Aadhaar Security: Creating a secure environment for Third parties and Government

[1]Siddharth Vagrecha, [2]Isha Agarwal, [3]Srushti Singh, [4]Apoorva K A
[1]Student, [2]Student, [3]Student, [4]Asst Professor
Jain Demeed To Be University

***Abstract* - In recent years we had heard about many aadhaar data/information that has been leaked. Largely, data breaches were from third-parties websites and applications. Due to which people have lost their trust on aadhaar card. Aadhaar, which is at most required for every identification process in India, requires a high level of security when sharing with third-parties websites or applications. With that idea, we have proposed a solution to protect aadhaar information on a digital platform. Our work is that aadhaar information must be converted into a HASH value using the hashing algorithm. This HASH value will be verified and authenticated by UIDIA and is stored in their database. This HASH value is sharable on third-party's digital platforms without revealing any personal information of the user/person such as Aadhaar UIN (Unique Identification Number). Thus, if any third-party suffer from cyber threats such as data breaches, the hacker will get only HASH values that cannot be reversed in order to get actual aadhaar information. Hence, we can create a secure environment for Third parties as well as the government.**

***keywords* - Aadhaar Security, Cryptography, Encryption, Hashing Algorithm, Information Security, Database, Web Application, Mobile Application.**

I. INTRODUCTION

The Group of Ministers (GoM) submitted its report in May 2001 in which it accepted the recommendation for an ID card and stated that a "multi-purpose National Identity Card" project would be started soon, with the card to be issued first in border villages and then elsewhere. In late September 2001 the Ministry of External Affairs proposed that a mandatory national identity card be issued. This announcement followed reports that some people had obtained multiple Indian passports with different details. This was attributed to the lack of computerisation between the passport centres. In December 2003 the Citizenship (Amendment) Bill 2003 was introduced in the Lok Sabha by L. K. Advani. It primarily aimed to provide various rights to persons of Indian origin, but the bill also introduced Clause 14 (a) that said: "The Central Government may compulsorily register every citizen of India and issue national identity card to him." [17].

The UIDAI was established on 28 January 2009 after the Planning Commission issued a notification. In April 2010 the logo and the brand name *Aadhaar* was launched by Nilekani. In May 2010 Nilekani said he would support legislation to protect the data held by the UIDAI [17].

A 12-digit unique identification number which is issued by the Indian government to every individual resident of India is known as an Aadhaar which is Unique Identification Number (UIN). The Planning Commission of India is responsible for managing Aadhaar numbers and Aadhaar identification cards, which entirely functions under the Unique Identification Authority of India (UIDAI). The main objective of the Aadhaar was to have a single, unique identification number that would contain all the details, including biometrics and iris scan of an individual resident of India [5],[17].

II. USES

An Aadhaar serves as an essential document when it comes to Know-Your-Customer (KYC), verification and identification purposes. Following are the platforms where Aadhaar is used:

- **Acquisition of passport –** Individuals who wish to obtain a passport, can use their Aadhaar as an identity proof as well as residence proof along with their application [3].
- **Opening bank accounts –** Aadhaar can be used for KYC, identification and verification purposes. Aadhaar is used as a valid address proof and photo ID proof while opening a bank account [3].
- **LPG subsidy –** The Aadhaar number is linked to the 17-digit LPG ID which provides the users with LPG subsidy directly to their respective bank accounts [3].
- **BHIM UPI –** Aadhaar is used as a KYC document for the BHIM UPI (Bharat Interface for Money; Unified Payment Interface) for making transactions online where the bank account is linked directly with applications (PhonePe, Google Pay, Paytm, etc.,.).

III. REAL-TIME AADHAAR DATA BREACHES CASE

As Aadhaar card is a unique number provided to every citizen of India so it is mandatory to link the aadhaar card to the third party (digital platform) like banks, Income tax department or other third party departments [8].

Last year in March 2018, it was noted that Aadhaar data was leaked on a system which was run by a state-owned utility company, Indane that allowed to access sensitive information like a name, bank details, Aadhaar number, on which UIDAI came out with the statement denying the breach and stated that there was absolutely no breach of Aadhaar database and it remains safe and secure by their end. While it is the third party which acts had a weak link and hence the data was leaked [8].

