Journal of Information Systems Engineering and Management
2025, 10(11s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Method of Designing Authentication Scheme for Aadhaar User

Dr. Swapnil S Ninawe[1], Dr. Pavithra G.[2], Dr. T.C. Manjunath[3*], Dr. Sandeep K.V.[4], Dr. Iffath Fawad[5], Chetan Umadi[6], Padmavathi M.[7], Ashwini Gowda H.B.[8]

[1, 7, 8,] Assistant Professor, Electronics and Communication Engineering
Dayananda Sagar College of Engineering, Bengaluru, Karnataka
[2] Associate Professor, Electronics and Communication Engineering,
Dayananda Sagar College of Engineering, Bengaluru, Karnataka
[4, 5, 6] Assistant Professors, Electronics & Telecommunication Engineering
Dayananda Sagar College of Engineering, Bengaluru, Karnataka
*[3 *] Professor, Dept. of Computer Science & Engineering,*
IoT, Cyber Security & Blockchain Technlogy,
Dean Research (R & D), Rajarajeswari College of Engineering, Bangalore, Karnataka
* corresponding author, Dr. Manjuath, Ph.D. (IIT Bombay), tcmanju@iitbombay.org

ARTICLE INFO

Received: 12 Nov 2024

Revised: 27 Dec 2024

Accepted: 14 Jan 2025

ABSTRACT

The Unique IDentification (UID) project is the flagship of government of India. The UID number or aadhaar number, which is a twelve-digit number, is issued by UID Authority of India (UIDAI) for all the citizens of India. Nowadays, government of India has made mandatory to connect aadhaar cards to other government issued documents such as bank passbook, PAN card, ration card, driving licence, SIM card, etc. Connecting aadhaar number to different social schemes has helped government in detection of multiple user accounts across different schemes. But this itself is not enough, since many users utilise social scheme facility for different purposes such as ration, subsidy, acquiring loan, special concessions, interest rates, etc. Presently there is no method at place, which can find out which social scheme authority must receive what information about users. In this paper, we propose a novel authentication scheme for revealing appropriate user information to social scheme authority. The method involve use of aadhaar number which is connected to user's name, gender, address, mobile number, etc. The designed system is simulated over authentication of a group of users across different social schemes. Our method can be used as a tool for securely authenticating officials for disclosure of user information.

Introduction: A Method of Designing Authentication Scheme for Aadhaar User - focuses on enhancing secure data sharing through Aadhaar. The paper proposes a novel authentication system to disclose specific user information to social scheme authorities, ensuring appropriate and secure access. By leveraging Aadhaar's connectivity with user data, the scheme facilitates precise authentication for various social benefits. The simulated method demonstrates secure and efficient data authentication for multiple schemes.

Objectives:

The primary objective of this study is to design and develop a novel authentication scheme that securely manages the disclosure of Aadhaar-linked user information to various social scheme authorities. The proposed system aims to address the lack of existing methods for determining which information should be shared with specific authorities based on the social schemes they govern. By leveraging the Aadhaar database, which contains user details such as name, gender, address, and mobile number, the scheme ensures precise and secure authentication.

Methods: The proposed method involves the development of a secure authentication scheme utilizing Aadhaar numbers as the primary identifier, linked to user-specific details such as name, gender, address, and mobile number. The system is designed to authenticate users based on their eligibility for various social schemes and ensure that only the necessary information is disclosed to the respective scheme authorities. This approach incorporates data encryption and access control mechanisms to protect sensitive user data and prevent unauthorized access. The method is simulated on a group of users, testing the authentication process across multiple social schemes to evaluate its efficiency and security. The simulation results demonstrate how the system enables precise information sharing, ensuring compliance with privacy regulations and enhancing trust in Aadhaar-based authentication processes.

Results: The proposed simulation results demonstrate the effectiveness and reliability of the authentication scheme in securely managing Aadhaar-based user information across various social schemes. The simulation involved a diverse group of users, each with unique eligibility criteria for specific government schemes such as subsidies, loans, and concessions. The system successfully authenticated users by verifying their Aadhaar-linked details and disclosed only the necessary information to the corresponding scheme authorities. The results highlighted the scheme's ability to prevent unauthorized access and protect user privacy through encryption and access control mechanisms. Additionally, the simulation confirmed the scheme's efficiency in handling multiple user authentications simultaneously, with minimal processing delays and accurate data sharing. These findings validate the potential of the proposed method to enhance the security and functionality of Aadhaar-based authentication systems.

Conclusions: The study presents a novel Aadhaar-based authentication scheme designed to securely and efficiently manage the disclosure of user information to various social scheme authorities. By leveraging encryption, access control mechanisms, and Aadhaar-linked user details, the method ensures accurate, privacy-preserving data sharing tailored to the requirements of individual schemes. The simulation results validate the scheme's effectiveness in authenticating users, safeguarding sensitive data, and streamlining access to government benefits. Overall, the proposed authentication framework offers a robust solution to address existing gaps in Aadhaar-based information management, enhancing security, trust, and operational efficiency.

Keywords: Aadhaar, Authentication, Certificate, Information, Social Schemes, User.

