IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 7, 2019, accepted January 19, 2019, date of publication January 31, 2019, date of current version February 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2896324

Automated User Authentication in Wireless Public Key Infrastructure for Mobile Devices Using Aadhar Card

KRISHNA PRAKASHA[1], BALACHANDRA MUNIYAL[1], AND VASUNDHARA ACHARYA[2]
[1]Department of Information & Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India
[2]Department of Computer Science & Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India

Corresponding author: Vasundhara Acharya (vasundhara.acharya@manipal.edu)

ABSTRACT Identification and authentication play a significant role in security controls. The manual process of user identification and authentication is time-consuming and tedious. The proposed research work aims to overcome this drawback and achieve user identification and authentication through an automated method using the Aadhar card. Aadhar project is developed by the Unique Identification Authority of India by merging biometrics and digitization. The details are stored in the form of a quick response code along with a 12-digit Aadhar card number. A model is built to capture the information from the Aadhar card. The mobile phones are used to obtain the data from the Aadhar card. The user validation is through two-step process using One Time Password and email address. The wireless public key infrastructure issues a digital certificate to the valid user. The proposed authentication and symmetric key exchange algorithm are formally verified and analyzed using automated validation of Internet security protocols and applications. The result of simulation proves that the proposed scheme is secure and safe. The experimental results show that time consumption for user authentication is acceptable. The acceptance of the proposed automated user identification and authentication model is authorized using a modified technology acceptance model. The result proves that there exists a strong relationship between the perceived usefulness of items and the Attribute Of Use (AOU). It also exhibits that the association between the AOU and user satisfaction is influential. The model demonstrates that the association between the Perceived Ease Of Use and attribute towards use is weak. The influence of exogenous variables over endogenous variables exhibits that the proposed model outperforms the traditional manual system and the target users are inclined towards it. The proposed model also finds its application in services which requires user authentication.

INDEX TERMS Aadhar card, authentication, security, TAM, WPKI.

I. INTRODUCTION

A mobile phone is considered one of the most innovative devices in modern times. The mobile applications stand in contrast to desktop applications. Apart from the usage of these applications for communication, they can also be used for User identification and authentication.

Entity authentication is used to prove the message source to the recipient. The entity (process, client or server) whose identity to be determined is called claimant, the other party trying to prove the status of the claimant is the verifier. User authentication is the fundamental building block and basis for most types of access control and user accountability. Internet Security Glossary (RFC 4949) defines the following two steps in authentication.

i. Identification step: Identifies the User.
ii. Verification step: It generates authentication information to bind the entity to the identifier.

User identification and authentication is essential because it enables organizations to keep their networks secure by permitting only authenticated Users (or processes) to access its protected resources. Once authenticated, a User or process is usually subjected to an authorization process as well, to determine whether the authenticated entity should be permitted to access a protected resource or system. A User could be authenticated but may fail to be given access to a resource if that User has no permission to access it. Authentication followed by authorization processes grants the access, or can

The associate editor coordinating the review of this manuscript and approving it for publication was Kaiping Xue.

even limit the level of access and action allowed for a particular entity. Authentication can be possible with a symmetric or asymmetric key in cryptographic systems. The commonly used authentication methods are listed below.

1) Kerberos: It is an open-source technique. It works based on the shared secret key system with a trusted third party.
2) Biometrics: It deals with body measurements and related calculations of an entity.
3) User name and Password: It uses preshared credentials.
4) Multifactor authentication: It makes use of two or more factors to authenticate. The example would be the system which requires both password and fingerprint to authenticate the User. Methods such as Challenge Handshake Authentication Protocol (CHAP) use combinations of User name and password to authenticate Users.
5) Single Sign-On (SSO): It authenticates a User once and authorizes multiple services.

The entities are to be verified to secure the resources from an unauthorized body using any available authentication method.