Breaches are happening not because of the core database, rather happening because of insecure government websites and third-parties with API access to the database [8].

Similarly, another case that happened in Telangana where aadhaar details were leaked.
When IT Grids, a company hired by the Telugu Desam Party (TDP) for developing its *Seva Mitra* app, has been found to have allegedly stored the data of 7.82 crore Indians from Andhra Pradesh and Telangana [17].

The Telangana State Forensic Science Laboratory (TSFSL) discovered this during its examination of the data recovered by the Telangana police from the premises of IT Grids (India) Pvt Ltd, on the **suspicion of breach of voter ID and Aadhaar data** according to a *Times of India* report [12],[13].

As per the investigation, it was discovered that the structure and size of the database held by IT Grids was similar to what was owned by the Unique Identification Authority of India (UIDAI) [13].

Another case that happened back in 2017, which is recently identified, that a copy of Aadhaar card owned by 34-year-old Maharashtra techie Ameya was uploaded online by miscreants years ago. Years later when the Ameya tried opening a bank account in 2017, he was told that it wouldn't be possible because his aadhaar card has already been linked to another bank account. He took serious cognizance of the matter and wrote to the concerned bank authorities about a possible Aadhaar fraud [6].

He decided to Google his name and was shocked to find out that a picture of his Aadhaar card had been shared by multiple websites. However, when reported to UIDAI authorities, he was told that they can't change his Aadhaar number and the only way out would be to cancel his card. Still today, he keeps receiving two or three authentication-failure emails, text messages and random calls. Thus, leaked aadhaar information leads to serious problems [6].

There were many more such cases, so our team decided to conduct a survey in order to get people's concerns about Aadhaar information with three basic questions. Questions are as follows:

1. Are you aware about Aadhaar breaches?
2. Is Aadhaar information really secure?
3. Does Aadhaar need more security features while sharing on different platforms (Offline or Online)?

The survey was taken by 130 people, where only 55% of people know about Aadhaar breaches. While asking about Aadhaar security, 35.4% rejected and 27.7% were not sure. Now, on asking about Aadhaar need more security features while sharing it on different platforms, 83% of people agreed. That means people who know about Aadhaar breaches as well as it's security, want more security features as they are not fully sure about aadhaar information security while sharing it online or offline.

IV. LITERATURE REVIEW

Aadhaar is a unique identification card issued to every individual who are citizen of India as it can verify and authenticate user's identity in an easy and cost effective way. The UIDAI works on biometrics where identity is defined as' Who you are' and authentication is defined as ' How you can prove your identity [1].
According to International Journal for Research in Applied Science and Engineering Technology, UIDAI uses biometrics system for authentication but this system might be vulnerable to some potential attacks. Some of such attacks are:
1. Data Leakage and private players: There are sequence of process involved in generating Aadhaar number before the actual database finally goes to the government that is, Central Identities Data Repository (CIDR) where initially, the registrars of aadhaar collect the data of individuals and store it which creates a major chance of for data leakage [1].
2. Human Error: The whole process to issue aadhaar number involves human beings who can cause problem either maliciously or accidently. They may leave the system unlocked [1].
3. Cryptographic Algorithm: Cryptographic algorithms are purchased from different vendors and CIDR is protected by commercial network security. Due to the purchased products, chances for data damage or hacking or eavesdropping increases exponentially [1].
Aadhaar Security is a major concern and so several acts and legislations have been passed to ensure security to the private details of the individuals of India. The data protection are based on amended IT Act, 2008 and some of the following acts are:

1. The Indian Penal Act, 1860
2. The Indian Contract Act, 1872
3. The public Financial Institutions Act, 1983
4. The Indian Telegraph Act, 1885