INTRODUCTION

In this paper, a method of designing authentication scheme for aadhaar user is presented. According to the statistics published in [5], India has already crossed 1 billion population. With such a steadily growing populated country, the use of multiple identity cards is not a viable option in providing social schemes for the benefit of people. Also, government of India or state government has to keep multiple records of social scheme users, which creates problems in implementing as well as managing social schemes. In order to counter these challenges, the Government of India (GOI) formed Unique Identification Authority of India (UIDAI) under the leadership of Mr. Nandan Nilekani. The UIDAI is accountable for issuing Unique IDentification (UID) number or aadhaar number for citizens of India. In order to acquire this 12-digit number, the citizens have to furnish their name, gender, address, etc. In the case of minor, the details of father, mother or guardian has to be mentioned. The UIDAI in turn scans finger prints as well as iris of citizens, and keeps the data safe in the repository. The aadhaar card then be used for opening bank account, acquiring SIM card, gas subsidy, etc. The operator at the counter enters 12-digit aadhaar number, and subsequently scans fingerprints for establishing identity of the user. On operator’s terminal, all user information is displayed irrespective of the social scheme the user has opted for. This can create serious issue because all user information is disclosed. A malicious operator can save all user information and may sell them to third party. Presently, aadhaar is facing too many obstacles, as mentioned above, despite of its benefits. This scheme will enhance the e-governance [1], and will enable entire digital ecosystem that includes direct transfer of subsidy to banks, insurance, employment schemes, etc.

1.1 Proposed Idea

In this paper, we proposed a novel authentication scheme for disclosure of appropriate user information. The proposed scheme reveals appropriate user information to proper authority where user has applied for social schemes.

1.2 Organisation of the Paper

The organisation of the rest of the paper is as follows. Section 2. covers some of the existing authentication schemes, where we discuss different schemes along with their advantages and disadvantages. The design of an authentication scheme for aadhaar user information is described in Section 3., followed by design for various social schemes in Section 4. Simulation results and conclusion are presented in Section 5 and Section 6, respectively.

2. Some of the Existing Authentication Schemes

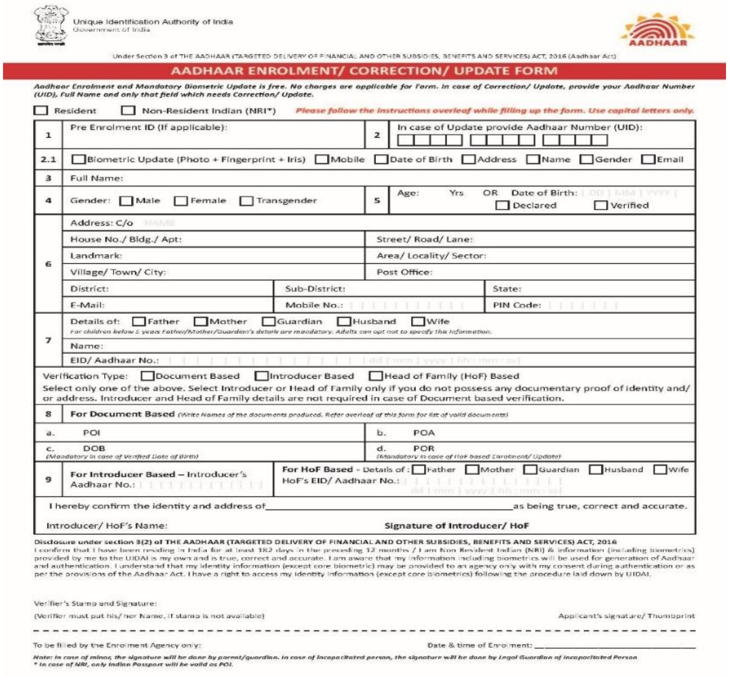
Group signature could be used for anonymous communications (shown by Chaum and van Heyst [2]). A group-signature scheme allowed a user of a group to anonymously sign a message on behalf of the group. This kind of scheme could provide unlinkability, anonymity and traceability. But a group leader was required for disclosing the original user's signature in the case of disputes. A method was studied in [3] for assessing network authentication risk and cyber-attack mitigation within an enterprise network using bipartite authentication graphs. The study demonstrated the value of the graph-based approaches on a real-world authentication data set. The main disadvantage of the method was its applicability, and also, they did not consider basic user parameters. A new authenticated key exchange pro- tocol was shown in [4] based on the exclusive secrets shared between friends. The protocol provided identity authentication and key exchange in a plain setting [10].

The protocol was also human error-tolerant. But the protocol required traditional approach where exclusive secrets were required to authenticate a user. The main advantage of the protocol was its efficiency, but its applicability was limited in nature. Some researchers have used pseudonym-based authentication for disclosing identity of users. But, the computation burden on system increased linearly due to factors such as public key, signature and certificates. The updation of public-private key was to be carried out every-time when the user's pseudonym was changed. Few researchers also proposed centralised approach for reducing computational burden on systems [7]. On the other hand, some researchers suggested independent user-based authentication. Both schemes were not easily scalable, and also centralised structure had the problem of single point of failure [9].

However, none of the schemes are effective for disclosing proper information to authorities. The reason is because a proper mechanism is not at place to understand which user information is to be disclosed while user applying for a particular social scheme [8].

3. Authentication Scheme for Aadhaar User Information

A typical aadhaar enrolment form is shown in Figure 1 (source: https://uidai.gov.in/). After filling the forms, a user is assigned a 12-digit aadhaar number. Whenever a user want apply for social schemes, the quotation of aadhaar number is mandatory. Now, for accessing social schemes, a user has to furnish aadhaar number. Also, first and foremost thing to establishing an identity of user is through biometric authentication [7].



Unique Identification Authority of India
Government of India

AADHAAR

Under Section 3 of THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016 (Aadhaar Act)

AADHAAR ENROLMENT/ CORRECTION/ UPDATE FORM

Aadhaar Enrolment and Mandatory Biometric Update is free. No charges are applicable for Form. In case of Correction/ Update, provide your Aadhaar Number (UID), Full Name and only that field which needs Correction/ Update.

