = SHA256(DeviceSerialNo) and an L1 device is identified by idHash = DeviceSerialNo||$\{\text{DeviceSerialNo; Timestamp}\}_{\text{CI}_\text{k}}$, where CI_k is the Chip Identity Certificate stored in secure storage area of the device. Each device provider has a unique key called device provider private key and each device has a unique key called device private key. The corresponding public keys are signed by UIDAI and the device provider respectively.

Each device provider provides a registered device service which provides two APIs, namely, capture and device_info. When an application needs to capture biometric of a person, the device captures required biometric records of the person using capture API and sign the same to obtain $\text{B}_{\text{Si}} = \{\text{SHA256}(\text{biorecord}_\text{i})|$ timestamp|| UniqueDe viceCode$\}_{\text{D}_\text{PRK}}$, where D_PRK is the device private key and i ranges from one to number of biometric records. Now, a Personal Identity Data (PID) block [133] is created which includes device identity (idHash), biometric records (B_{Si}), device provider identifier, registered device service version and device model identifier. device_info is used to obtain device specific information. Device encrypts the PID block using a dynamic session key, which is further encrypted with UIDAI public key. The encrypted PID block is send to the application.

At present, registered devices are supposed to be connected locally to the system and are primarily designed to handle biometric data. Although at present, this model may be suffice, with the proliferation of connected devices and online services,

registered devices may soon become ubiquitous, required to operate remotely and to process other sensitive personal data as well. In a ubiquitous world of registered devices, an application may want to query and use a valid registered device having a specific set of attributes rather than a registered device having a specific random string of serial number or a model number. Since identity of the device may be correlated with identify of its owner, owner of the device may not want to disclose identity of the device to protect his privacy. Owner may just want to let the device be recognized as a valid registered device having a certain set of attributes. Since present model of registered devices is based on PKI infrastructure, it has some inherent limitations such as it attests device identity to a message and not to the device attributes. Furthermore, the present model of registered devices can be improved in providing attribute-based discovery and usage of the device while still maintaining the device privacy.

In Attribute-based signature [94], signer is represented by a set of attributes rather than his identity and the signature assures that the signer holds a specific set of attributes. Although, attribute-based signature seems a natural choice here, the scheme is still not used widely and a careful and efficient construction is still one of the major issues. Moreover, during usage of the device, multiple authorities may participate in assigning attributes to the device. For example, device attributes may be assigned by manufacturer, operational attributes may be assigned by hosting agency, context attributes may be assigned by hosting service, usage attributes may be assigned by operations team and the user himself, etc.

This chapter presents a scheme to implement privacy enhanced fine-grained access control devices in which multiple authorities may participate to arrive at an attribute-based token which can be used to assure the validity and the possession of a specific set of attributes. The token can be reused till it expires and is collusion resistant.

Rest of this chapter is organized as follows. Section 7.2 presents some of the

related work, section 7.3 presents our proposed model, section 7.4 presents an informal security analysis, section 7.5 presents performance analysis and section 7.6 presents summary of this chapter.

7.2 Related Work

Public Key Infrastructure (PKI) was introduced by Diffie and Hellman in 1977 [95]. Most of the traditional secure systems are built using PKI. In PKI, every subject has a private key and a corresponding public key. A trusted entity called Certificate Authority certifies public key of the subject and issues him a Digital Signature Certificate (DSC). PKI has an additional overhead of management of DSCs.

Identity-based encryption (IBE) was introduced by Shamir in 1984 [96] at a broad level without details on its construction. In year 2001, Boneh and Franklin [97] introduced a possible construction of the same using bilinear pairing. In IBE, each subject has a well-defined identity. A trusted entity known as Private Key Generator (PKG) hosts a master public key and generates a private key for a given identity. The corresponding public key can be derived from the identity and the master public key. IBE has a benefit over PKI in that there is no overhead of certificate management and public key of a subject can be derived directly from identity of the subject.

Attribute-based encryption (ABE) can be divided in two categories, Key Policy Attribute-based Encryption (KP-ABE) and Ciphertext Policy Attribute-based Encryption (CP-ABE). The first was introduced by Sahai et. al [79] and the second was introduced by Benthencourt et. al [81]. In KP-ABE, private key is linked with the access policy and ciphertext is linked with a set of attributes. A receiver can decrypt a ciphertext only if access policy in his private key satisfies attributes in the ciphertext. In CP-ABE, private key is linked with a set of attributes and ciphertext is linked with an access policy. A receiver can decrypt a ciphertext only if attributes in his private key satisfies access policy in the ciphertext.

In Attribute-based Signature (ABS), a signature is based on signer's attributes and implies possession of certain attributes by the signer. ABS facilitates the signer to sign a document proving possession of certain attributes without even revealing his attributes. Guo et al. [94] proposed an initial ABS scheme in which they used strong extended Diffie Hellman assumption to prove their claims. Later Tan et al. [99] presented a weakness in Guo's scheme and explained that the scheme is weak for partial key replacement attacks. Later, Maji et al. [100] proposed a scheme which can use different kinds of gates such as AND gates, OR gates or threshold gates.

7.3 Our Construction

In this section, we describe the proposed construction of privacy enhanced registered devices for fine-grained access control using attribute-based signature.

An attribute is represented by a descriptive string and has an associated private key and a corresponding public key. A private key can be any integer and a public key is a point on the chosen group. The proposed scheme introduces two entities. First is *Attribute Management Authority of India (AMAI)* which manages the whole set of device attributes and assigns a range of attributes to individual agencies to manage the range further. Second is *Attribute Service Provider (ATSP)*, which manages its assigned range of attributes by choosing private keys for each attribute in the range. Since during usage of the device, attributes to a device can be assigned by multiple entities; there can be multiple ATSPs such as device manufacturer, device firmware provider, host software, host agencies, user itself, etc. However, the scheme assumes only one AMAI.

7.3.1 Attribute Management Authority of India (AMAI)

AMAI executes a setup(k) procedure to initialize its parameters. k is used to choose two suitable cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order p where p is a prime number. The groups are chosen such that the discrete logarithm problem is hard on them. AMAI chooses generator elements from each group. Let g_1 and g_2 are the generators of $\mathbb{G}_1$ and g_2 respectively. Now, the AMAI choses a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ such that the bilinear Diffie Hellman problem is hard on it. Now, from the universe of attributes $\mathbb{U} = \{1, 2, ...n\}$, AMAI delegates management of a specific subset of attributes to a specific cateogry of ATSPs. For example, AMAI can assign attributes $\{1 - 50\}$ to itself, $\{51 - 100\}$ to manufacturers, $\{101 - 150\}$ to host agencies, etc. These attributes are represented by $\mathbb{A}_{\text{AMAI}}$, $\mathbb{A}_{\text{ATSP}_1}$, and $\mathbb{A}_{\text{ATSP}_2}$ and so on. User is also given an ownership of some of the attributes. These attributes may represent his consent, the intended purpose of consuming his data, the expected user of his data, etc.

AMAI generates random numbers $\gamma \in_R \mathbb{Z}_p$ and $t_i \in_r \mathbb{Z}_p$ for each attribute $i \in \mathbb{A}_{\text{AMAI}}$ and computes its private key SK, derives the public key MPK and a master public key MPK.

$$\begin{aligned} \text{SK} &= \{\gamma, \{t_i\}_{\forall i \in \mathbb{A}_{\text{AMAI}}}\} \\ \text{PK} &= \{g^{\gamma}, \{g^{\gamma}\}_{\text{PVTA}}, \{T_i, \{T_i\}_{\text{PVTA}}\}_{\forall i \in \mathbb{A}_{\text{AMAI}}}\} \\ \text{MPK} &= \{\mathbb{A}_{\text{AMAI}}, \mathbb{A}_{\text{ATSP}_1}, \mathbb{A}_{\text{ATSP}_2}, \mathbb{A}_{\text{ATSP}_i}, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, p\} \end{aligned} \tag{7.1}$$

where $T_i = g^{t_i}$ and $\{T_i\}_{\text{PVTA}}$ is T_i signed by another private key PVTA of AMAI.

7.3.2 Attribute Service Providers (ATSP)

All ATSPs need to register with AMAI. ATSP_i generates random numbers $\alpha \in_R \mathbb{Z}_p$ and $t_i \in_R \mathbb{Z}_p$ for each attribute $i \in \mathbb{A}_{\text{ATSP}_i}$, derives public keys $T_i = g^{t_i}$ and sends

them to AMAI for attestation. AMAI verifies validity of the $ATSP_i$, signs the received public keys using its private key PVTA and sends them back to $ATSP_i$. $ATSP_i$ now has its private key ASK_i and corresponding public key APK_i.

$$\begin{aligned} ASK_i &= \{\alpha, \{t_i\}_{\forall i \in \mathbb{A}_{ATSP_i}}\} \\ APK_i &= \{g^{\alpha}, \{g^{\alpha}\}_{PVTAA}, \{T_i, \{T_i\}_{PVTAA}\}_{\forall i \in \mathbb{A}_{ATSP_i}}\} \end{aligned} \tag{7.2}$$

7.3.3 Attribute-based Private Key

During usage of the device, a device is assigned attributes from multiple ATSPs such as the manufacturer, the firmware agency, the host agency, the user, etc. Each ATSP creates an access subtree representing device attributes it has assigned to the device. These access subtrees are combined to form a common access tree. All attributes from a single ATSP are assumed to be in one access subtree. Refer figure 7.1 for an illustration of an access tree $\mathcal{T}$.