One of the journal published a paper, which proposed an idea to implement temporary virtual ID for identification process. As it is valid only for a particular time period for time of generation and also be used for single time. While generating this virtual ID, UIDIA might need to maintain more systems to generate this ID, authenticate it, algorithm to make it used only for one time and systems to make it secure [10].
It will make security more complex but at the same time, a time taking job. In order to implement this system some complexions needs to be removed while maintaining security [10].
According to our research Aadhaar's privacy protection will require; a) An independent third party that acts as an online auditor; b) Analysis of the modern tools and techniques of computer science, and; c) The appropriate legal and policy frameworks that

authenticate and identify in a modern digital setting. For example, a new or existing mobile number must be linked to the Aadhaar, Aadhaar must be linked to a new or existing driving license, for existing or new bank accounts/for making transactions above 50,000 and more, etc. Hence, the above features show that Aadhaar is important for every citizen in India. The Attorney General of India (AGI), in the Supreme Court, stated that the citizens of India have no constitutional rights to privacy, to protect the government's stand. Later, the finance minister, passed the Aadhaar as a money bill and announced that "the government pre-supposes privacy as a fundamental right". They also claimed that the security features were improved when compared to the previous version. Supreme Court (SC) provided a verdict that said, "Right to Privacy is fundamental right and it is intrinsic to right to life" (i.e., needs to be protected). The government has taken many steps to solve the issue of leaking of information, for example, the use of Virtual Identification (VID, 16-digit number) in organizations and local government offices to preserve the privacy of an individual. Honourable Supreme Court stated that Aadhaar must be linked to the PAN card and not with the bank account directly (for KYC purpose) [9].

This resulted in confusion about the impact on privacy of the Aadhaar. The main concerns about the security and privacy of Aadhaar are as follows:

- An individual can be identified and authorized without revealing the unique Aadhaar number or demographic and biometric data [9].
- Tracking people with legal provisions (i.e., with the permission of the government), mass surveillance and protection from inside attacks or external hacks [9].
- A solution to some crucial questions regarding the safety of Aadhaar:
    1. Is there any way to protect an individual's data or information that is present on the UIDAI database? For example, a software or a mechanism.
    2. Is it possible to ensure that the transactions, investigation and analytics are carried out in a safe way either through auditing or pre-approved and tamper proof computer programs? Are the programs legal and true to policy frameworks?
    3. Is there a strategy for recovering lost data or protect the revealed data?

The government needs to consider the following points:

- Unique Identification Database must be designed as critical infrastructure along with the testing of all Aadhaar enabled applications with respect to security.
- Mobile phones and laptops must be ensured with device level encryption along with a novel encryption policy for Aadhaar enabled applications.
- To prevent attacks on Aadhaar database a Computer Emergency Response Team (CERT).
- Tie up with private sectors like International Electronic and Electrical Engineers (IEEE) and the Internet Engineering Task Force (IETF) or Internet Society to create unique security standards/platforms.

There are several problems with the Aadhaar:

- Privacy concerns from Aadhaar leaks.
- The cost of the Aadhaar project.
- Coercion to register for Aadhaar-voluntary and mandatory.
- No legal basis for the UID project.
- False claims of preventing corruption.
- The new bailout plan for banks.
- Potential for misuse.
- Illegal immigration and terrorism.
- Unauthorized use of Aadhaar cards.
- Irrelevant storage of Aadhaar data

SWOT ANALYSIS:

STRENGTHS:

The unique identification numbers provide an identity to those who need it the most, i.e., the poor and the marginalized people living in the rural areas [7].

WEAKNESS:

The Aadhaar project is stated as unconstitutional since it is neither supported by any law nor does it safeguard the civil liberties of citizens. Initially, UIDAI stated that UID number is optional but now the government has made it mandatory. Since the crimes pertaining to Aadhaar are increasing with time it has been proved that the Aadhaar and UIDAI are most offensive tools of civil liberty violations in India [7].

OPPORTUNITIES:

The Aadhaar project serves as opportunities for IT hardware as well as software companies that will run the system. The equipment that is required for enrolment centres costs about 3 lakh Rupees which when multiplied by 350-400 will be equal to the costs for a single district. Therefore, enrolment in a single district will cost about 10 crore Rupees-12 crore Rupees. This does not include the cost that is required to get people to enrol through the State machinery, the logistics or the administrative expenses. Introduction of smart cards can also be an advantage to the government [7].

THREATS:

Aadhaar cards enable all the personal detail of individual to be available at any point. This eases the task of hackers as they can steal any personal information of an individual for any wrong purpose. Corruption is another potential incentive for an official to leak any kind of information from the database. Also, human error cannot be removed completely which can limit the success of the project [7].