□ Resident □ Non-Resident Indian (NRI*) *Please follow the instructions overleaf while filling up the form. Use capital letters only.*

1 Pre Enrolment ID (If applicable):

2 In case of Update provide Aadhaar Number (UID): □□□□ □□□□ □□□□

2.1 □ Biometric Update (Photo + Fingerprint + Iris) □ Mobile □ Date of Birth □ Address □ Name □ Gender □ Email

3 Full Name:

4 Gender: □ Male □ Female □ Transgender

5 Age: Yrs OR Date of Birth: DD | MM | YYYY
□ Declared □ Verified

6 Address: C/o NAME
House No./ Bldg./ Apt:
Street/ Road/ Lane:
Landmark:
Area/ Locality/ Sector:
Village/ Town/ City:
Post Office:
District:
Sub-District:
State:
E-Mail:
Mobile No.:
PIN Code:

7 Details of: □ Father □ Mother □ Guardian □ Husband □ Wife
For children below 5 years Father/Mother/Guardian's details are mandatory. Adults can opt not to specify this information.
Name:
EID/ Aadhaar No.: dd | mm | yyyy | hh : mm : ss

Verification Type: □ Document Based □ Introducer Based □ Head of Family (HoF) Based
Select only one of the above. Select Introducer or Head of Family only if you do not possess any documentary proof of identity and/ or address. Introducer and Head of Family details are not required in case of Document based verification.

8 **For Document Based** *(Write Names of the documents produced. Refer overleaf of this form for list of valid documents)*
a. POI
b. POA
c. DOB *(Mandatory in case of Verified Date of Birth)*
d. POR *(Mandatory in case of HoF based Enrolment/ Update)*

9 **For Introducer Based** – Introducer's Aadhaar No.:
For HoF Based - Details of : □ Father □ Mother □ Guardian □ Husband □ Wife
HoF's EID/ Aadhaar No.: dd | mm | yyyy | hh : mm : ss

I hereby confirm the identity and address of ____________________ as being true, correct and accurate.

Introducer/ HoF's Name:
Signature of Introducer/ HoF

Disclosure under section 3(2) of THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016
I confirm that I have been residing in India for at least 182 days in the preceding 12 months / I am Non Resident Indian (NRI) & information (including biometrics) provided by me to the UIDAI is my own and is true, correct and accurate. I am aware that my information including biometrics will be used for generation of Aadhaar and authentication. I understand that my identity information (except core biometric) may be provided to an agency only with my consent during authentication or as per the provisions of the Aadhaar Act. I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI.

Verifier's Stamp and Signature:
(Verifier must put his/ her Name, if stamp is not available)
Applicant's signature/ Thumbprint

To be filled by the Enrolment Agency only:
Date & time of Enrolment: ________________

Note: In case of minor, the signature will be done by parent/guardian. In case of Incapacitated person, the signature will be done by Legal Guardian of Incapacitated Person
** In case of NRI, only Indian Passport will be valid as POI.*

Fig. 1: Aadhaar enrolment form

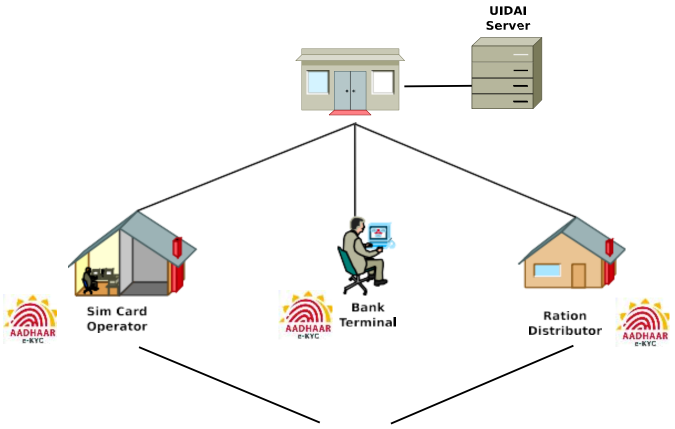


Fig. 2: Authentication using aadhaar through e-KYC for accessing social schemes

A typical authentication of a user at different social scheme terminal is shown in Figure 2. We consider three such social schemes such as bank terminal, SIM card operator and ration distributor. The user has to provide his 12-digit aadhaar number to operator. Social scheme authorities have biometric authentication device which recognises fingerprints as inputs. These authorities are connected to UIDAI main office which has stored user information on servers. UIDAI pre-authenticates authorities and allows them to view user information upon successful authentication through a biometric device installed on terminal. We consider fields in the aadhaar form for i^{th} user as a set of attributes given by

$$Info_i = \{info\ 1, info\ 2, \dots\dots, info\ m\} \ (1)$$

where *info* 1 could be name, *info* 2 could be email address, and so on. Subsequently, we define weight *of* each information for a particular social scheme as

$$\sum_{p=1}^{m} W^{ss}_{info\ p} = 1 \ (2)$$

Consider that a k^{th} social scheme requires l number of user attributes as

$$SS_k = \{info\ 1, info\ 3, \dots\dots, info\ L\} \ (3)$$

Hence, the requirement of attributes of a user a_i for a particular k^{th} social scheme is given by

$$a_i^k = Info_i \cap SS_k \ (4)$$

and corresponding weight of an i^{th} user for a particular k^{th} social scheme is given by

$$W_{a_i^k} = \sum_{p=1}^{n} W^{ss}_{info\ p} \ (5)$$

where $\forall p\ s.t. (info\ p\ \in\ Info_i) \cap (info\ p\ \in\ SS_k) \neq \varphi$

Whenever a z^{th} new social scheme is declared and requires association with x^{th} and y^{th} social schemes, the a_i information disclosure for z^{th} social scheme is given by

$$q^z = Info_i \cap \left(SS_x \cup SS_y\right)$$

Table 1: Notations and their meaning used in the proposed scheme.