A typical procedure for a device with identifier ID_i to generate its attribute-based private key against an access tree $\mathcal{T}_j$ is illustrated in algorithm 7.1. IDT_{ij} represents ID_i and $\mathcal{T}_j$ collectively. The device calls PullKeyAll(IDT_{ij}, K) API (refer algorithm 7.3) of AMAI to retrieve attribute-based private key components from each participating ATSP by calling PullKeyAll(IDT_{ij}, K) API (refer algorithm 7.2) of each participating ATSP. Two helper functions GetATSP($\mathcal{T}$) and genParitalKey(IDT_{ij}, K, r) are used in these algorithms. GetATSP($\mathcal{T}$) returns a set of ATSPs which contributed in assigning some attributes in $\mathcal{T}$. $L(\mathcal{T}) = \text{leaves}(T) \cap \mathbb{A}_{ATSP_i}$.

ATSPs use genParitalKey(IDT_{ij}, K, α) to compute their part of attribute-based private key. This procedure works as follows. Let λ represents a set of attributes assigned by $ATSP_i$ to device with identity ID_i. For root node R, a polynomial q_R is chosen with degree $d_R = k_R - 1$, where k_R is the threshold value of the root node. A random number α is assigned to $q_R(0)$ such that $q_R(0) = \alpha$ and rest of the d_R points are chosen randomly to define the polynomial q_R completely. Let k_x represents the threshold value of node x. Now, for each child node x of root node, a polynomial q_x

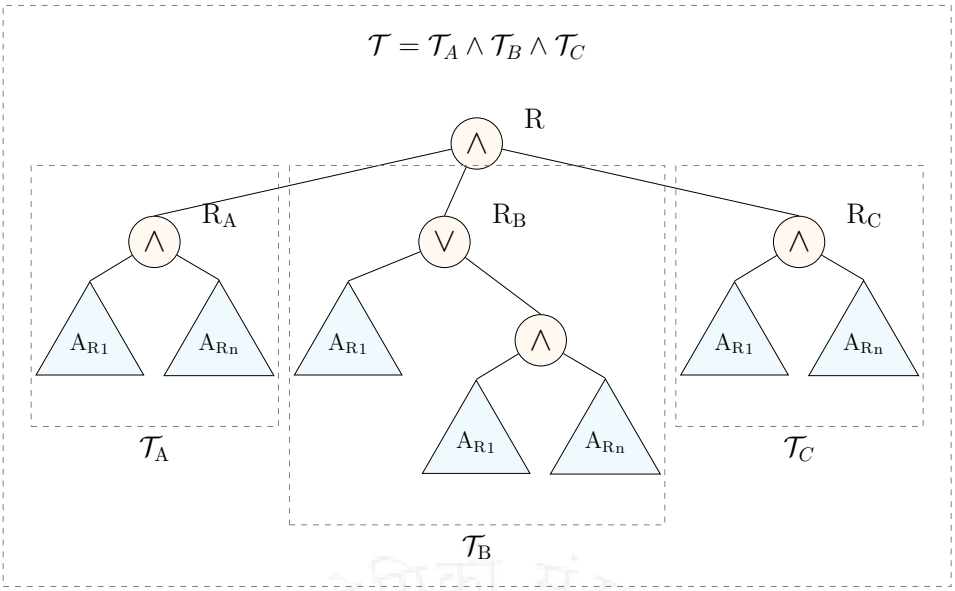


Figure 7.1: Example of an access policy tree

with degree d_x which is equal to $k_x - 1$ is chosen. $q_{parent(x)}(index(x))$ is assigned to $q_x(0)$ such that $q_x(0) = q_{parent(x)}(index(x))$ and other d_x points are chosen randomly to define the polynomial q_x completely. The same process is used to generate polynomial for each node (including the leaves). Now, for each leaf node x, $M_{1_x} = K^{q_x(0)/t_i}$ is computed where $i = att(x)$, $x \in \lambda$ and K is a group element. Attribute-based private key assigned by $ATSP_i$ to the device is $\langle M_{1_x} = K^{q_x(0)/t_i}, M_2 = K^{\alpha} \rangle$. Each participating ATSP provides its part of attribute-based private key in a similar way.

7.3.4 Token Generation

Generation of private key is a costly operation since it involves computation and retrieval from multiple participating agencies and hence doing so for each request may not be very efficient. For better efficiency, a reusable token can be used which contains in it the private key and other parameters such as token expiry date from all participating ATSP $\in$ GetATSP($\mathcal{T}$) where GetATSP($\mathcal{T}$) represents all ATSPs which has some contribution of attributes in $\mathcal{T}$. For requests with same access tree, same token can be reused till it expires. A token is generated by mutual collaboration of all participating ATSPs in arriving at a common group element $K \in \mathbb{G}_1$. ATSP pulls an updated value of K using $PullK(IDT_{ij}, K)$ and push the updated value of K using $PushK(IDT_{ij}, K)$. $GenCommonK(IDT_{ij}, K)$ lets AMAI facilitates arrive at a common group element K. Device initiats token generation using $GenTok(IDT_{ij}, K)$ API. Details of these functions are explained in algorithms [7.4 - 7.7]. At the end, a token ABT_{ij} is generated in the device.

Algorithm 7.1 Device : GenPvtKey

Require: $\langle \mathrm{IDT_{ij}} \rangle$

$\mathrm{r} \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$

$\mathrm{K} \leftarrow \mathrm{g^r}$

$\langle \mathrm{M_1}, \mathrm{M_2} \rangle \leftarrow \mathrm{AMAI : PullKeyAll(IDT_{ij}, K)}$

$\mathrm{IDT_{ij}} =$

$\mathrm{ID_{ij}} : \mathrm{ID_i}, \mathcal{T}_{\mathrm{j}}$

$\mathrm{M_1} : \mathrm{M_{1_{AMAI}}} \cup \mathrm{M_{1_{ATSP_1}}} \cup \mathrm{M_{1_{ATSP_2}}} \cup ...$

$\mathrm{M_2} : \mathrm{K}^{\alpha}, \mathrm{K}^{\beta}, \mathrm{K}^{\gamma}, ...$

return

Algorithm 7.2 ATSP : PullKey

Require: $\langle \mathrm{IDT_{ij}}, \mathrm{K} \rangle$

$\alpha \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$

$\langle \mathrm{M_1}, \mathrm{M_2} \rangle \leftarrow \mathrm{genParitalKey(IDT_{ij}, K}, \alpha)$

$\mathrm{M_{1_x}} = \mathrm{K}^{\mathrm{q_x(0)/t_i}} \quad \forall \mathrm{x} \in \mathrm{L(IDT_{ij} \rightarrow T)}$

$\mathrm{M_2} = \mathrm{K}^{\alpha}$

return $\langle \mathrm{M_1}, \mathrm{M_2} \rangle$

Algorithm 7.3 AMAI : PullKeyAll

Require: $\langle \mathrm{IDT_{ij}}, \mathrm{K} \rangle$

$\mathrm{M_1} = \mathrm{M_2} = \phi$

$\mathrm{ATSP} \leftarrow \mathrm{GetATSP(IDT_{ij} \rightarrow T)}$

while ATSP $\neq$ empty **do**

$\mathrm{ATSP_i} \leftarrow \mathrm{DEQUEUE(ATSP)}$

Call API of $\mathrm{ATSP_i}$ API :

$\langle \mathrm{M_1\prime}, \mathrm{M_2\prime} \rangle \leftarrow \mathrm{PullKey(IDT_{ij}, K)}$