AADHAAR PAY:

As a result of demonetization, that took place on 8 November 2016, many queued up to exchange money and withdraw the new currency from the bank and ATM. Therefore, cashless transaction came into existence. Many applications came into picture like Paytm, Google Pay and PhonePe. Aadhaar card cashless transaction also came into existence where the user simply enters their Aadhaar card number and the amount would be debited from their account directly. IDFC Bank Ltd becomes the first Indian Bank to launch Aadhaar Pay 28. IDFC bank launched its first biometric enabled transaction method in which the person pays the merchants using his/her fingerprint. This idea was implemented for those who didn't have smart phones or if owning one, but without banking features. Syndicate Bank, Punjab National Bank, Bank of Baroda and IndusInd Bank will also start Aadhaar Pay soon [2].

The finance minister announced that government marks privacy as a fundamental right while getting the aadhaar bill passed as money bill and also claimed that the bill has strict privacy when compared to previous version (Scroll Staff, 2016) [11].

But, not the government neither the UIDAI made clear about the privacy concerns that are addressed and the methods been deployed [11].

The important questions "whether the breach of privacy is inevitable and whether any technological aspects can make aadhaar safe" have not been answered adequately [11].

V. HASHING

Hashing is a method of cryptography that converts any form of data into a unique string of text. Hash function that is suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size and is a one-way function. One-way function means a function which is practically infeasible to invert (to its original message).

VI. HASHING ALGORITHM

SHA-256

SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2) and is one of the strongest hash functions available. SHA-256 is not much more complex to code than SHA-1 and has not yet been compromised in any way. The 256-bit key makes it a good partner-function for AES. It runs for 64 rounds and performs operations AND, XOR, ROT, ADD(mod 2_{32}), OR and SHR [4],[15].

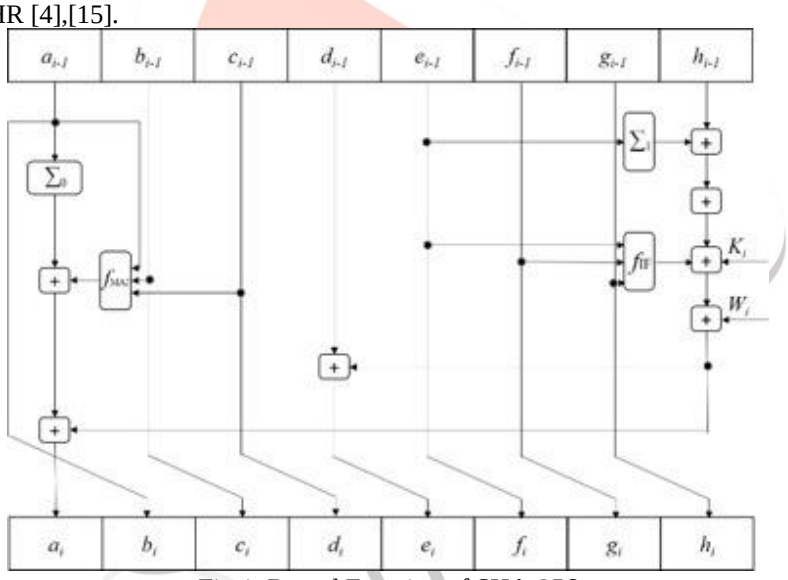

Fig 1: Round Function of SHA-256

SHA-512

SHA-512 is a kind of 'signature' or unique 512-bits (64 bytes) code for a text or data file. SHA-512 generates an almost-unique 512 bits or 64 bytes hash for given data. It is represented in hexadecimal (0-9 and A-F). As it is 64 bytes hash value, makes very difficult to reverse the process to get original data. It runs for 80 rounds and performs operations AND, XOR, ROT, ADD(mod 2_{64}), OR and SHR [4],[15].