There are four general means of authenticating a User.

i. Something the individual knows: Ex: passwords, PIN and answers to prearranged questions.
ii. Something the individual possess: Ex: cryptographic keys, smart card and electronic key card.
iii. Something the individual is (static biometrics): Ex: fingerprint recognition, retina and face.
iv. Something the individual does (dynamic biometrics): Ex: voice recognition, handwriting etc.

In the proposed work, a smartphone is used to achieve the Aadhar card scanning. The User is identified and authenticated based on the Aadhar card credentials and issued a digital certificate. Aadhar project is developed by the (Unique Identification Authority of India) UIDAI by merging biometrics and digitization. It contains demographic details of a citizen such as name, sex, fingerprint, and iris [1]. The User details are stored in a smart card. These details are stored in the form of QR code along with a 12-digit Aadhar card number. Scanning of the QR code will retrieve and display all coded information. The unique smart card is issued to every citizen, and it can be used to avail different government services. Aadhar authentication provides digital online identity platform, and Aadhar number identified entity can be verified globally. The UIDAI delivers Aadhar based authentication service to the requesting entity before granting the service.

The proposed research work focuses on an automated User identification and authentication mechanism using Aadhar card in contrast to traditional manual User confrontation system adopted as shown in Figure 1. The time consumed in the manual confrontation of the User can be avoided using the proposed method. The safe transmission of user credentials to the certificate issuer is achieved using public key encryption. The two-way authentication using mobile phone and email is used to ensure the legitimacy of the certificate requester. The mobile devices are resource constrained,

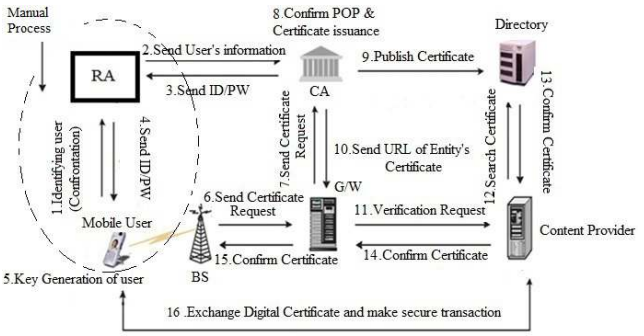

FIGURE 1. Wireless Public Key Infrastructure [2].

so traditional cryptographic algorithms or packages cannot be incorporated directly. The limitation of computational capability, the processing speed of the mobile or wireless devices are some of the boundaries if they act as a client in M-Commerce (Mobile Commerce) transactions. In asymmetric key cryptographic systems, digital certificates can be used for user authentication. Digital certificate verification by a resource-constrained device is also a challenge to be addressed in M-Commerce. The audit can be delegated to some trusted third party and result of certificate verification is used to establish the connection. The usage of efficient certificate verification mechanism plays the essential role if mobile devices are in the certificate verification process. Efficient Certificate Revocation List (ECRL) [3] is used for fast verification of digital certificates. The fundamental problem addressed in this research work is automated User identification and authentication using the Aadhar card. The outcome of the research work is automated User authentication and the issue of the digital certificate to the User that can be used in M-Commerce transactions.

A. LIMITATIONS OF MOBILE PHONE, WIRELESS NETWORKS AND REQUIREMENTS OF WIRELESS PUBLIC KEY INFRASTRUCTURE (WPKI)

Lee *et al.* [2] discussed the limitations of the wireless environment during the implementation of WPKI. The identified challenges were low bandwidth, high latency, non-secure connections and equipment limitations such as less storage, less powerful CPU, small battery life, tiny display and input devices. Due to these limitations, mobile devices are resource constrained and computationally inefficient compared to traditional high-performance computers and servers. The mobile phone lacks in computing capabilities of PKI (Public Key Infrastructure) operations such as key generation, encryption, and digital signature generation and verification involving complex mathematical operations. The CRL (Certificate Revocation List) verification and validation also demand high memory for storage. Because of these challenges, there exists a need for an efficient protocol to manage the certificate life cycle. The following requirements are identified to apply WPKI to the mobile phone through wireless internet.