$\mathrm{M_1} = \mathrm{M_1} \cup \mathrm{M_1\prime}$

$\mathrm{M_2} = \mathrm{M_2}, \mathrm{M_2\prime}$

end while

return $\langle \mathrm{M_1}, \mathrm{M_2} \rangle$

Algorithm 7.4 ATSP : PullK

Require: $\langle \mathrm{IDT_{ij}}, \mathrm{K} \rangle$

$\mathrm{r} \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$

Store mapping : $\mathrm{IDT_{ij}} \leftrightarrow \mathrm{r}$

return $\mathrm{K^{r}}$

Algorithm 7.5 AMAI : GenCommonK

Require: $\langle \mathrm{IDT_{ij}}, \mathrm{K} \rangle$

$\mathrm{ATSP} \leftarrow \mathrm{GetATSP}(\mathrm{IDT_{ij}} \rightarrow \mathrm{T})$

for all elements $\mathrm{ATSP_i}$ in ATSP **do**

$\mathrm{K} \leftarrow \mathrm{ATSP_i.PullK}(\mathrm{IDT_{ij}}, \mathrm{K})$

end for

$\mathrm{ATSP} \leftarrow \mathrm{GetATSP}(\mathrm{IDT_{ij}} \rightarrow \mathrm{T})$

for all elements $\mathrm{ATSP_i}$ in ATSP **do**

$\mathrm{ATSP_i.PushK}(\mathrm{IDT_{ij}}, \mathrm{K})$

end for

return K

Algorithm 7.6 ATSP : PushK

Require: $\langle \mathrm{IDT_{ij}}, \mathrm{K} \rangle$

$\mathrm{r} \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$

Update mapping : $\mathrm{IDT_{ij}} \leftrightarrow \mathrm{K}$

return

Algorithm 7.7 Device : GenTok

Require: $\langle \mathrm{IDT_{ij}} \rangle$

$\mathrm{r} \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$

$\mathrm{K} \leftarrow \mathrm{g^{r}}$

$\mathrm{K} \leftarrow \mathrm{AMAI : GenCommonK}(\mathrm{IDT_{ij}}, \mathrm{K})$

Store mapping : $\mathrm{IDT_{ij}} \leftrightarrow \mathrm{K}$

$\langle \mathrm{M_1}, \mathrm{M_2} \rangle \leftarrow \mathrm{AMAI : PullKeyAll}(\mathrm{IDT_{ij}}, \mathrm{K})$

$\mathrm{IDT_{ij}} =$

$\mathrm{ID_{ij}} : \mathrm{ID_i}, \mathcal{T}_{\mathrm{j}}$

$\mathrm{M_1} : \mathrm{M_{1_{ATSP_1}}} \cup \mathrm{M_{1_{ATSP_2}}} \cup ...$

$\mathrm{M_2} : \mathrm{K}^{\alpha}, \mathrm{K}^{\beta}, \mathrm{K}^{\gamma}, ...$

return

$$\mathrm{ABT_{ij}} = \begin{cases} \mathrm{IDT_{ij}} & = \mathrm{ID_i}, \mathcal{T}_\mathrm{j} \\ \mathrm{M_1} & = \bigcup_{\forall \mathrm{k}} \mathrm{M1_{ATSP_k}} \quad \mid \mathrm{ATSP_k \in GetATSP}(\mathcal{T}_\mathrm{j}) \\ \mathrm{M_2} & = \mathrm{K}^\alpha, \mathrm{K}^\beta, \mathrm{K}^\gamma, .. \mid \alpha,\beta,\gamma,.. \in \text{Secrets with } \mathrm{ATSP_k} \end{cases} \tag{7.3}$$

7.3.5 Privacy enhanced token-based device signature

When device needs to sign a message m, it uses a random number $\mathrm{r_4} \in_\mathrm{R} \mathbb{Z}_\mathrm{p}$, one way secure hash H(m) of message and the token $\mathrm{ABT_{ij}}$ to compute signature σ_ij as below. This attribute-based signature is given to the consumer application.

$$\sigma_\mathrm{ij} = \begin{cases} \mathrm{A} = \mathrm{g}^{\mathrm{r_4}} \\ \mathrm{C} = \mathrm{g}^{\frac{1}{\mathrm{r_4}+\mathrm{H(m)}}} \\ \mathrm{D} = \{\mathrm{K}^\alpha\}^{\mathrm{r_4}} \cdot \{\mathrm{K}^\beta\}^{\mathrm{r_4}} \cdot \{\mathrm{K}^\gamma\}^{\mathrm{r_4}} \ldots \\ \quad = \mathrm{g}^{\mathrm{r_4}(\prod_{\forall \mathrm{k}} \mathrm{r_k})(\sum_{\forall \mathrm{k}} \mathrm{ASK_k})} \\ \mathrm{E_i} = \mathrm{M_1}^{\mathrm{r_4}} = \mathrm{g}^{\mathrm{r_4}(\prod_{\forall \mathrm{k}} \mathrm{r_k})(\frac{\mathrm{q_x}(0)}{\mathrm{t_i}})} \end{cases}_{\forall\ \mathrm{k} \mid \mathrm{ATSP_k} \in \mathrm{GetATSP}(\mathcal{T})} \tag{7.4}$$

7.3.6 Signature Verification

Consumer application can use an offline procedure $\mathrm{Verify}(\mathrm{M}, \sigma, \mathrm{MPK})$ for verification. This procedure uses the function $\mathrm{VerN}(\mathrm{T_i}, \mathrm{E_i}, \mathrm{i})$, where first parameter is the public key of the attribute i, second parameter is the corresponding private key and third parameter is the attribute of the node i = attr(x). The function is defined as below.

$$\mathrm{VerN}(\mathrm{T_i}, \mathrm{E_i}, \mathrm{x}) = \begin{cases} \mathrm{e}(\mathrm{T_x}, \mathrm{E_x}) & \text{if } \mathrm{attr(x)} \in \gamma \\ \perp & \text{otherwise} \end{cases} \tag{7.5}$$

$\mathrm{VerN}(\mathrm{T_z}, \mathrm{E_z}, \mathrm{z})$ is called for every child node z of non-leaf node x and the result is stored in $\mathrm{L_z}$. Let $\mathrm{k_x}$ represents node x threshold value and the set of child nodes z of node x is represented by a $\mathrm{k_x}$ size set $\mathrm{V_x}$ such that $\mathrm{L_z} \neq \perp$. If $\mathrm{V_x}$ does not exists then the function returns $\perp$ implying the node is not satisfied. If $\mathrm{V_x}$ exists, $\mathrm{L_x}$ is computed as below.

$$
\begin{aligned}
\mathrm{L_x} &= \prod_{\mathrm{z}\in \mathrm{V_x}} \mathrm{L_z}^{\Delta_{\mathrm{i},\mathrm{V_x}'}(0)} \quad \text{where } \mathrm{i} = \mathrm{index(z)}, \mathrm{V_x}\prime = \{\mathrm{index(z)} : \mathrm{z} \in \mathrm{V_x}\} \\
&= \prod_{\mathrm{z}\in \mathrm{V_x}} \mathrm{L_z}^{\Delta_{\mathrm{i},\mathrm{V_x}'}(0)} \\
&= \prod_{\mathrm{z}\in \mathrm{V_x}} (\mathrm{e(g,g)}^{\mathrm{rr_4 q_z}(0)})^{\Delta_{\mathrm{i},\mathrm{V_x}'}(0)} \\
&= \prod_{\mathrm{z}\in \mathrm{V_x}} (\mathrm{e(g,g)}^{\mathrm{rr_4 q_{parent(z)}(index(z))}})^{\Delta_{\mathrm{i},\mathrm{V_x}'}(0)} \\
&= \prod_{\mathrm{z}\in \mathrm{V_x}} \mathrm{e(g,g)}^{\mathrm{rr_4 q_x(i)}\Delta_{\mathrm{i},\mathrm{V_x}'}(0)} \\
&= \mathrm{e(g,g)}^{\mathrm{rr_4 q_x}(0)} \text{ using polynomial interpolation}
\end{aligned} \tag{7.6}
$$

It can be verified that R, $\mathrm{VerN}(\mathrm{T_R}, \mathrm{E_R}, \mathrm{R}) = \mathrm{e(g,g)}^{\mathrm{r_4}(\prod_{\forall \mathrm{k}} \mathrm{r_k})(\Sigma_{\forall \mathrm{k}} \mathrm{ASK_k})}$ if signature satisfies the access tree $\mathcal{T}_\mathrm{R}$.

To ensure that the signer holds necessary attributes, the verifier verifies whether following equalities hold valid and if they are, the signature is considered valid.

$$
\begin{aligned}
\mathrm{e(g,D)} &\stackrel{?}{=} \mathrm{L_R} \\
\mathrm{e(g^m.A, C)} &\stackrel{?}{=} \mathrm{e(g,g)}
\end{aligned} \tag{7.7}
$$

7.4 Security Analysis

This section presents an informal security analysis of the proposed model. Traditional security requirements such as confidentiality, data integrity and mutual authentication are assumed to be present and are intentionally kept out of scope for

this chapter.

Neither the signed document nor the signature contains any information about identity of the signer. At the receiver side, verification of a signature does not require signer identity to be known. Hence signer privacy is maintained.

It can be deduced that with the strong extended Diffie Hellman assumption, the proposed model is existential-unforgeable under chosen-message (eu-cma) attack. Using proof-by-contradiction method, if the model is forgeable with a non-negligible advantage ϵ, then the S-EDH assumption can also be broken with the same advantage ϵ. Furthermore, since private key of the device is always kept in a secure storage such as Trusted Execution Environment (TEE), partial key replacement attack is also not possible.