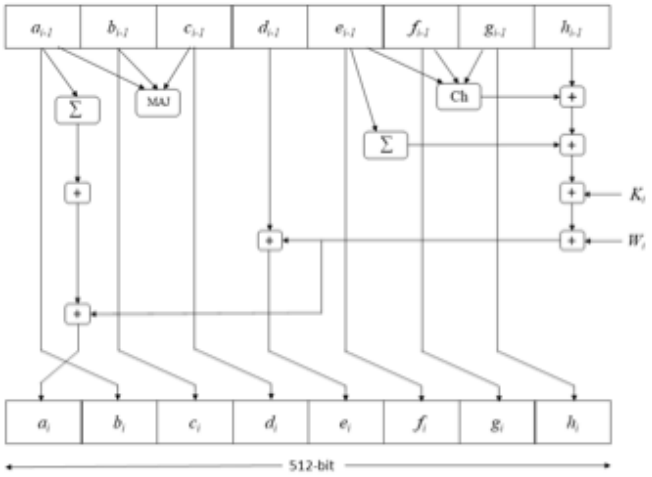

Fig 2: Round Function of SHA-512

MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value (16 bytes). Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It runs 4 rounds [15],[16].

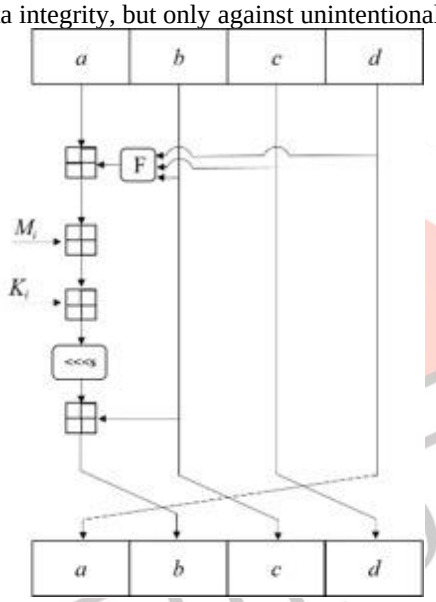

Fig 3: Round Function of MD5

VII. PROPOSED METHODOLOGY

Our solution for the above real-time threats is to implement a secure environment for Government and Third-Parties to verify the user identity over the internet without providing the actual Aadhaar information. Instead of providing the actual aadhaar information, we can provide a HASH value which is generated using a hashing algorithm that contains aadhaar information such as Name, Address, Date of Birth and Aadhaar UIN. This HASH value will be verified by the UIDAI. Using this HASH value, third parties can identify users over their websites or network for KYC purposes.

So, if any third party suffers from any kind of data breach, aadhaar information will be leaked as hash values that cannot be reversed in order to get actual aadhaar information.

Thus, it creates a secure environment for government and third parties where information will be protected and follows CIA model.

VIII. IMPLEMENTATION PROCESS

Our proposed implementation is web-based and same can be implemented on mobile application. In the implementation we need following servers and systems:

- Web server (supported with php and MySQL)
- Database server
- SHA-512 hash value generator (Java or Python)

Our implementation is to demonstrate SQL Injection (most common threat found on third parties websites and applications). We have created a website which contain a form. This form accepts following details:

- Name
- Hash value
- Submit Button

Form's information will be stored in database server (MySQL) using POST method (php). Now to demonstrate SQL Injection (Database Breach). Our website is vulnerable to SQL Injection. Our team conducted SQL Injection on our vulnerable website in order to leak aadhaar database.

When we compromised our website, as the result, aadhaar information was leaked in the form of Hash Value. Thus, hacker will get only HASH value which is very difficult the reversed it in its original information.

IX. WORKING

To overcome problems like data breaches over government and third-parties websites, aadhaar information will be converted into a hash value using a hashing algorithm such as SHA-256, SHA512 and MD5.

Our work emphasis on the usage of SHA-512 to generate HASH value as it is most secure amongst. Once the hash value is generated, the information stored in hash value needs to be authenticated. The UIDAI authorities would verify and authenticate the hash value in the same manner, they used to verify and authenticate aadhaar information.

Once UIDAI verifies and authenticates the HASH value, it must be stored in their database so that it can be cross-matched to verify the identity from the user/person. Now, when a user gives this hash value to any third-party's platform (including websites, mobile apps, etc.,.) it can be used to verify user identity without revealing their personal information as well as aadhaar number. Instead of storing user's aadhaar number, the third-parties can store these hash values. This will create a secure environment for users as well as third parties who deal with sensitive information.