Notation	Meaning
a	User
$UIDAI\ \ or\ \ u$	Unique IDentification Authority of India
$SSP\ \ or\ \ s$	Social Service Provider
E_{ksu}	Encryption using shared secret key between s and u
N_{su}	Nonce for the message between s and u
K_{su}	Shared secret key between s and u
M_{su}	Encrypted message from s to u
$H(K_{su})$	Hashing of the shared secret key Ksu
D^u_{su}	Decryption at u using key between s and u
C_a	Certificate of a user

E_{kas}	Encryption using shared secret key between a and s
CF_a	User information
$H()$	Hash function
$K_{as} = K_{sa}$	Shared secret key between a user and s
D_{as}^{s}	Decryption at s using secret key between a and s
$A(a)$	Initial authentication of a user
$A(a)'$	Updated authentication of a user
C_a	Certificate of a user
M_{as}	Encrypted message from a to s

Similarly, $W_{U_i^z}$ can also be calculated as be shown in the equation (5).

We now propose the authentication scheme which has two levels of authentication. In the first level, the UIDAI assigns the authentication certificate for all the users. Subsequently when the user wants to acquire social services, the authentication certificate is updated by UIDAI. We found that this way of certification will enforce the uniformity among all the users who want to access different social schemes. Some of the notations used in the authentication of users are shown in Table 1.

3.1 Level 1: Authentication Certificate Generation for a User By The UIDAI

The UIDAI gathers user information, and assigns the authentication certificate by using the following 3 steps.

Step 1: Initially, a user "a" computes the nonce (N_{au}), and the encryption of (N_{au}) and CF_a using K_{au} is performed. Also, hashing of the shared secret key (K_{au}) between the user and the UIDAI is carried out.

$$M_{au} = E_{K_{au}}(N_{au}||CF_a)\ ;\ K_{au1} = H(K_{au})\ (6)$$

Step 2: At the UIDAI, the decryption of M_{au} using the shared secret key (K_{au}) along with the verification of the user is realised. Also, hashing of the shared secret key (K_{au}) between the user and the UIDAI is carried out.

$$D_{au}^{u} = D_{Kau}(M_{au});\ K_{au1} = H(K_{au})\ (7)$$

Now, the encryption of the nonce (N_{ua}) and the authentication certificate of the user (C_a) using K_{ua} is performed.

$$M_{ua} = E_{k_{ua}}(N_{ua}||C_a)\ (8)$$

Step 3: At the user, the decryption of M_{ua} using the shared secret key (K_{ua}) is realised, and the

$$D_{ua}^{a} = D_{kua}(M_{ua})\ (9)$$

Now, when the user want to acquire social services, the user carries this authentication certificate to a par ticular service provider. The service provider in turn contacts UIDAI who updates the certificate for that particular service.

3.2 Level 2 : Updation of authentication certificate of user by the UIDAI for a particular social scheme

The UIDAI gathers a particular social scheme information and updates authentication of a user with respect to a particular social scheme as follows.

Step 1: Initially, a social scheme provider (s) computes a nonce (N_{su}), and the encryption of (N_{su}) and C_a using K_{su} is performed. Also, hashing of the shared secret key (K_{su}) between s and u is carried out.

$$M_{su} = E_{k_{su}}(N_{su}||C_a)\ ;\ K_{su1} = H(K_{su})\ (10)$$

Step 2: At u, the decryption of M_{su} using the shared secret key (K_{su}) along with the verification of the user is achieved. Also, hashing of the shared secret key (K_{su}) between s and u is performed.

$$D_{su}^{u} = D_{Ksu}(M_{su});\ K_{su1} = H(K_{su})\ (11)$$

Now, the encryption of the nonce (N_{us}) and the updated authentication certificate of the user C_a' using K_{us} is carried out.

$$M_{su} = E_{K_{su}}(N_{us}||C'_a) \text{ (12)}$$

Step 3: At s, the decryption of M_{us} using the shared secret key (K_{us}) is achieved, and the updated authentication certificate of the user (C′) is acquired.

$$D^u_{su} = D_{Kus}(M_{us}) \text{ (13)}$$

Hence, in summary, the authentication of a user is the sum of initial authentication of a user and updated authentication of a user.

$$A'(a) = A(a) + A(a)' \text{ (14)}$$

3.3 Level 3 : Authentication Certificate Size

The authentication certificate size of a user "a" varies based on basic information of a user, social schemes accessed and updation of certificate. General formula for calculation of the certificate size of a user "a" is given as

Authentication certificate size (a)

= User Name + Address + Time Stamp + DOB + Issuing Authority + Family Members Details + Signature Algorithm + Validity + Other Attributes

= UN+Addr+TS+DOB+IA+FMD+SA +V +Atrr (15)

Typically, Actor Name (UN) is considered to be of 15 Bytes, Address (Addr) is 30 Bytes, Time Stamp (TS) is 4 Bytes, DOB is of 2 Bytes, Issuing Authority (IA) of 5 Bytes, Family Members Details (FMD) is variable in size, Signature Algorithm (SA) is 25 Bytes, Validity (V) is 4 Bytes, and Other Attributes (Atrr) is variable in size. The maximum authentication certificate size of a user is given by

Authentication certificate size (a)

= UN + Addr + TS + DOB + IA + FMD + SA + V + Atrr 15 + 30 + 4 + 2 + 5 + 80 + 25 + 4 + 80

= 245 Bytes (16)

