ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 4, DOI: 10.29027/IJIRASE.v2.i4.2018, 295-297, October 2018

A Study on Cryptographic Algorithms with Key Size Comparison and Role of Cryptography in Aadhaar Data Security

P.Tamilarasi [1] , S.**Sowmya**[2]
[1,2] Assistant Professor , R.B.Gothi Jain College For Women, Chennai.
tamilmalu@yahoo.com,sowmya.e1988@gmail.com

ABSTRACT: *With the improvement of communication technology a desire for secure communication also arises and that is fulfilled by different data security techniques like cryptography, digital applies, watermarking etc. Cryptography is an data encryption /decryption technique used for network security when different networks are interconnected. It is used to secure the data transmission from attacks and intrusions. Security of data is one of the foremost vital factors of information technology. Aadhaar number is a 12-digit unmistakable number issued by the Indian government to every individual occupant of India. It is distinctive number that will capture all demographic and biometric data, of each resident Indian individual. This paper is split into 6 sections contain components of cryptography, types of encryption algorithms, comparison of algorithms, mode of data security in Aadhaar, encryption techniques applied in Aadhaar, challenges in Aadhaar security.*

Keywords: *Cryptography, Encryption algorithms, Demographic Data, Aadhaar Security.*

1.Introduction

Cryptography is a framework which is wanted to change the data and can be used to give distinctive security related thoughts, for instance, mystery, data trustworthiness, approval, endorsement and non-denial.

1.1 **Components of Cryptographic system: -**

(a) **Plain Text:** It is the secret or confidential data to be secured while transmission.

(b) **Cipher Text:** It is the transformed and changed plain text which is not understandable while merely looking at it.

(c) **Encryption Algorithm:** It is a mathematical step-by-step process used for converting plain text into cipher text based on some encryption key. Different examples of such algorithm are AES, DES, blowfish and serpent etc. It is used at sender's side.

(d) **Decryption Algorithm**: It is exactly the reverse mathematical process of used encryption algorithm. It takes cipher text and decryption key to produce original plain text. It is used at receiver's side.

(e) **Encryption Key**: This key is an esteem that is the lead part of the cryptographic framework which is either known just to sender or to both sender and collector.

(f) **Decryption Key**: This key is the value known to receiver and it may or may not be identical to encryption key. It is applied within decryption algorithm to generate the plain text back from received cipher text. A collection that contains all possible decryption keys is known as Key Space.

2. **Asymmetric Algorithms**

Unbalanced calculations utilize an alternate key to scramble than they do to unscramble. The scrambling key is known as the general population key and the unscrambling key is the private key. There are two unbalanced calculations.

1. RSA- RSA stands for Rivest-Shamir-Adleman. Open key encryption check. RSA is viewed as an uneven estimation in light of its utilization of a few keys. The RSA figuring joins three stages: key age, encryption and disentangling. Key age RSA consolidates an open key and a private key. People when all is said in done key can be known by everybody and is utilized for scrambling messages. Messages encoded with people overall key must be unscrambled in a sensible extent of time utilizing the private key.

2.ECC-Elliptical curve cryptography (ECC) is an open key encryption system dependent on elliptic turn theory that can be utilized to make quicker, more small, and all the more convincing cryptographic keys. ECC makes keys through the properties of the elliptic bend condition rather than the standard technique for age as the result of sweeping prime numbers. ECC can yield a level of security with a 164-piece key that particular structures require a 1,024-piece key to accomplish. Since ECC sets up for all intents and purposes indistinguishable security with lower figuring force and battery asset use, it is twisting up widely utilized for adaptable applications figure1 .

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 4, DOI: 10.29027/IJIRASE.v2.i4.2018, 295-297, October 2018

3.Comparison of Algorithms

Table 1 Comparison of Symmetric Algorithms

Algorithm	Key Size	Block Size	Round	Structure
Blowfish	32-448	64	16	Feistel
AES	128-256	128	10,12,14	Substitution, Permutation
DES	64	64	16	Feistel

Table 2 Comparison of Asymmetric Algorithms

Key Generation Performance			
Key Length(Bits)		Time(S)	
RSA	ECC	RSA	ECC
1024	163	0.16	0.08
2240	233	7.47	0.18
3072	284	9.8	0.27
7680	409	133.9	0.64
15360	571	679.06	1.44

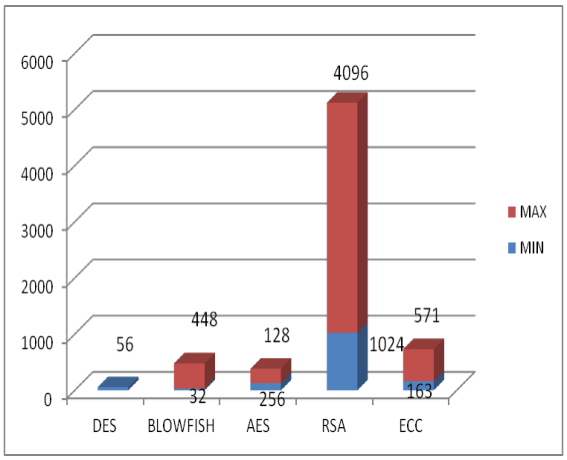

Figure 1 Key Size Comparison

4. Encryption Techniques Applied in Aadhaar

4.1 PID Block

The PID block is then registered with the AUA(Authentication User Agency)s digital key and passed to the ASA(Authentication Service Agency). The ASA then build a API(Application Programming Interfaces) call, with its belonging unique digital identifiers then a success or failure feedback is returned .Each device must be recorded with the UIDAI along with the device provider's Identification, a unique identifier (i.e. serial number), a digitally signed authentication, along with the provider's key will be issued by the UIDAI. All of these analysis are part of the meta-data of the authentication or eKYC request.

