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.