4 Design of Authentication Scheme for Aadhaar User In formation for Various Social Schemes

We now describe social schemes along with necessary aadhaar user information. Table 2 shows aadhaar user information along with their corresponding weight for a particular social scheme. Bank terminal: Opening of a bank account requires name, gender, DOB and address of a user. Once the bank account is opened, the transactions are autho rised at terminals using *e*-KYC. Thus, we have

$$SS_b = \{info\ 1, info\ 2, info\ 3, infor\ 4\} \text{ (17)}$$

$$Info_i = \{info\ 1, info\ 2, infor\ 4\} \text{ (18)}$$

$$a_i^b = \{info\ 1, info\ 2, info\ 4\} \text{ (19)}$$

$$a_i^b = \{w^b_{info1} + w^b_{info2} + w^b_{info4}\} = 0.5 \text{ (20)}$$

SIM card operator: Subscriber Identification Module (SIM) cards are a smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if re moved. For acquiring SIM cards at any operator, the operator should establish name, gender, address and DoB of users. They are no.1, no. 2, no. 3 and no. 4 fields in the aadhaar form. We have

$$SS_c = \{info\ 1, info\ 2, info\ 3, infor\ 4\} \text{ (21)}$$

Thus,

$$a_i^c = \{info\ 1, info\ 2, info\ 3, info\ 4\} \text{ (22)}$$

$$W_{a_i^c} = \sum_{p=1}^{4} W^c_{info\ p} = 0.43 \text{ (23)}$$

Now, consider that for using a new social scheme, bank details and SIM card details are required.

Thus,

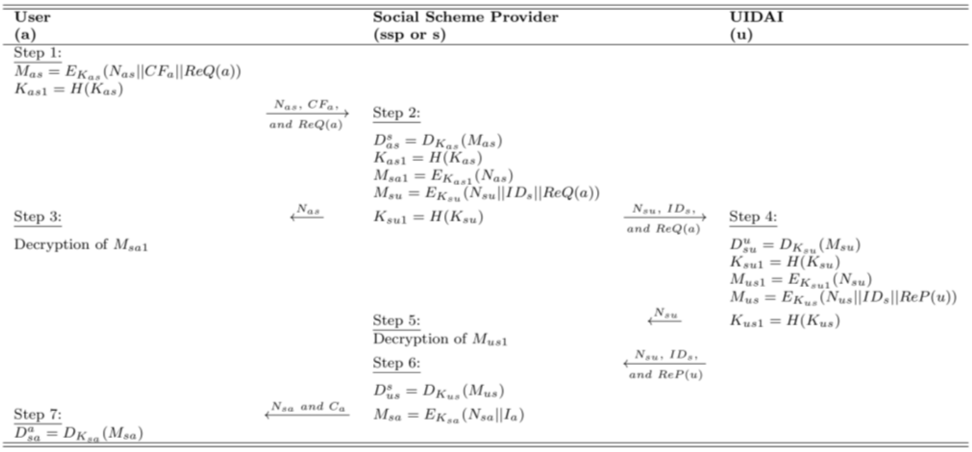
$$a_i^z = Info_i \cap (SS_b \cup SS_c) = \{info\ 1, info\ 2\} \quad (24)$$

Thus, only name and gender will be disclosed to new social scheme provider. Consider a user at a bank terminal and want to ac cess his bank account. The social scheme provider (ssp) at bank terminal requests UIDAI regarding the user information. Upon reception of user information, the UIDAI appropriately updates user authentication certicate. Table 3 shows the complete structure of au thentication for aadhaar user information. Some of the associated terms are described in Table 4.

Table 2: User information and their corresponding weights for a particular social scheme.

Field	User Information	Weight for bank scheme	Weight for SIM scheme	Weight for ration scheme
Field 3	Name (*info* 1)	0.32	0.09	0.15
Field 4	Gender (*info* 2)	0.06	0.04	0.05
Field 5	DOB (*info* 3)	0.09	0.16	0.19
Field 6	Address (*info* 4)	0.12	0.14	0.16
	Email (*info* 5)	0.05	0.18	0.07
	Mobile No. (*info* 6)	0.15	0.20	0.018
Field 7	Guardian Name (*info* 7)	0.073	0.05	0.04
	Guardian Aadhaar No. (*info* 8)	0.048	0.045	0.019
Field 8	Document based (*info* 9)	0.036	0.04	0.041
Field 9	Introducer's based (*info* 10)	0.031	0.035	0.032
	HOF based (*info* 11)	0.022	0.02	0.23

Table 3: Acquisition of aadhaar user information at bank terminal.



User **(a)**		**Social Scheme Provider** **(ssp or s)**		**UIDAI** **(u)**
Step 1: $M_{as} = E_{K_{as}}(N_{as}\|\|CF_a\|\|ReQ(a))$ $K_{as1} = H(K_{as})$				
	$\xrightarrow[and\ ReQ(a)]{N_{as},\ CF_a,}$	Step 2: $D_{as}^s = D_{K_{as}}(M_{as})$ $K_{as1} = H(K_{as})$ $M_{sa1} = E_{K_{as1}}(N_{as})$ $M_{su} = E_{K_{su}}(N_{su}\|\|ID_s\|\|ReQ(a))$ $K_{su1} = H(K_{su})$		
Step 3: Decryption of M_{sa1}	$\xleftarrow{N_{as}}$		$\xrightarrow[and\ ReQ(a)]{N_{su},\ ID_s,}$	Step 4: $D_{su}^u = D_{K_{su}}(M_{su})$ $K_{su1} = H(K_{su})$ $M_{us1} = E_{K_{su1}}(N_{su})$ $M_{us} = E_{K_{us}}(N_{us}\|\|ID_s\|\|ReP(u))$ $K_{us1} = H(K_{us})$
		Step 5: Decryption of M_{us1}	$\xleftarrow{N_{su}}$	
		Step 6: $D_{us}^s = D_{K_{us}}(M_{us})$ $M_{sa} = E_{K_{sa}}(N_{sa}\|\|I_a)$	$\xleftarrow[and\ ReP(u)]{N_{su},\ ID_s,}$	
Step 7: $D_{sa}^a = D_{K_{sa}}(M_{sa})$	$\xleftarrow{N_{sa}\ and\ C_a}$			

Table 4: Notations and their meaning used in authentication of aadhaar user information.