Our goal is to show that for every adversary $\mathcal{A}$ and environment $\mathcal{Z}$, there exists a simulator $\mathcal{S}$ such that $\mathcal{Z}$ cannot distinguish whether it is interacting in the real world with $\mathcal{A}$ or the ideal world with $\mathcal{S}$. $\mathcal{S}$ is given a black-box access to $\mathcal{A}$. In our description, $\mathcal{S}$ will use $\mathcal{A}$ to simulate conversations with $\mathcal{Z}$. Specifically, $\mathcal{S}$ will directly forward all messages from $\mathcal{A}$ to $\mathcal{Z}$ and from $\mathcal{Z}$ to $\mathcal{A}$.

Adversary $\mathcal{A}$ produces signature σ and message m such that verification succeeds and yet simulator $\mathcal{S}$ never gave $\mathcal{A}$ this user's signature on m. This scenario occurs with only negligible probability under the EDH assumption.

Recall that EDH takes as input $(g, g^x, \bar{g}, \bar{g}^x)$ together with access to oracle $O_x(.)$ that takes input $c \in \mathbb{Z}^*$ and produces output $(g^x, \bar{g}^{\frac{1}{x+v}}, \bar{g}^{\frac{1}{v+c}})$ for any $v, \in_R \mathbb{Z}^*{}_p$. The goal is to produce a tuple $(c, a, a^v, \bar{g}^{\frac{1}{x+v}}, \bar{g}^{\frac{1}{v+c}})$ for any $a \in \mathbb{G}_1$ and any $v, c \in \mathbb{Z}^*$ such that c was not queried to the oracle. When adversary $\mathcal{A}$ succeeds with probability ϵ, then $\mathcal{S}$ solves the EDH problem with probability ϵ. $\mathcal{S}$ proceeds as follows.

- **Setup**: $\mathcal{S}$ establishes the global parameters and the key generation.

  [a] Setup public parameters such as $(g, \bar{g})$.

[b] Guess which honest user $\mathcal{A}$ will attack. Give this user, the public key $pk^* = (g, \bar{g}, g^x, \bar{g}^x, g^r, g^{t_1}, g^{t_2}, ..., g^{t_u}, g^c)$, for random $r \in_R \mathbb{Z}_p$. (Logically this assigns user, the secret key, $sk^* = (t_1, t_2, ..., t_u, c)$).

- **Signing:** When $\mathcal{A}$ is asked for a signature on $m \in \mathbb{Z}_p^*$ from the honest user associated with secret key sk^*:

  [a] Query oracle $O_x(m)$ to get output $(g^v, \bar{g}^{\frac{1}{x+v}}, \bar{g}^{\frac{1}{c+v}})$.

  [b] $\mathcal{A}$ responds with signature $S = g^r, \bar{g}^{\frac{1}{y+r}}, \bar{g}^{\frac{1}{m+r}}, \bar{g}^{wr}, \{\bar{g}^{(r\frac{q_x(0)}{t_i})}\}_{\forall i \in \gamma}$

- **Verification**: $\mathcal{S}$ verifies the sinagure produced by $\mathcal{A}$

- **Output**: Suppose $\mathcal{A}$ produces a valid signature σ' for a new message $m' \in \mathbb{Z}_p^*$ for the user with key sk^*. Then $\mathcal{S}$ outputs (m', σ) to solve the EDH problem.

It is easy to observe that $\mathcal{S}$ perfectly simulates the signature world for $\mathcal{A}$. When $\mathcal{A}$ succeeds with probability ϵ, then $\mathcal{S}$ solves the EDH problem with probability ϵ. Hence, the proposed scheme is existentially unforgeable under chosen-message attack under the strong extended Diffie Hellman assumption.

7.5 Performance Analysis

Present model of registered devices is based on PKI and not on attribute-based schemes, hence, the two models may not be compared efficiently. In this analysis, number of signing, exponent and pairing operations are computed for each phase of the model. Functions NL($\mathcal{T}$) and L($\mathcal{T}$) computes number of non-leaf nodes and leaf-nodes respectively in a given access tree $\mathcal{T}$. N number of ATSPs are assumed to contribute an average of $\mathcal{A}_{ATSP}$ attributes in access tree $\mathcal{T}$. The model consists of five phases, setup, registration, token generation, signature and verification. Most of these phases are one time activities except signature which is invoked for every request. As can be seen from the table below, the signature cost includes linear

		Signing	Exponent	Pairing
Setup	AMAI	$\lvert\mathcal{A}_{\text{AMAI}}\rvert + 1$	$\lvert\mathcal{A}_{\text{AMAI}}\rvert + 1$	
	ATSP			
	Device			
ATSP Registration	AMAI	$\text{N} * (\lvert\mathcal{A}_{\text{ATSP}}\rvert + 1)$		
	ATSP		$\text{N} * (\lvert\mathcal{A}_{\text{ATSP}}\rvert + 1)$	
	Device			
Token Generation	AMAI			
	ATSP		$\text{N} * (\lvert\text{L}(\mathcal{T}_{\text{ATSP}})\rvert + 1)$	
	Device		1	
Attribute based Signature	AMAI			
	ATSP			
	Device		$\lvert\text{L}(\mathcal{T})\rvert + 5$	
eSign Verification	Any		$\lvert\text{NL}(\mathcal{T})\rvert$	$\lvert\text{L}(\mathcal{T})\rvert + 2$

Table 7.1: Performance assessment: Number of operations

number of exponent operations and grows linear to the number of attributes.

$$\text{AmortizedCost}_{\text{DeviceSign}} = \mathcal{O}(\text{L(T)}) * \text{Cost}_{\text{exponent}} \tag{7.8}$$

7.6 Summary

With proliferation of Aadhaar based services, ubiquitous computing devices, IoT and 5G, the number and use of registered devices is expected to grow in terms of volume and sensitivity of data they carry. Two foreseeable requirements in this direction are attribute-based verification and owner and hence device identity privacy. This chapter presents a mechanism to extend present model of registered devices to achieve these two requirements.

This page intentionally left blank.

Chapter 8

Conclusion and Future Work

Since the establishment of Aadhaar, the Government has built various online digital services such as eSign, DigiLocker, etc. Although critiques have raised some privacy related concerns in Aadhaar project, we consider it as a courageous initiative in a developing country like India and if implemented in the right way has the potential to help India compete in digital revolution across the world.

8.1 Summary

This research presents five major contributions to improve privacy of Aadhaar-based e-Governance services in India.

The first contribution is to present privacy-enhanced eSign model in which participating entities such as users, UIDAI and ESP can enforce their privacy policies by encoding them in specially devised digital tokens. In the present model of eSign, subscriber's eKYC information is retrieved in full and is given in full for unlimited time to all the entities who receives boolean consent from the subscriber. This access mechanism reflects a restrictive *self-only, full-resource and unlimited* access control. A subscriber may wish to have a better fine-grained access control mech-

anism that allows third entities to access part of a resource that can be used only for a specific purpose and only for a limited time. The proposed scheme reflects a *third-entity-also, partial resource, use-limited and time-limited* fine-grained access mechanism. A formal security analysis is presented using Burrows-Abadi-Needham (BAN) logic.

The second contribution is to present privacy-enhanced eSign model in which the signer signs the document using his attributes and does not have to reveal his identity for the verifier to verify the signed document. This is an improvement over the present model of eSign in which identity of the signer is revealed to the receiver, which may not be required in some cases and may not even be suitable. For example, the same person can hold multiple roles in an organisation such as an employee of an organization, principal investigator of a project, executive director of an organisation and even an interim director-general. In certain cases, the role of the person is important in signature rather than his/her name. The proposed scheme uses attribute-based signature and devised a digital token to improve the performance of the eSign process.

The third contribution is to present privacy-enhanced DigiLocker in which subscriber can encrypt his documents with a privacy policy so that only those requesters whose attributes satisfy the privacy policy can decrypt and retrieve the document. In the present model of DigiLocker, subscriber's documents are hosted on a public cloud which is assumed to be a trusted entity. However, cloud storage may not be trustworthy and may be susceptible to insider attacks. Moreover, instead of providing a reactive access authorization to a single requester, a subscriber may want to provide a proactive fine-grained access authorization to multiple requesters meeting certain criteria of attributes. The proposed scheme is proved to be secure against an adaptive chosen-plaintext attack (CPA) if any polynomial-time adversary has only a negligible advantage in the IND-sAtt-CPA game.

The fourth contribution is to present a privacy-enhanced scheme in an auto-

mated toll tax collection service in which a vehicle does not have to disclose its identity to the toll station to get a toll ticket. The proposed scheme uses lightweight operations such as cryptographic hash, XOR and concatenation functions. A formal security analysis is presented using Burrows-Abadi-Needham (BAN) logic.