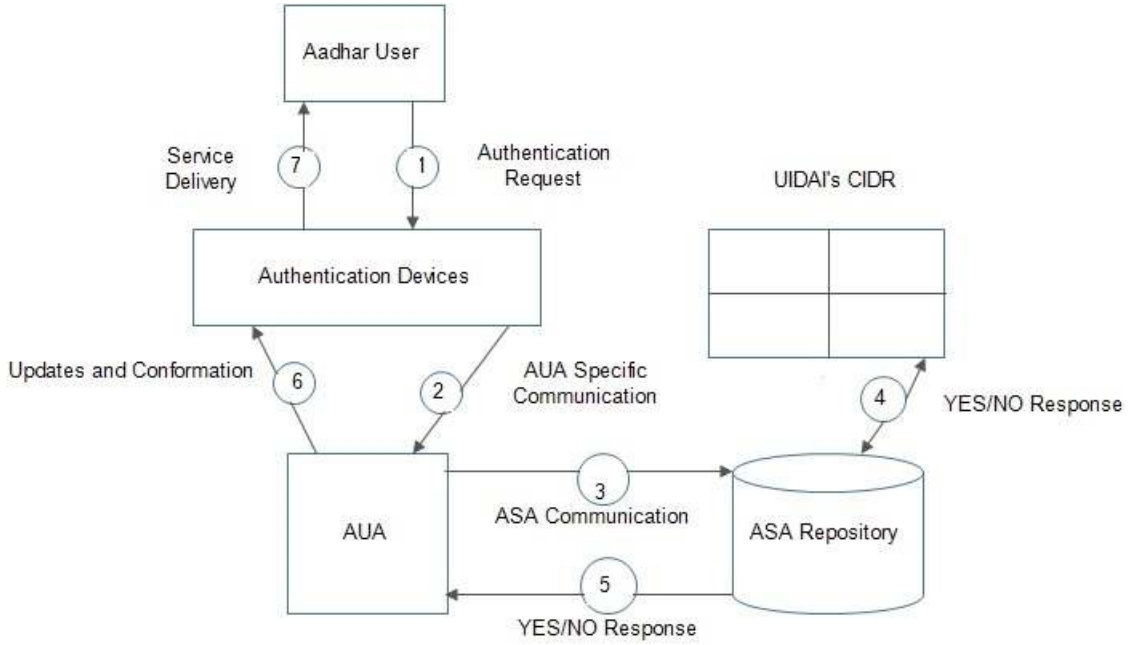

FIGURE 2. Aadhar system architecture.

1) Minimize the data size to be stored on the mobile phone and also for the transmission.
2) Optimize the certificate validation scheme.
3) Efficient Certificate Management Protocol through wireless bandwidth.

In [2], WPKI model used a manual procedure for User identification and authentication using confrontation. The confrontation may consume an indefinite amount of time due to external parameters and also depending on the number of people waiting for verification. The system depicted in [2] shows that mobile devices are responsible for key generation. The key production involves the complex mathematical operation, and it is a challenge for resource-constrained devices. In the proposed work, mobile devices are relieved from these complex mathematical operations to solve the above problems. In the proposed authentication and symmetric key exchange algorithm, the complex mathematical operations are delegated to resource abundant and computationally efficient devices. The safety and security of the proposed method are validated using formal verification technique. The simulation results demonstrate that the scheme is safe and secure. The proposed system involves automated user identification and authentication to issue digital certificates in contrast to manual confrontation. Digital certificate verification is a challenge for resource-constrained devices used in mobile commerce environment. It is handled by incorporating a fast certificate verification mechanism such as ECRL. The experimentation shows that time consumption for authentication is acceptable.

The following section briefly explains the Aadhar system model to issue Aadhar card in India.

B. AADHAR SYSTEM MODEL

The Aadhar system architecture has the following components as shown in Figure 2 [4].