Notation	Meaning
a *or* A	User
ssp or s	Social Scheme Provider
u	UIDAI
E_{kas}	Encryption using key between a and s
N_{as}	Nonce for the message between a and s
K_{as}	Shared secret key between a and s
M_{as}	Encrypted message from a to s
$H(K_{as})$	Hashing of the shared secret key K_{as}
D_{as}^s	Decryption at s using secret key between a and s

4 Updation of the user authentication Certificate

Users often access different social schemes to get benefited from them. Hence, the authentication certificate of such users must be updated based on the schemes to which they are entitled to. Consider the banking services, where a user wants to access certain schemes. Thus, initial and updated authentication certificate of "*a*" is given as follows.

Initial authentication certificate of a $Initial\ authentication\ certificate(a)$

$= UN + Addr + TS + DOB + IA + FMD + SA + V + Atrr$

$= 15 + 25 + 4 + 2 + 5 + 20 + 25 + 4 + 15 = 115\ Bytes$ (25)

The Updated authentication certicate of a Updated authentication certificate (a)

$= UN + Addr + TS + DOB + IA + FMD + SA + V + Atrr$

$= 15 + 25 + 4 + 2 + 5 + 20 + 25 + 4 + 30$

$= 130\ Bytes$ *(26)*

5 Simulation Enivronment & Results

In this section, we first describe simulation environment along with results obtained in the case of the proposed scheme and the OTP scheme. We simulated the system on intel core2duo processor with 2.5 GHz speed and 2 GB RAM. We used J2EE, where 10K users and 10 group managers were considered. Even though we have used core2duo Pentium processor (slightly new processor in the market), we have restricted the number of processors that were used so as to create the effect of intel Pentium CPU that was used in the OTP [6] scheme. We have chosen the OTP scheme to contrast with our scheme because the OTP scheme is widely used for authentication of users. In authentication of users, features such as name, address, PAN card, etc., are important so as to securely acquire information of relevant users. We wanted to build a scheme in which a user won't have to explicitly provide credentials (as in contrast with the OTP scheme where the account information and password is explicitly required).

We have simulated the proposed scheme (on Java platform) and compared results with the OTP scheme. As be shown in Fig. 3, the graph is plotted as the average time taken for authentication against a set of users. It shows that as the number of users increases, the time taken for authentication also increases. The reason for such a characteristic is due to the fact that various users belonging to different groups are authenticated simultaneously through respective group managers. In the OTP scheme, groups of users do not exist and hence requires more time to authenticate users. This also can be cross-checked from the fact that for a small number of users, the time taken for authentication is somewhat same in the schemes. The result in Fig. 4 shows the average memory size against a set of users, and demonstrates that the memory size increases with the increase in the number of users. For the OTP scheme, since the OTP is of static in nature, the memory size of users remains same. On the other hand, various users at different social schemes exist in the proposed scheme. Thus, the memory size varies in accordance with the features and social schemes.

The Fig. 5 shows the average time taken for authentication against number of social schemes, and demon strates that as the number of social schemes increases, the time taken for authentication increases. This is due to the fact that the memory size varies with respect to features and social schemes. The memory size increases with the increase in intermediate users in the proposed scheme. But the memory size of user increases even more in the case of the OTP scheme. This is due to the number of parameters that are considered in the authentication process of the OTP scheme. The average memory size for users up to six social schemes is plotted in Fig. 6, and shows that the memory size varies from 150 Bytes to 210 Bytes while it is constant (256 Bytes) for the OTP scheme. The variation in the memory size for various social schemes increases because of the increase in number of users. Table 5 is a snapshot of the performance result of the authentication scheme. The response time of the system is very fast because the information needed to be hashed is very small.

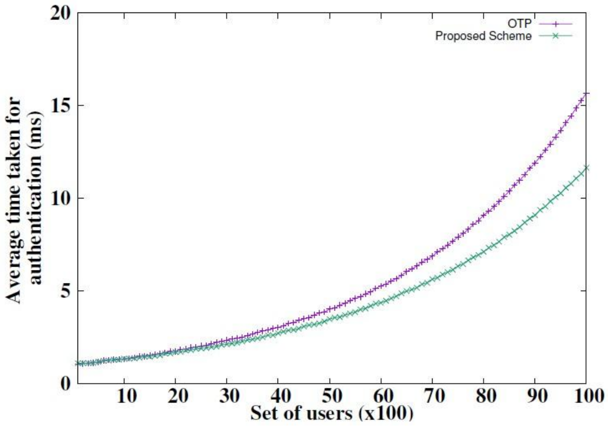


Figure 3: Average time taken for authentication vs set of users.

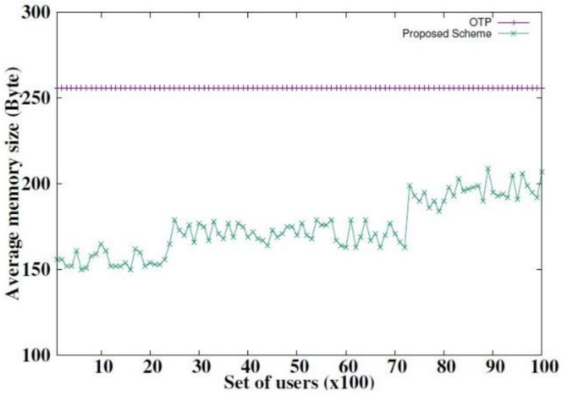


Figure 4: Average memory size vs Set of users.