The fifth contribution is to present privacy-enhanced scheme for registered devices in which a genuine device is recognized not just by its model number and serial number but by its attributes which can be assigned to it by multiple authorities and the device signs each message with its attributes. Registered devices are designated devices in the Aadhaar ecosystem which is used to capture and transmit biometric. Biometric is sensitive data and utmost care should be taken to ensure the security of devices carrying them. The use of these devices is expected to grow more and such devices are expected to carry more than just biometric data such as personal identifiable information, financial data, medical data, etc. Although at present, this model may suffice, with the proliferation of connected devices and online services, registered devices may soon become ubiquitous, required to operate remotely and to process other sensitive personal data as well. In a ubiquitous world of registered devices, an application may want to query and use a valid registered device having a specific set of attributes rather than a registered device having a specific random string of serial number or model number. Since the identity of the device may be correlated with the identity of its owner, the owner of the device may not want to disclose the identity of the device to protect his privacy. The owner may just want to let the device be recognized as a valid registered device having a certain set of attributes.

8.2 Future Research Avenues

The research work in this thesis provide ample space and promulgate several clear directions for future research endeavours. Though the proposed digital tokens facilitate encoding privacy policies, they can further be integrated with hardware tokens

such as FIDO to protect against phishing attacks and to provide a better user experience. Other mechanisms also exist to enhance privacy-related aspects even further. Some of such notable mechanisms which can be used to improve privacy are listed below.

Secure multi-party computation [134]. One method to secure private data is offered by secure multi-party computation Secure multi-party computation is a field of cryptography that allows several mutually distrustful parties, each wishing to maintain privacy of their input data, to perform some computation on their joint data. This is a rich field with several efficient mechanisms in place to perform a large class of interesting computations privately. The tools and techniques from this field may be relevant to the Aadhaar project: for instance, one may use a secret-sharing scheme to split the database across two servers belonging to different entities, ensuring that the two servers have disjoint sets of system administrators and diverse operating systems and hardware. This ensures that even if one server is hacked into, the data remains protected. Secure multiparty computation can be used to answer queries on the data distributed across servers.

Homomorphic and functional encryption [135]. Another security threat is the possibility of server breaches, whether the attack is launched from inside or outside the organisation. To prevent a server breach from leaking valuable user data, critical data needs to be stored on the server in encrypted form. However, encrypting data using standard methods leads to loss of functionality, such as the ability to perform data analytics. Recently, advanced forms of encryption have been designed by the cryptographic community that allow an untrusted server to compute on data "blindfolded". Two striking examples of such encryption mechanisms are the notions of homomorphic encryption and functional encryption. At a high level, these systems allow sensitive data to be encrypted in a way that allows sophisticated computation on the data in its encrypted form. Thus, the functionality offered by data analytics can be enjoyed while ensuring privacy.

Such mechanisms may be very pertinent to ensuring privacy of data in the UIDAI database. However, while these systems are substantial achievements in cryptographic design, they remain far too slow for practical use. Nevertheless, for restricted classes of computations, such algorithms may be deployed. Third party intervention will be required to set up the computation in the encrypted domain.

Symmetric Searchable Encryption and Extensions [136]. Another method to perform useful computations on encrypted data is offered by the field of symmetric searchable encryption, which enables searching on encrypted data. Unlike notions such as functional encryption and homomorphic encryption described above, algorithms developed in the context of searchable encryption are highly efficient and scale well for massive sized data, such as the UIDAI data. For many investigative applications, tools and techniques developed in the context of searchable encryption appear to be very relevant.

Whiteboxing and code obfuscation [137]. Another useful class of defenses against insider attacks comes from techniques developed in the area of whitebox cryptography. Typically, one assumes that attacks are blackbox, i.e., an attacker has access to the input and the output of a program, but not to the internal workings of the program. However, an insider may have full access to the source code and binary file running on the system, and also the corresponding memory pages during execution. Additionally, the attacker can also possibly make use for debuggers and emulators, intercept system calls and tamper with the binary and its execution. Such attacks are called whitebox attacks, and whitebox cryptography aims to implement cryptographic procedures in software that transform and obfuscate code and data in such a way so that the cryptographic assets remain secure even when subject to whitebox attacks.

Although whitebox cryptography and obfuscation have been plagued with numerous attacks and there are impossibility results in theory for the general problem, successful whiteboxing in specific situations may well be possible. Many software

packages that provide whitebox protection in restricted scenarios are available, and despite the lack of rigorous cryptographic guarantees, seem to work well in practice. Such packages may be deployed to enhance security against insider attacks. Note that the whitebox protection of security keys and the decryption code will have to be put in place by an independent third party.

Bibliography

[1] R. Khera. *The Aadhaar debate: Where are the sociologists?* 2018. URL: https://doi.org/10.1177/0069966718787029.

[2] UIDAI. *Aadhaar Annual Report 2018-19*. 2019. URL: https://www.uidai.gov.in/images/AADHAR_AR_2018_19_ENG_approved.pdf.

[3] Vivek Raghavan, Sanjay Jain, and Pramod Varma. "India stack—digital infrastructure as public good". In: *Communications of the ACM* 62.11 (2019), pp. 76–81.

[4] V. Krishna. *India Stack – A change agent for government, startups and corporates to serve citizens*. 2016. URL: https://yourstory.com/2016/07/india-stack/.

[5] P. Thimmaya. *India stack: To serve the underserved*. 2017. URL: https://www.financialexpress.com/industry/technology/india-stack-to-serve-the-underserved/821926/.

[6] R. Khera. *Impact of Aadhaar on welfare programmes*. 2017. URL: https://doi.org/10.2139/ssrn.3045235.

[7] Subodh Sharma. *Virtual ID is a good beginning; much more remains to be done*. 2018. URL: http://www.governancenow.com/views/interview/virtual-id-is-a-good-beginning-much-more-remains-to-be-done.

[8] Daniel J. Solove. *Understanding privacy*. Harvard University Press, 2008.

[9] Asia-Pacific Economic Cooperation. "APEC privacy framework". In: *Asia Pacific Economic Cooperation Secretariat* 81 (2005).

[10] Paul Voigt and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)". In: *A Practical Guide, 1st Ed., Cham: Springer International Publishing* (2017).

[11] UN High-Level Committee on Management (HLCM). *Personal Data Protection and Privacy Principles*. URL: https://www.unsceb.org/CEBPublicFiles/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf.

[12] Organisation for Economic Co-operation and Development. *The OECD Privacy Framework*. URL: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[13] International Standards Organization. *Information technology — Security techniques — Privacy framework*. URL: https://www.iso.org/standard/45123.html.

[14] Ann Cavoukian. "Privacy by design". In: *Take the challenge. Information and privacy commissioner of Ontario, Canada* (2009).

[15] Menaka Guruswamy. "Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors". In: *American Journal of International Law* 111.4 (2017), pp. 994–1000. DOI: 10.1017/ajil.2017.92.

[16] Qun Ni et al. "Privacy-aware role-based access control". In: *ACM Transactions on Information and System Security (TISSEC)* 13.3 (2010), pp. 1–31.

[17] Amirreza Masoumzadeh and James BD Joshi. "PuRBAC: Purpose-aware role-based access control". In: *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer. 2008, pp. 1104–1121.

[18] Naikuo Yang, Howard Barringer, and Ning Zhang. "A purpose-based access control model". In: *Third International Symposium on Information Assurance and Security*. IEEE. 2007, pp. 143–148.

[19] Adi Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[20] Fatih Emekcci et al. "Privacy preserving decision tree learning over multiple parties". In: *Data & Knowledge Engineering* 63.2 (2007), pp. 348–361.

[21] Tatiana Ermakova and Benjamin Fabian. "Secret sharing for health data in multi-provider clouds". In: *2013 IEEE 15th conference on business informatics*. IEEE. 2013, pp. 93–100.

[22] Jiguo Li et al. "Flexible and fine-grained attribute-based data storage in cloud computing". In: *IEEE Transactions on Services Computing* 10.5 (2016), pp. 785–796.

[23] Vipul Goyal et al. "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proceedings of the 13th ACM conference on Computer and communications security*. 2006, pp. 89–98.

[24] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption". In: *2007 IEEE symposium on security and privacy (SP'07)*. IEEE. 2007, pp. 321–334.

[25] Jiguo Li et al. "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage". In: *IEEE Systems Journal* 12.2 (2017), pp. 1767–1777.

[26] Jiguo Li et al. "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length". In: *Security and Communication Networks* 2017 (2017).

[27] Jiguo Li et al. "Full verifiability for outsourced decryption in attribute based encryption". In: *IEEE transactions on services computing* 13.3 (2017), pp. 478–487.

[28] Keita Emura et al. "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length". In: *International Conference on Information Security Practice and Experience*. Springer. 2009, pp. 13–23.

[29] Cheng Chen, Zhenfeng Zhang, and Dengguo Feng. "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost". In: *International Conference on Provable Security*. Springer. 2011, pp. 84–101.

[30] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 2009, pp. 169–178.

[31] Zvika Brakerski and Vinod Vaikuntanathan. "Efficient fully homomorphic encryption from (standard) LWE". In: *SIAM Journal on Computing* 43.2 (2014), pp. 831–871.

[32] Junfeng Fan and Frederik Vercauteren. "Somewhat practical fully homomorphic encryption." In: *IACR Cryptol. ePrint Arch.* 2012 (2012), p. 144.