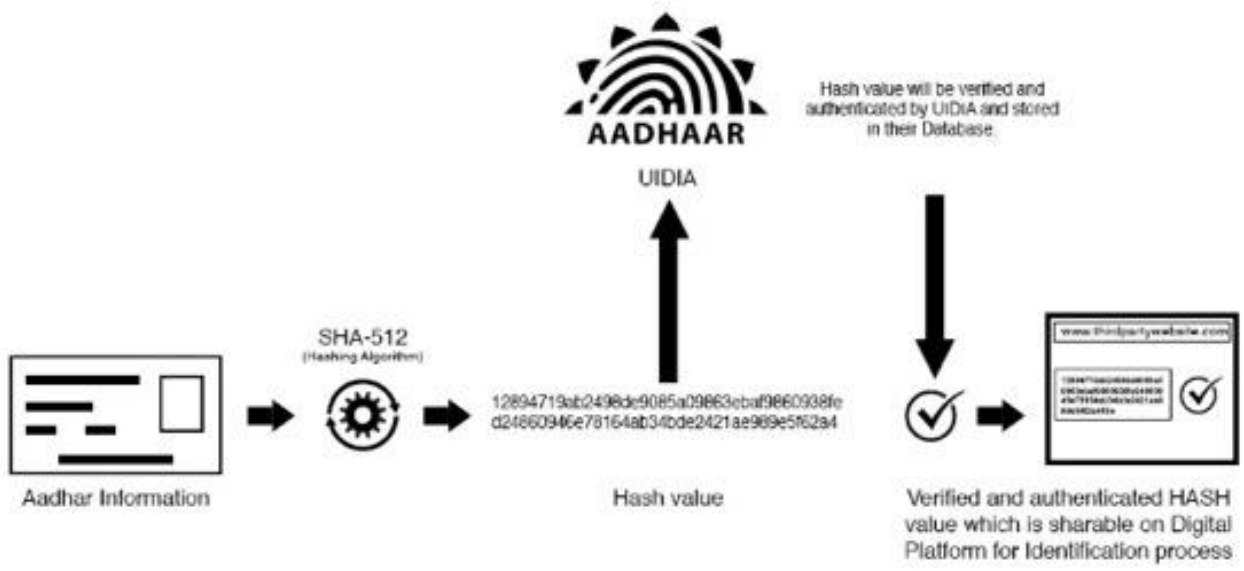

Fig 4: How hash value will generate and sharable

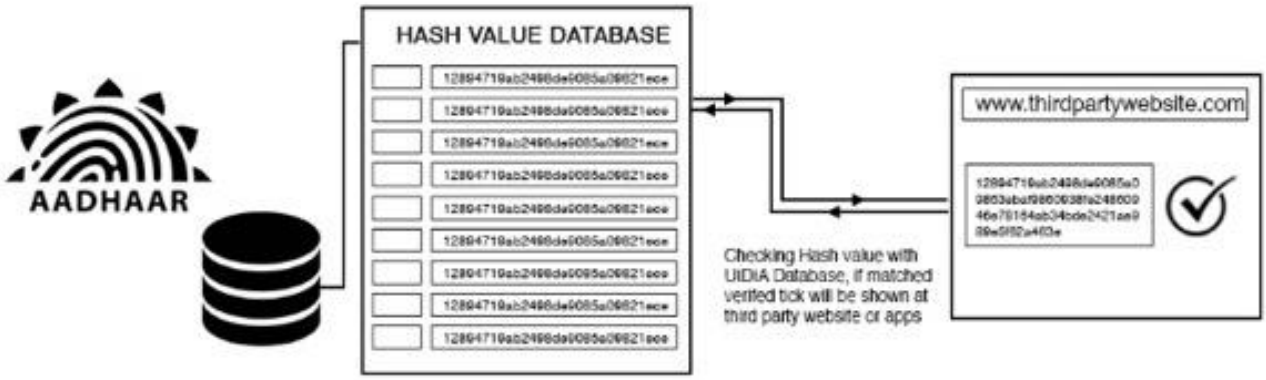

Fig 5: Checking hash value with the UIDIA database to verify User Identification

X. CONCLUSION

As the aadhaar information is converted into the hash values it makes it difficult for the hackers to reverse the hashing process in order to get actual information. As aadhaar number is linked to Bank Accounts, PAN information, SIM cards, and many more sensitive things, it makes difficult for hackers to gain those aadhaar number to gather information related to user's bank account and so on. Thus, in order to get aadhaar number, hackers must reverse the hash value which is a time taking (months or years) and difficult process. The future work can be extended with the implementation of encryption process after generating the hash value.