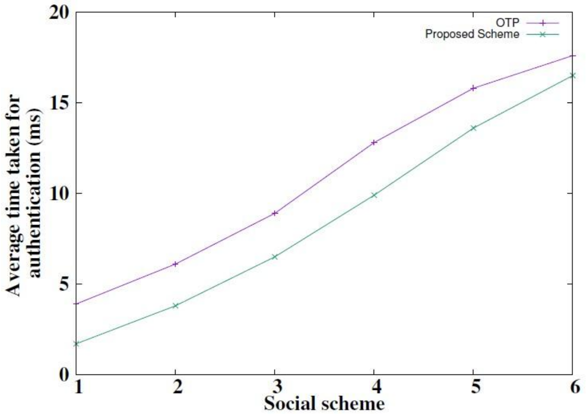


Figure 5: Average time taken for authentication vs number of social schemes.

In order to demonstrate the stability of the models, we use measures such as precision, recall, and *F*-measure. Precision, as described in equation (27), is the fraction of the retrieved user parameters that are relevant to provide authentication to users. On the other hand, recall is the fraction of the relevant user parameters that are retrieved as defined in equation 28. As depicted in equation 29, the combination of precision and recall is the F-measure which is the weighted harmonic mean of precision and recall. In the case of the OTP scheme, the parameters under consideration were time ($U_{OT\ P}$ and $S_{OT\ P}$), specific device, MAC address, and IMEI number. As be shown in Fig. 7, Fig. 8, and Fig. 9, precision, recall, and F-measure obtained via proposed scheme is better than the OTP scheme. In order to demonstrate the trade-off between precision and recall, the graph in Fig. 10 shows that decrease in precision increases recall for both the models. But the proposed scheme produced robust precision and recall values than the OTP scheme.

Table 5: Test number vs Response time.

Test Number	Response Time (ms) Using Proposed Scheme	Response Time (ms) Using OTP
1	0.0025	0.004
2	0.0028	0.005
3	0.0026	0.012
4	0.0023	0.003
5	0.0025	0.003

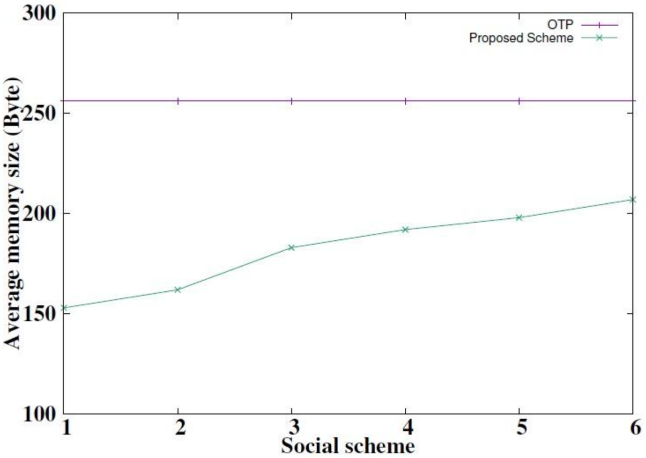


Figure 6: Average memory size vs Number of social schemes

$$Precision = \frac{|\{relevant\ parameters\} \cap \{retrieved\ parameters\}|}{|\{retrieved\ parameters\}|} \quad (27)$$

$$Recall = \frac{|\{relevant\ parameters\} \cap \{retrieved\ parameters\}|}{|\{relavant\ parameters\}|} \quad (28)$$

$$F - Measure = 2 \left\{\frac{Precision \times Recall}{Precision + Recall}\right\} \quad (29)$$

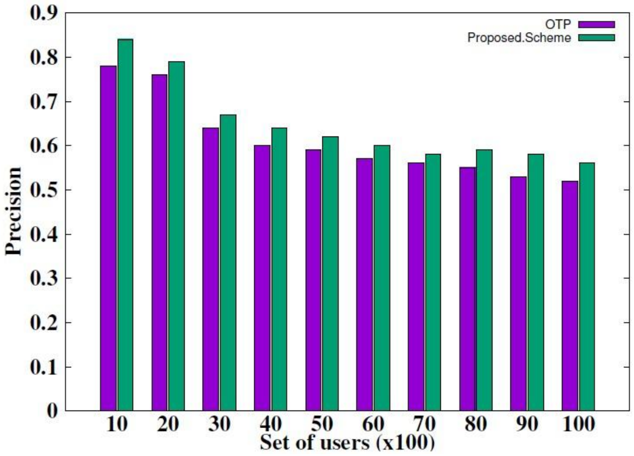


Figure 7: Precision vs Set of users.

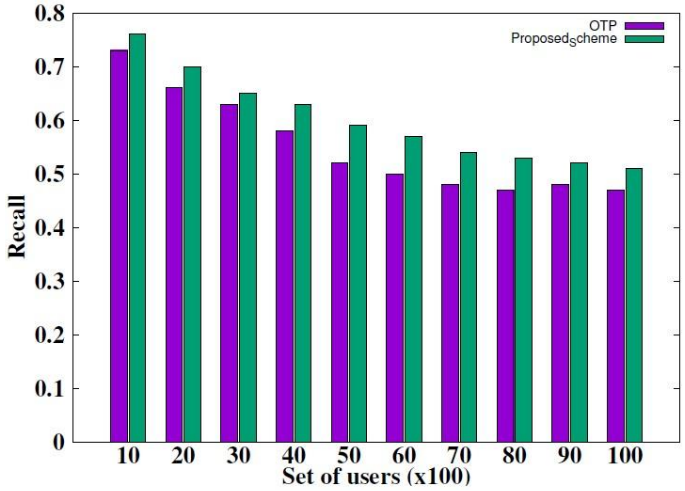


Figure 8: Recall vs Set of users.