[33] Craig Gentry, Amit Sahai, and Brent Waters. "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based". In: *Annual Cryptology Conference*. Springer. 2013, pp. 75–92.

[34] Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan. "Can homomorphic encryption be practical?" In: *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*. 2011, pp. 113–124.

[35] Thore Graepel, Kristin Lauter, and Michael Naehrig. "ML confidential: Machine learning on encrypted data". In: *International Conference on Information Security and Cryptology*. Springer. 2012, pp. 1–21.

[36] Kristin Lauter, Adriana Lopez-Alt, and Michael Naehrig. "Private computation on encrypted genomic data". In: *International Conference on Cryptology and Information Security in Latin America*. Springer. 2014, pp. 3–27.

[37] Michel Abdalla et al. "Simple functional encryption schemes for inner products". In: *IACR International Workshop on Public Key Cryptography*. Springer. 2015, pp. 733–751.

[38] Michel Abdalla et al. "Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings". In: *Annual International Cryptology Conference*. Springer. 2018, pp. 597–627.

[39] Shweta Agrawal, Benot Libert, and Damien Stehle. "Fully secure functional encryption for inner products, from standard assumptions". In: *Annual International Cryptology Conference*. Springer. 2016, pp. 333–362.

[40] Jeremy Chotard et al. "Decentralized multi-client functional encryption for inner product". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2018, pp. 703–732.

[41] Edouard Dufour Sans, Romain Gay, and David Pointcheval. "Reading in the dark: Classifying encrypted digits with functional encryption". In: *IACR Cryptol. ePrint Archive* 206 (2018), p. 2018.

[42] Philippe Golle, Jessica Staddon, and Brent Waters. "Secure conjunctive keyword search over encrypted data". In: *International conference on applied cryptography and network security*. Springer. 2004, pp. 31–45.

[43] Florian Hahn and Florian Kerschbaum. "Searchable encryption with secure and efficient updates". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, pp. 310–320.

[44] Kee Sung Kim et al. "Forward secure dynamic searchable symmetric encryption with efficient updates". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, pp. 1449–1463.

[45] Cong Wang et al. "Enabling secure and efficient ranked keyword search over outsourced cloud data". In: *IEEE Transactions on parallel and distributed systems* 23.8 (2011), pp. 1467–1479.

[46] Cong Wang et al. "Secure ranked keyword search over encrypted cloud data". In: *2010 IEEE 30th international conference on distributed computing systems*. IEEE. 2010, pp. 253–262.

[47] Mingwu Zhang, Shaochen Zhang, and Lein Harn. "An efficient and adaptive data-hiding scheme based on secure random matrix". In: *Plos one* 14.10 (2019), e0222892.

[48] Qian Wang et al. "Searchable encryption over feature-rich data". In: *IEEE Transactions on Dependable and Secure Computing* 15.3 (2016), pp. 496–510.

[49] Emil Stefanov, Charalampos Papamanthou, and Elaine Shi. "Practical Dynamic Searchable Encryption with Small Leakage." In: *NDSS*. Vol. 71. 2014, pp. 72–75.

[50] Ian F Blake and Vladimir Kolesnikov. "Strong conditional oblivious transfer and computing on intervals". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2004, pp. 515–529.

[51] Jing Li et al. "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing". In: *Journal of Parallel and Distributed Computing* 130 (2019), pp. 91–97.

[52] Khaled Riad, Rafik Hamza, and Hongyang Yan. "Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records". In: *IEEE Access* 7 (2019), pp. 86384–86393. DOI: 10.1109/ACCESS.2019.2926354.

[53] Jin Li et al. "Searchable Symmetric Encryption with Forward Search Privacy". In: *IEEE Transactions on Dependable and Secure Computing* 18.1 (2021), pp. 460–474. DOI: 10.1109/TDSC.2019.2894411.

[54] B. Chor et al. "Private information retrieval". In: *Proceedings of IEEE 36th Annual Foundations of Computer Science*. 1995, pp. 41–50. DOI: 10.1109/SFCS.1995.492461.

[55] E. Kushilevitz and R. Ostrovsky. "Replication is not needed: single database, computationally-private information retrieval". In: *Proceedings 38th Annual Symposium on Foundations of Computer Science*. 1997, pp. 364–373. DOI: 10.1109/SFCS.1997.646125.

[56] Christian Cachin, Silvio Micali, and Markus Stadler. "Computationally Private Information Retrieval with Polylogarithmic Communication". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by Jacques Stern. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 402–414. ISBN: 978-3-540-48910-8.

[57] Yan-Cheng Chang. "Single Database Private Information Retrieval with Logarithmic Communication". In: *Information Security and Privacy*. Ed. by Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 50–61. ISBN: 978-3-540-27800-9.

[58] Craig Gentry and Zulfikar Ramzan. "Single-Database Private Information Retrieval with Constant Communication Rate". In: *Automata, Languages and Programming*. Ed. by Luis Caires et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 803–815. ISBN: 978-3-540-31691-6.

[59] Michael O. Rabin. *How To Exchange Secrets with Oblivious Transfer*. Harvard University Technical Report 81 talr@watson.ibm.com 12955 received 21 Jun 2005. 2005. URL: http://eprint.iacr.org/2005/187.

[60] Dahlia Malkhi et al. "Fairplay—A Secure Two-Party Computation System". In: *13th USENIX Security Symposium (USENIX Security 04)*. San Diego, CA: USENIX Association, Aug. 2004. URL: https://www.usenix.org/conference/13th-usenix-security-symposium/fairplay%7B%5Ctextemdash%7D-secure-two-party-computation-system.

[61] Assaf Ben-David, Noam Nisan, and Benny Pinkas. "FairplayMP: a system for secure multi-party computation." In: *ACM Conference on Computer and Communications Security*. Ed. by Peng Ning, Paul F. Syverson, and Somesh Jha. ACM, 2008, pp. 257–266. ISBN: 978-1-59593-810-7. URL: http://dblp.uni-trier.de/db/conf/ccs/ccs2008.html#Ben-DavidNP08.

[62] Janus Dam Nielsen, Jakob Illeborg Pagter, and Michael Bladt Stausholm. "Location privacy via actively secure private proximity testing". In: *PerCom Workshops*. IEEE Computer Society, 2012, pp. 381–386.

[63] Peter Bogetoft et al. "Secure Multiparty Computation Goes Live". In: *Financial Cryptography and Data Security*. Ed. by Roger Dingledine and Philippe Golle. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 325–343. ISBN: 978-3-642-03549-4.

[64] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. *The knowledge complexity of interactive proof systems*. 1989.

[65] Manuel Blum, Paul Feldman, and Silvio Micali. "Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract)". In: *STOC*. ACM, 1988, pp. 103–112.

[66] Manuel Blum, Paul Feldman, and Silvio Micali. "Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract)". In: *STOC*. ACM, 1988, pp. 103–112.

[67] Stephanie Bayer and Jens Groth. "Efficient Zero-Knowledge Argument for Correctness of a Shuffle". In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 263–280. ISBN: 978-3-642-29011-4.

[68] Jens Groth. "Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures". In: *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 4284. Lecture Notes in Computer Science. Springer, 2006, pp. 444–459. DOI: 10.1007/11935230_29. URL: https://iacr.org/archive/asiacrypt2006/42840449/42840449.pdf.

[69] Jens Groth. "Fully Anonymous Group Signatures Without Random Oracles". In: *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*. Vol. 4833. Lecture Notes in Computer Science. Springer, 2007, pp. 164–180. DOI: 10.1007/978-3-540-76900-2_10. URL: https://iacr.org/archive/asiacrypt2007/48330162/48330162.pdf.

[70] Bernd Frohlich et al. "Quantum Secured Gigabit Passive Optical Networks". In: *Optical Fiber Communication Conference*. Optical Society of America, 2015, W4F.1. DOI: 10.1364/OFC.2015.W4F.1. URL: http://www.osapublishing.org/abstract.cfm?URI=OFC-2015-W4F.1.

[71] Omer K. Jasim Mohammad et al. "Cryptographic Cloud Computing Environment as a More Trusted Communication Environment". In: *Int. J. Grid High Perform. Comput.* 6.2 (2014), pp. 38–51.

[72] Vijey Thayananthan and A. Albeshri. "Big Data Security Issues and Quantum Cryptography for Cloud Computing". In: *International Journal of Computer Applications* 180 (2018), pp. 22–28.

[73] M. Fujiwara et al. "Highly Secure Network Switches with Quantum Key Distribution Systems". In: *Int. J. Netw. Secur.* 17 (2015), pp. 34–39.

[74] Vincent C Hu et al. "Guide to attribute based access control (abac) definition and considerations (draft)". In: *NIST special publication* 800.162 (2013).

[75] David F Ferraiolo et al. "Proposed NIST standard for role-based access control". In: *ACM Transactions on Information and System Security (TISSEC)* 4.3 (2001), pp. 224–274.

[76] Ravi S Sandhu. "Role-based access control". In: *Advances in computers*. Vol. 46. Elsevier, 1998, pp. 237–286.