4.2 Data Security

There are number of encryption and decryption standards are used in Aadhaar data protection at various levels of Aadhaar data collection. We discussed few of encryption techniques used in Aadhaar data security.

- Demographic data are segregated into independent databases secured between firewalls; a single database does not have all the user's information in one location.
- A Network to the CIDR is only available to ASAs (27 entities) over 1-to-1 dedicated line.
- The PID block is encoded with Advanced Encryption Standard-256 by using a one-time session key. The session key is encoded with a 2048-bit UIDAI issued key. This makes it intensely expensive to break.
- The PID block contains a timestamp and a one-time session key to prohibit an action of reuse.
- The digital key of the certified device, the AUA and the ASA are logged and authenticated for every transaction.
- The session key used for the PID block must not be stocked and should not be rehashed across transactions.
- GCM encryption was added in API v2.0
- Network connectivity between the ASA and AUA must be protected through a dedicated line or at least a VPN/SSL.
- The ASA's duty to guarantee this connectivity demand.
- Multi-factor authentication (using Aadhaar ID,OTP) is also ready for use over the API.
- In this case where self-service is not possible and operator impedance is necessary to operate a device, the operator must be authenticated and their Aadhaar number is logged to accomplish any activity.
- ASA and certified devices do not store PIB blocks beyond a few seconds in cache for buffering. Device applications and ASAs are confirmed by the UIDAI .
- Enrolment client software is entirely written, maintained and provided directly by the UIDAI.

- All meta-data of a request timestamp, the entities involved are made available online for around 6 months.
- The CIDR in its entirety is situated in the middle of India and all certification requests route inside the Country.
- The Aadhaar number itself is arbitrary and is not based on any identifying personal factors of the holder.
- The UIDAI provides the option to generate a further randomized 16-digit Virtual ID for authentication requests. Users should not share their Aadhaar ID with providers. There are no deadline to generate new Virtual IDs for the same Aadhaar, the old one is undoubtedly discarded, and once a new ID is generated.

5. Challenges in Aadhaar Data Security

In this section the issues of data security and requirement analysis for privacy and security. Several issues has been listed in form government analyzation.

A. Security and Privacy Issues in Aadhaar: Aadhaar provides many advantages to individuals, it is not free from privacy and security issues. Many security and privacy issues can occur during several stages of the Aadhaar lifecycle. Security and privacy issues may occur during the collection, transmission and storage of Aadhaar details in the centralized database. These problems have to be taken care of assiduously. Alternatively, many individuals may be affected by a diversity of serious issues.

B. Private Players and Data Leakage: At the beginning, the registrars of Aadhaar collect information of individuals and store the data that is collected from the citizen; this creates a major chance for data leakage or flow. There are many personnel details involved in the entire series of processes of enrollment and generation of Aadhaar numbers before the database finally goes to the government-reserved Central Identities Data Repository. The probity and responsibility of the people involved in the tasks needs to be confirmed.

C. Security and Privacy Challenges in a integrated (centralized) UID Database: The CIDR database is a integrated database that includes data about everything concerning an individual. Snooping and hacking into the database is always e System"

possible. The creation of a enormous centralized database, the transmission of sensitive data over networks in real-time, present important operational and security responsibility. If the database crashed, the entire identification system will be unsuccessful. To avoid this problem, designers should provide high repetition by using parallel systems and mirrors to ensure accuracy and opportunity.

6. Conclusion

Technique to perform supportive counts on encoded data is offered by the field of symmetric open encryption, which engages looking for on mixed data. These calculations created with regards to accessible encryption are very effective and scale well for monstrous estimated information, for example, the UIDAI information. For some, insightful applications, devices and procedures created with regards to accessible encryption seem, by all accounts, to be exceptionally significant.

7. References

[1].Rajesh R Mane, "A Review on Cryptography Algorithms, Attacks and Encryption Tools", International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Vol. 3, Issue 9 (September 2015).

[2]. Anjula Gupta and Navpreet Kaur Walia, " Cryptography Algorithms: A Review", International Journal of Engineering Development and Research, ISSN: 2321- 9939, Volume 2, Issue 2.

[3].Divya Sukhija, "A Review Paper on AES and DES Cryptography Algorithms", International Journal electronics and Computer Science Engineering, ISSN: 2277-1956, V3 N4-354-359.

[4]. Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Crypt ology, vol. 14, p. 255-293, 2001.

[5]. Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.

Key Size Comparison Chart.

[6].Aadhaar Data Security and Authentication Https://uidai.gov.in/authentication/authentication-ove rview/authentication

[7]. Gary C. Kessler "An Overview of Cryptography"

[8]. Nishaal J. Parmar and Pramode K. Verma, "A Comparative Evaluation of Algorithms in the Implementation of an Ultra-Secure Router-to-Router Key Exchang