1) UIDAI (Unique Identification Authority of India): It is responsible for maintaining User biometric information, credentials and to provide authentication and identification service to the requester. It uses Central Identities Data Repository (CIDR) to store the credentials.
2) The Authentication User Agency (AUA): AUA is meant for providing User services after successful User authentication with the help of CIDR. E.g., The banks or different state/central government agencies.
3) The Authentication Service Agency (ASA): ASA has a formal contract with the UIDAI and maintains a secure channel with the CIDR on behalf of the AUA for authentication request transmission.
4) The Users: People registered with the UIDAI and had an Aadhar number for unique identification.
5) Authentication device: It is termed as Point Of Sale (POS) device. The device captures biometric data from the Aadhar card holders and transmits data for authentication and receives authentication results.
6) Enrollment systems: They are distributed devices located at multiple sites, appointed by the UIDAI. These devices are meant for capturing the User demographic details.

Information and communication technology acceptance play a significant role in the study of information systems. The successful implementation of any information system is evaluated by a User acceptance [5]. The TAM (Technology Acceptance Model) is a model to access the User acceptance by the physiological interaction of a User with technology

and the mobile application. TAM is a method to model and test the User acceptance of the proposed new technology. The acceptance of the proposed system by the target Users is validated using a modified TAM with added parameters. The IT innovation in organizational contexts is better explained by TAM and also by Unified Theory of Acceptance and Use of Technology (UTAUT). Based on the Theory of Reasoned Action (TRA) the TAM is developed [6]. Based on the individual User′s general behavior the TRA is constructed. Various studies are performed for mobile learning acceptance [7]. TAM asserted that the actual use is related to individuals attitude towards using technology and it identified two prominent determinants of system usage namely the Perceived Usefulness (PUS) and the Perceived Ease Of Use (PEU) [8]. Technological perceptions of the User have a significant effect on mobile commerce [9]. It is also found that mobile commerce is significantly influenced by the success of Mobile payment (M-Payment) [10]. TAM finds User acceptance of a product, based on the actual usage of four internal variables. In the proposed work, a modified TAM is built to measure the adoption rate of the usage of mobile phones to achieve User identification and authentication.

II. RELATED WORK

A. LITERATURE REVIEW RELATED TO PUBLIC KEY INFRASTRUCTURE AND AUTHENTICATION

K.Prakasha et al., proposed a new method of developing CRL called ECRL for faster digital certificate verification in resource-constrained devices [3]. The approach was able to verify the digital certificates in the WPKI efficiently.

Zareen and Jabin [11] highlighted the importance of mobile devices to overcome the requirement of physical presence of a user at the time or in the place of authentication. The paper discussed an authentic mobile biometric signature verification and the importance of mobile devices for authentication. The research work also stressed the importance of the combination of mobile devices and biometric information in the possible application areas such as mobile commerce, military, banking transactions to prevent token theft, forgotten or misused passwords. The authors actively claimed that mobile with biometric authentication would be the technology for future.

Lee *et al.* [2], proposed WPKI technology that provided a similar security level as Wired PKI supporting the mobile phone. The User authentication for issuing digital certificate was done through confrontation, and it was found to be a significant drawback with indefinite time consumption.

Fongen [12] proposed a solution for the optimization of PKI by using temporary certificates, which did not need a revocation mechanism and the use of cached validation proofs to save protocol round trips. The scheme relieved a PKI from maintaining and distributing revocation lists, which left the system with smaller bandwidth and connectivity requirements. The distribution of revocation lists was replaced with temporary certificates, which were issued every few hours only to its owner/granted/authorized Users, excluding the unauthorized Users. But the arrangement is not compatible with COTS software products and leads to the requirement of customized clients.

Wang *et al.* [13] proposed a technique to prevent the probable damages done by breached Certificate Authorities (CA). A method to mitigate the issue of CA breaches by using multiple signatures in CAs was proposed. If 'n'is the number of signatures issued then, compromise of 'n-1' signatures would not break the PKI system. Even though the work was successful in reducing the CA breaches, the system introduces redundancy and not suggested for resource limited devices.