[77] Simone Fischer-Hübner et al. *IT-security and privacy: design and use of privacy-enhancing security mechanisms*. 1958. Springer Science & Business Media, 2001.

[78] Qun Ni et al. "Conditional privacy-aware role based access control". In: *European Symposium on Research in Computer Security*. Springer. 2007, pp. 72–89.

[79] Vipul Goyal et al. "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proceedings of the 13th ACM conference on Computer and communications security*. 2006, pp. 89–98.

[80] Mikko Kiviharju et al. "Enforcing Role-Based Access Control with Attribute-Based Cryptography for Environments with Multi-Level Security Requirements". In: (2016).

[81] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption". In: *2007 IEEE symposium on security and privacy (SP'07)*. IEEE. 2007, pp. 321–334.

[82] Jin Li et al. "Attribute-based signature and its applications". In: *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. 2010, pp. 60–69.

[83] Rakesh Bobba et al. "Attribute-based messaging: Access control and confidentiality". In: *ACM Transactions on Information and System Security (TISSEC)* 13.4 (2010), pp. 1–35.

[84] UIDAI. *Unique Identification Authority of India*. URL: https://uidai.gov.in%20(2017).

[85] Wikipedia. *Aadhaar*. URL: https://en.wikipedia.org/wiki/Aadhaar%20(2017).

[86] Reserve Bank of India. *Master Direction - Know Your Customer (KYC) Direction, 2016*. URL: https://rbidocs.rbi.org.in/rdocs/notification/PDF%5C%5Cs/18MDKYCD8E68EB1%203629A4A82BE8E06E606C57E57.PDF%20(2018).

[87] Christian Paquin and Greg Zaverucha. "U-prove cryptographic specification v1. 1". In: *Technical Report, Microsoft Corporation* (2011).

[88] David Chaum. "Blind signatures for untraceable payments". In: *Advances in cryptology*. Springer. 1983, pp. 199–203.

[89] Dick Hardt. "RFC 6749—The OAuth 2.0 Authorization Framework, 2012". In: *Retrieved from the Internet* (2017), pp. 1–76.

[90] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. Tech. rep. Manubot, 2019.

[91] UIDAI. *Aadhaar e-KYC API Specification - Version 2.1*. URL: https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_1.pdf.

[92] CCA. *eSign Service*. URL: http://cca.gov.in/cca/?q=eSign.html.

[93] Michael Burrows, Martin Abadi, and Roger Michael Needham. "A logic of authentication". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 426.1871 (1989), pp. 233–271.

[94] Guo Shanqing and Zeng Yingpei. "Attribute-based signature scheme". In: *2008 International Conference on Information Security and Assurance (ISA 2008)*. IEEE. 2008, pp. 509–511.

[95] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[96] Adi Shamir. "Identity-based cryptosystems and signature schemes". In: *Workshop on the theory and application of cryptographic techniques*. Springer. 1984, pp. 47–53.

[97] Dan Boneh and Matt Franklin. "Identity-based encryption from the Weil pairing". In: *Annual international cryptology conference*. Springer. 2001, pp. 213–229.

[98] Clifford Cocks. "An identity based encryption scheme based on quadratic residues". In: *IMA international conference on cryptography and coding*. Springer. 2001, pp. 360–363.

[99] Syh-Yuan Tan, Swee-Huay Heng, and Bok-Min Goi. "On the security of an attribute-based signature scheme". In: *International Conference on U-and E-Service, Science and Technology*. Springer. 2009, pp. 161–168.

[100] Hemanta K Maji, Manoj Prabhakaran, and Mike Rosulek. "Attribute-based signatures". In: *Cryptographers' track at the RSA conference*. Springer. 2011, pp. 376–392.

[101] Amos Beimel et al. *Secure schemes for secret sharing and key distribution*. Technion-Israel Institute of technology, Faculty of computer science, 1996.

[102] UIDAI. *What is Aadhaar*. URL: `https://uidai.gov.in/myaadhaar/about-your-aadhaar.html`.

[103] Zhibin Zhou and Dijiang Huang. "Efficient and secure data storage operations for mobile cloud computing". In: *2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm)*. IEEE. 2012, pp. 37–45.

[104] Yi-mu Ji et al. "A Privacy Protection Method Based on CP-ABE and KP-ABE for Cloud Computing." In: *JSW* 9.6 (2014), pp. 1367–1375.

[105] MeitY. *Digital Locker Technical Specification (DLTS)*. URL: `https://img1.digitallocker.gov.in/assets/img/technicalspecifications-dlts-ver-2.3.pdf`.

[106] Luan Ibraimi et al. "Efficient and provable secure ciphertext-policy attribute-based encryption schemes". In: *International Conference on Information Security Practice and Experience*. Springer. 2009, pp. 1–12.

[107] Florian Dotzer. "Privacy issues in vehicular ad hoc networks". In: *International Workshop on Privacy Enhancing Technologies*. Springer. 2005, pp. 197–209.

[108] Yang Ming and Xiaoqin Shen. "PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks". In: *Sensors* 18.5 (2018), p. 1573.

[109] Yang Ming and Hongliang Cheng. "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs". In: *Mobile Information Systems* 2019 (2019).

[110] Changhui Hu et al. "Efficient HMAC-based secure communication for VANETs". In: *Computer Networks* 56.9 (2012), pp. 2292–2303.

[111] Xiaoping Xue and Jia Ding. "LPA: a new location-based privacy-preserving authentication protocol in VANET". In: *Security and Communication Networks* 5.1 (2012), pp. 69–78.

[112] Chenxi Zhang et al. "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks". In: *2008 IEEE international conference on communications*. IEEE. 2008, pp. 1451–1457.

[113] Tat Wing Chim et al. "SPECS: Secure and privacy enhancing communications schemes for VANETs". In: *Ad Hoc Networks* 9.2 (2011), pp. 189–203.

[114] Kyung-Ah Shim. "CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks". In: *IEEE transactions on vehicular technology* 61.4 (2012), pp. 1874–1883.

[115] Murtadha A Alazzawi et al. "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network". In: *IEEE Access* 7 (2019), pp. 71424–71435.

[116] Majid Bayat et al. "NERA: A new and efficient RSU based authentication scheme for VANETs". In: *Wireless networks* 26.5 (2020), pp. 3083–3098.

[117] Junko Ohya, Yoshiro Seki, and Katsuyoshi Suzuki. "A study on operation of ETC (electronic toll collection)". In: *Proceedings 199 IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems (Cat. No. 99TH8383)*. IEEE. 1999, pp. 581–584.

[118] Xiaodong Lin. "Secure and privacy-preserving vehicular communications". In: (2008).

[119] Andrew J Blumberg, Lauren S Keeler, and Abhi Shelat. "Automated traffic enforcement which respects" driver privacy"". In: *Proceedings. 2005 IEEE Intelligent Transportation Systems, 2005.* IEEE. 2005, pp. 941–946.

[120] Jeyanthi Hall et al. "WPP: A secure payment protocol for supporting credit- and debit-card transactions over wireless networks". In: *IEEE International Conference on Telecommunications (ICT)*. Citeseer. 2001.

[121] Carmela Troncoso et al. "Pripayd: Privacy-friendly pay-as-you-drive insurance". In: *IEEE Transactions on Dependable and Secure Computing* 8.5 (2010), pp. 742–755.

[122] Josep Balasch, Ingrid Verbauwhede, and Bart Preneel. "An embedded platform for privacy-friendly road charging applications". In: *2010 Design, Automation & Test in Europe Conference & Exhibition (DATE 2010)*. IEEE. 2010, pp. 867–872.

[123] Raluca Ada Popa, Hari Balakrishnan, and Andrew J Blumberg. "VPriv: Protecting privacy in location-based vehicular services". In: (2009).

[124] Josep Balasch et al. "PrETP: Privacy-Preserving Electronic Toll Pricing." In: *USENIX Security Symposium*. Vol. 10. 2010, pp. 63–78.

[125] Santosh K Misra and Nilmini Wickamasinghe. "Security of a mobile transaction: A trust model". In: *Electronic Commerce Research* 4.4 (2004), pp. 359–372.

[126] Marko Hassinen, Konstantin Hyppönen, and Keijo Haataja. "An open, PKI-based mobile payment system". In: *International Conference on Emerging Trends in Information and Communication Security*. Springer. 2006, pp. 86–100.

[127] Hong Wang and Evangelos Kranakis. *Secure wireless payment protocol*. Carleton University, 2002.

[128] Suresh Chari et al. "Security Issues in M—Commerce: A Usage—Based Taxonomy". In: *E-commerce agents*. Springer, 2001, pp. 264–282.

[129] Jesús Téllez Isaac, Sherali Zeadally, and José Sierra Cámara. "A lightweight secure mobile payment protocol for vehicular ad-hoc networks (VANETs)". In: *Electronic Commerce Research* 12.1 (2012), pp. 97–123.

[130] Bruno Blanchet et al. "ProVerif 2.00: automatic cryptographic protocol verifier, user manual and tutorial". In: *Version from* (2018), pp. 05–16.