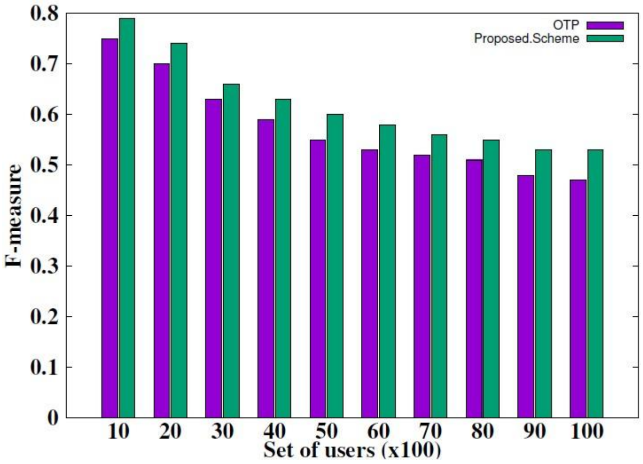


Fig. 9 : *F*-measure vs Set of users.

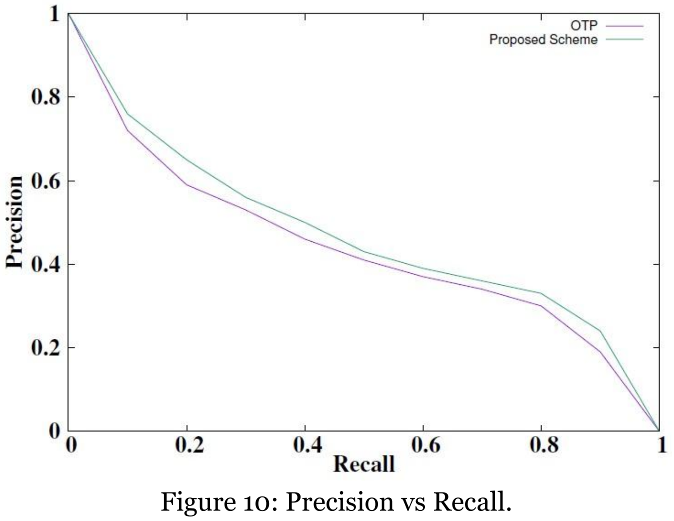


Figure 10: Precision vs Recall.

6. CONCLUSIONS

A method of designing authentication scheme for aadhaar user was developed in this paper. We considered the problem of appropriate disclosure of aadhaar user information to proper authorities by exploiting the parameters of users. The main theme of the paper was to address aadhaar user information disclosure which facilitated authorities to acquire sufficient information about users. Furthermore, instead of traditional approaches that utilised rule or tag-based method, the proposed system first classified users based on utilisation of a social scheme. Secondly, it utilised various parameters of users, and appropriate information was disclosed to authorities. At last, the designed scheme was simulated, where the acquisition of information of aadhaar users across various schemes were carried out. The graphs obtained through simulations were consistent with the the application and generalised formulation. We also compared the proposed model with the OTP scheme, and showed that our model performed better in terms of accurately providing aadhaar information of users.

REFRENCES

[1] Abhijit Banerjee, Esther Duflo, Clément Imbert, Santhosh Mathew, Rohini Pande, "E-governance, accountability, and leakage in public programs: Experimental evidence from a financial management reform in india," *London, Centre forEconomic Policy Research*, 2017.

[2] E. Bresson and J. Stern, "Efficient revocation in group signatures," *Public Key Cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001 Cheju Island, Korea, February 13–15, 2001 Proceedings*, pp. 190–206, 2001.

[3] A.D. Kent, L.M. Liebrock, and J.C. Neil, "Authentication graphs: Analyzing user behavior within an enterprise network," *Computers and Security*, vol. 48, pp. 150–166, 2015.

[4] L. Li, X. Zhao, and G. Xue, "An identity authenti- cation protocol in online social networks," *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 28–29, 2012.

[5] D.R.T. Manjul Mayank Pandey and D.A. Choubey, "Population dynamics in india," *Inter- national Journal of Scientific and Engineering Re- search*, vol. 6, pp. 2106–2133, 2015.

[6] X. Ren and X.-W. Wu, "A novel dynamic user au- thentication scheme," *2012 International Symposium on, Communication* & Infor*mation Technologies (ISCIT),* pp. 713–717, 2012.

[7] *Z. Yan, Y. Chen, and Y. Shen, "Percontrep: a practical reputation system for pervasive content ser- vices," The Journal of Supercomputing,* vol. 70, pp. 1051–1074, 2014.

[8] N. Lakshmi, *et.al.*, "CMOS Implementation of Multipath Fully Differential OTA with Dual Flipped Voltage Follower in 50 nm and 75 nm CMOS Technologies using Cadence Tool," *2024 IEEE* ICDCOT, 2024, pp. 1-8. https://doi.org/10.1109/ICDCOT61034.2024.10515482

[9] V.K. Suhasini, *et.al.*, "Detection of Skin Cancer using Artificial Intelligence & Machine Learning Concepts," *2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications* (ICCCMLA), Goa, India, 2022, pp. 343-347, https://doi.org/10.1109/ICCCMLA56841.2022.9989146

[10] Hayder M.A., *et.al.*, "An Innovative Artificial Intelligence Based Decision Making System for Public Health Crisis Virtual Reality Rehabilitation", *Scopus Indexed Journal of Machine and Computing*, vol. 5, no. 1, pp. 561-575, January 2025, https://doi.org/10.53759/7669/jmc202505044