Sangram and Biswas proposed mobile home agent based registration authority and overcame the limitations of the mobile applications by proposing an ECC (Elliptic Curve Cryptography) based mobile PKI. The model was successful in resisting the different attacks. The study also compared the proposed PKI with the existing PKI [14].

Ma *et al.* [15] proposed four policies to enhance the privacy of the User's data in public key encryption with equality test (PKEET) scheme. The model was built to assist flexible authorization. The computational security of the model was proved using Diffie–Hellman assumption in the random oracle model.

Kim and Lee [16] proposed a scalable trust management system for the Internet of Things. The system was locally centralized and globally distributed. A network architecture termed as 'Auth' was deployed on edge devices. Authentication service was provided for locally registered entities. The trust relationship with others 'Auths' was maintained globally. The system was resilient to attacks due to the distributed trust.

Roy *et al.* [17] proposed an economical and secure User authentication scheme for mobile based services. The authentication was based on the cryptographic hash, bitwise XOR and fuzzy functions. The proposed model was robust to passive and active attacks. The absence of the registration center in the authentication procedure reduced the communication cost. The proposed scheme proved to be secure and economical when compared to the other existing models.

Park *et al.* [18] proposed an anonymous authentication scheme involving the sharing of keys between the home agent and foreign agent. Random oracle model was used to achieve the formal verification of the proposed model. It was robust to man in the middle attack and replay attack. The proposed method performed better than existing schemes in terms of security.

Tu and Lai [19] proposed a model to achieve authentication of legitimate Users using noisy channels. The message authentication was treated as a hypothesis testing problem. Authentication exponent and authenticated channel capacity of noise channel were explored. The study about the speed at which the successful attack could be driven to zero was conducted in authentication exponent. In the authenticated channel capacity a study about the most substantial data transmission rate for which the attacker's success rate could be

made small was conducted. The scheme was able to overcome the uncertainties in eavesdropper's channels.

Luo *et al.* [20] proposed a scheme to achieve authentication using the encrypted negative password. The initial plain password was hashed using the cryptographic hash function. The resultant was converted to a negative password. It was later encrypted using a symmetric key algorithm. The model was able to withstand the lookup table attack and dictionary attack.

Erdem and Sandıkkaya [21] proposed an architecture to establish a secure One Time Password (OTP) with two-factor authentication scheme. The second source of authentication was outsourced. The security and privacy factors are analyzed to verify the validity of the model.

Fan *et al.* [22] proposed a secure way of mobile payment using a Secure Mutual Authentication Protocol (SMAP) based on the Universal 2nd Factor (U2F) protocol. The mutual authentication was performed using an asymmetric cryptosystem. The protocol provided security for the individual's information and user's account information.

Madhusudhan *et al.* [23] proposed a dynamic authentication scheme using the smart card. The method was based on ECC. It made use of fewer hash functions that contributed to its light weightness. The formal verification using AVISPA ((Automated Validation of Internet Security Protocols and Applications) results show that the technique is safe and free from vulnerabilities.

Madhusudhan and Hegde [24] discussed a lightweight authentication scheme to address the vulnerabilities involved in WANG Ding *et al.* [25]. The proposed system has lesser hash functions and reduced complex modular mathematical operations. The security analysis of the proposed scheme was verified using the AVISPA tool and found to be safe.

Pippal *et al.* [26] discussed the vulnerability present in the RSA (Rivest-Shamir-Adleman) based smart card authentication scheme. They identified that the proposal failed to satisfy the user needs and was vulnerable to impersonation attack. A comparative analysis of existing schemes was also provided.

B. LITERATURE REVIEW RELATED TO ACCESS CONTROL

Kayes *et al.* [27] proposed a framework for the Context-Aware Access Control Application (CACC). A policy ontology was built to model the CACC policies. The policy enforcement architecture provided the support to access the resources according to the dynamically changing context information. The model and the framework was evaluated using the policies presented in the health care scenarios and case studies. The performance of the model was assessed using the response time.