[131] Mark Dermot Ryan and Ben Smyth. "Applied pi calculus." In: *Formal Models and Techniques for Analyzing Security Protocols* 5 (2011), pp. 112–142.

[132] MeitY. *Aadhaar Registered Devices Technical Specification v2.0*. 2019. URL: `https://uidai.gov.in/images/resource/Aadhaar_Registered_Devices_2_0_4.pdf`.

[133] MeitY. *Aadhaar Authentication API Specification v2.0*. 2017. URL: `https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf`.

[134] Ronald Cramer, Ivan Bjerre Damgård, et al. *Secure multiparty computation*. Cambridge University Press, 2015.

[135] Xun Yi, Russell Paulet, and Elisa Bertino. "Homomorphic encryption". In: *Homomorphic Encryption and Applications*. Springer, 2014, pp. 27–46.

[136] Reza Curtmola et al. "Searchable symmetric encryption: improved definitions and efficient constructions". In: *Journal of Computer Security* 19.5 (2011), pp. 895–934.

[137] Patrice Godefroid, Michael Y Levin, David A Molnar, et al. "Automated whitebox fuzz testing." In: *NDSS*. Vol. 8. 2008, pp. 151–166.

[138] Albert Einstein. "Zur Elektrodynamik bewegter Körper. (German) [On the electrodynamics of moving bodies]". In: *Annalen der Physik* 322.10 (1905), pp. 891–921. DOI: http://dx.doi.org/10.1002/andp.19053221004.

[139] Cong Zuo et al. "CCA-secure ABE with outsourced decryption for fog computing". In: *Future Generation Computer Systems* 78 (2018), pp. 730–738.

[140] Alleaume et al. "Using quantum key distribution for cryptographic purposes: A survey." In: *Theor. Comput. Sci.* 560 (2014), pp. 62–81. URL: http://dblp.uni-trier.de/db/journals/tcs/tcs560.html#AlleaumeBBDDGGGLLMPPPPRRRRSSWZ14

[141] Data Security Council of India. *DSCI Privacy Framework (DPF)*. URL: https://www.dsci.in/content/dsci-privacy-framework-dpf.

[142] Data Security Council of India. *DSCI Assessment Framework - Privacy (DAF-P)*. URL: https://www.dsci.in/content/dsci-assessment-framework-privacy-daf-p.

[143] Data Security Council of India. *DSCI Security Framework (DSF)*. URL: https://www.dsci.in/content/dsci-security-framework-dsf.

[144] Data Security Council of India. *DSCI Assessment Framework - Security (DAF-S)*. URL: https://www.dsci.in/content/dsci-assessment-framework-security-daf-s.

[145] Paul Adrien Maurice Dirac. *The Principles of Quantum Mechanics*. International series of monographs on physics. Clarendon Press, 1981.

[146] Donald Knuth. *Knuth: Computers and Typesetting*. URL: http://www-cs-faculty.stanford.edu/~uno/abcde.html.

[147] Donald E. Knuth. "Fundamental Algorithms". In: Addison-Wesley, 1973. Chap. 1.2.

[148] Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[149] Ralph C Merkle. "A digital signature based on a conventional encryption function". In: *Conference on the theory and application of cryptographic techniques*. Springer. 1987, pp. 369–378.

[150] PKIA2017. *Development of Smart Authentication and Identification in Asia*. URL: http://pkiindia.in/pkia/%5C#preceding.

[151] CCA. *PKI framework in India*. URL: http://www.cca.gov.in/cca/?q=pki_frame%20work.html.

[152] CCA. *Public key certificate classes*. URL: http://www.cca.gov.in/cca/?q=node/45.

[153] CCA. *Empanelled eSign Service Providers*. URL: http://www.cca.gov.in/cca/?q=service-providers.html.

[154] M Jones, J Bradley, and N Sakimura. "Rfc 7519: Json web token (jwt)". In: *Date Retr* 5 (2015), p. 2017.

[155] Michael Jones et al. "Cbor web token (cwt)". In: *RFC 8392, Standards Track, IETF* (2018).

[156] Government of India. *Digital India*. URL: https://www.digitalindia.gov.in.

[157] UIDAI. *Aadhaar*. URL: https://uidai.gov.in/what-is-aadhaar.html.

[158] Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. "An efficient signature scheme from bilinear pairings and its applications". In: *International Workshop on Public Key Cryptography*. Springer. 2004, pp. 277–290.

[159] Yacov Yacobi. "A Note on the Bilinear Diffie-Hellman Assumption." In: *IACR Cryptol. ePrint Arch.* 2002 (2002), p. 113.

[160] Giuseppe Ateniese et al. "Practical Group Signatures without Random Oracles." In: *IACR Cryptol. ePrint Arch.* 2005 (2005), p. 385.

[161] Michael O Rabin. "How To Exchange Secrets with Oblivious Transfer." In: *IACR Cryptol. ePrint Arch.* 2005.187 (2005).

[162] Oded Goldreich. "Secure multi-party computation". In: *Manuscript. Preliminary version* 78 (1998).

[163] GoI. *Digital India Initiatives*. URL: `https://www.digitalindia.gov.in/di-initiatives`.

[164] UIDAI. *About UIDAI*. URL: `https://uidai.gov.in`.

[165] GoI. *DigiLocker*. URL: `https://digilocker.gov.in`.

[166] Tata Memorial Cenentre. *National Centre Grid*. URL: `https://tmc.gov.in/ncg`.

[167] Rafail Ostrovsky, Amit Sahai, and Brent Waters. "Attribute-based encryption with non-monotonic access structures". In: *Proceedings of the 14th ACM conference on Computer and communications security*. 2007, pp. 195–203.

[168] GoI. *The Gazette of India, Part II, Section 3, Subsection i*. URL: `https://www.meity.gov.in/writereaddata/files/Digi%20Locker%20Rules%20%20and%20Amendment.pdf`.

[169] MeitY. *Authorized Partner API Specification*. URL: `https://partners.digitallocker.gov.in/assets/img/digitallocker%20authorized%20partner%20api%20specification%20v1.2.pdf`.

[170] Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. "An efficient signature scheme from bilinear pairings and its applications". In: *International Workshop on Public Key Cryptography*. Springer. 2004, pp. 277–290.

[171] Andrew Justin Blumberg and Robin Chase. "Congestion Pricing That Preserves Driver Privacy". In: *2006 IEEE Intelligent Transportation Systems Conference*. IEEE. 2006, pp. 725–732.

[172] MeitY. *Aadhaar eKYC API Specification, v2.1*. 2017. URL: `https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_1.pdf`.

[173] MeitY. *eSign API Specifications v3.2*. 2019. URL: http://cca.gov.in/sites/files/pdf/esign/eSign-APIv3.2.pdf.

[174] Syh-Yuan Tan, Swee-Huay Heng, and Bok-Min Goi. "On the security of an attribute-based signature scheme". In: *International Conference on U-and E-Service, Science and Technology*. Springer. 2009, pp. 161–168.

[175] Leslie Lamport. "The temporal logic of actions". In: *ACM Transactions on Programming Languages and Systems (TOPLAS)* 16.3 (1994), pp. 872–923.

[176] Jayavardhana Gubbi et al. "Internet of Things (IoT): A vision, architectural elements, and future directions". In: *Future generation computer systems* 29.7 (2013), pp. 1645–1660.

[177] Partha Bhattacharjee and Goutam Sanyal. "New admission control algorithm based on effective bandwidth for a multi-class network". In: *2008 16th IEEE International Conference on Networks*. IEEE. 2008, pp. 1–6.

Publications From This Thesis

The work discussed in this thesis has led to the following publications.

1 Bakshi Puneet, Sukumar Nandi, "Privacy Enhanced DigiLocker using Ciphertext - Policy Attribute-Based Encryption", 2020, 17th International Conference on Security and Cryptography (SECRYPT), Springer, 2020.

2 Bakshi Puneet, Sukumar Nandi, "Privacy Enhanced Registered Devices for Fine-grained Access Control", 2020, Advanced Computing and Communications (ADCOM), Springer, 2020.

3 Bakshi, Puneet, Neelakantan Subramanian, and Sukumar Nandi. "Using digital tokens to improve amortized performance of eSign", 2018 IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/ DataCom/CyberSciTech), IEEE, 2018.

4 Bakshi, Puneet, and Sukumar Nandi. "Using Privacy Enhancing and Fine-Grained Access Controlled eKYC to implement Privacy Aware eSign", Advances in Science, Technology and Engineering Systems Journal, Vol. 4, No. 4, 347-358, 2019.

5 Bakshi, Puneet, and Sukumar Nandi. "Secure, Privacy Enhanced and Anony-

mous Communication between Vehicle and Infrastructure", Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), IEEE, 2019.

6 Bakshi, Puneet, and Sukumar Nandi. "Privacy Enhanced Attribute based eSign", 6th International Conference on Natural Language Processing, AIRCC, 2020.