XI. REFERENCES

[1] A.K.R.S. Anusha and Dr. G. Rajkumar, "Privacy and Security Issues in Aadhaar", Available Online: www.ijraset.com, ISSN: 2321-9653; IC Value 45.98: Volume 5 Issue VIII, August 2017
[2] Amit Kumar Tyagi, G. Rekha and N. Sreenath, "Is Your Privacy Safe with Aadhaar?: An Open Discussion", 5th IEEE International Conference on Parallel, Distributed and Grid Computing (PGDC-2018), 20-22 Dec, 2018, Solan, India.
[3] Bankbazaar, "Uses and Benefits of Aadhaar Card", Available Online: https://www.bankbazaar.com/aadhar-card/benefits-of-aadhar-card-govt.html
[4] Chris Veness, "SHA-256 Cryptographic Hash Algorithm", Available online: https://www.movable-type.co.uk/scripts/sha256.html
[5] Margaret Rouse, "Aadhaar", Available Online: https://whatis.techtarget.com/definition/Aadhaar
[6] Moneycontrol, " 'Living hell' says techie whose Aadhaar card image was shared online.", Available online: https://www.moneycontrol.com/news/india/living-hell-says-techie-whose-aadhaar-card-image-was-shared-online-4783181.html, Jan 3, 2020
[7] Mugdha Patil, "Analytical Study of Privacy And Security Ways Of Aadhaar, Volume-4 Issue- 5, 2018, IJARIIE-ISSN (O):2395-4398.
[8] Nilesh Christopher, "Security experts say need to secure Aadhaar ecosystem, warn about third party leaks", Available online: https://economictimes.indiatimes.com/news/politics-and-nation/there-is-a-need-to-secure-full-aadhaar-ecosystem-experts/articleshow/63459367.cms, Mar 26, 2018
[9] Raja Siddharth Raju, Sukhdev Singh and Kiran Khatter, "Aadhaar Card: Challenges and Impact on Digital Transformation".
[10] Shaurya Shekhar and Vasantha W B, "Privacy and Security in Aadhaar", IJEDR 2018, Volume 6, Issue 4, ISSN: 2321-9939, October 2018.
[11] Shweta Agarwal, Subhashis Banerjee and Subodh Sharma, "Privacy and Security of Aadhaar: A Computer Science Perspective", Volume 52 Journal: Economic and Political Weekly, 16th September 2017.
[12] Srinath Vudali, "Aadhaar details of 7.82 crore from Telangana and Andhra found in possession of IT Grids (India) Pvt Ltd", Available Online: https://timesofindia.indiatimes.com/city/hyderabad/aadhaar-details-of-7-82-crore-from-telangana-and-andhra-found-in-possession-of-it-grids-india-pvt-ltd/articleshow/68865938.cms, Apr 13, 2019.
[13] tech2 News Staff, "Aadhaar security breaches: here are the major untoward incidents that have happened with aadhaar and what was actually affected", Available online: https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html, SEP 25, 2018
[14] tech2 News Staff, "Aadhaar data leak: Details of 7.82 cr Indians from AP and Telangana found on IT Grids' database", Available online: https://www.firstpost.com/india/aadhaar-data-leak-details-of-7-82-cr-indians-from-ap-and-telangana-found-on-it-grids-database-6448961.html, Apr 15, 2019
[15] Wikipedia, "Secure Hashing Algorithm", Available Online: https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
[16] Wikipedia, "MD5", Available Online: https://en.wikipedia.org/wiki/MD5
[17] Wikipedia, "Aadhaar", Available Online: https://en.wikipedia.org/wiki/Aadhaar