Ruj *et al.* [28] proposed a decentralized access control scheme to authenticate the Users anonymously and to achieve secure storage of data on the cloud. In the proposed model Users had access control and allowed only valid Users to decrypt the data. The model was comparable to centralized schemes regarding overheads.

Kayes *et al.* [29] proposed a context-aware control access structure to access the data from multiple sources. It combined the benefits of the fog computing and the traditional context-sensitive access control mechanism. The unified set of access control mechanisms eliminated the processing overhead. The formal approach was realized using the unified data ontology. Case study and prototype were employed to test the applicability of the model.

Castiglione *et al.* [30] proposed two constructions for key assignment. The first construction was dependant upon the symmetric encryption and perfect secret sharing. The second one was established using public-key threshold broadcast encryption. The model was able to address the cases when special permissions were required.

Liu *et al.* [31] proposed a role-based access control model to achieve resource sharing. An optimal authorization route was used to identify the authorization state. Single-goal-role authorization routes and multi-goal-role authorization routes were evaluated using an algorithm termed as PGAO*. The model provided a secure way to access the resources in Manufacturing Internet of Things (MIoT).

C. LITERATURE REVIEW RELATED TO TECHNOLOGY ACCEPTANCE MODEL

Nikou and Economides [32], discussed the Mobile Based Assessment (MBA) for investigating the factors that influence behavioral intention to use. MBA is a novel method of assessment using Wireless technology and mobile devices. Various technical and social aspects were taken into consideration, and their impact on User acceptance was determined. The experiment was conducted on a population of size 145. The model was able to predict 47 percent of variations in the behavioral intentions of the User in using the MBA. Even though the model was able to predict the student's intention to use the MBA, more in-depth research was required to discuss the acceptance of mobile learning and acceptance.

Schierz *et al.* [5] discussed an empirical approach to determine the User acceptance for the mobile payment services. Eight hypotheses related to the technical aspect and one more hypothesis with social aspect was discussed. The experiment was conducted on a population from Germany. The measured items were formulated in the form of a seven-point scale. The latent variables were examined using a structural equations modeling and a maximum likelihood procedure. The examinations identified that the perceived compatibility and the individual′s mobility had an enormous impact on the User acceptance of the mobile payment services.

Ooi and Tan [33] proposed a TAM to determine Smart card credit card adoption. It consisted of Mobile Usefulness (MU) and Mobile Ease Of Use (MEU). Additional mobile constructs were added to reduce the complexity. The work was successful in developing the smart phone-based credit card system, but the demographic information included only the younger generation.

Chau and Hu [34] in their study performed a comparison between the three models namely: TAM, the Theory of

Planned Behaviour (TPB), and a decomposed TPB model. They found that TAM was better in performance than the other two.

Ervasti and Helaakoski [35] conducted a survey to study the mobile service development process and factors that influence the acceptance of mobile services in Finland. Through the study, the authors discovered the factors that affect consumers attitude towards mobile services. The study is found to be useful for mobile service providers to choose the right strategies.

Muller-Seitz *et al.* [36] studied the factors crucial for the successful introduction of new technology. The authors analyzed customer acceptance of Radio Frequency Identification (RFID) using the TAM model. The research work found that the attitude towards novel techniques has an impact on the PEU.

From the study of literature, it can be concluded that techniques incorporated in existing PKIs have some limitations. There exists a need for design and implementation of an efficient WPKI architecture with fast certificate verification capability to mitigate the human intervention.

D. RESEARCH CONTRIBUTIONS

The Contributions in the paper are listed below.

1) In the proposed research work, Aadhar card based automated user identification and authentication system is developed to issue digital certificates in a WPKI.
2) Delegation of complex mathematical operations and key generation from resource constrained mobile devices to resource intensive servers and a method for safe key transfer to the mobile devices is proposed and validated.
3) No trusted third party like registration authority is involved in the User authentication process to reduce communication time, cost and also minimizes the number of entities contributing to optimized WPKI.
4) Security validation of the proposed authentication and symmetric key exchange mechanism using AVISPA formal verification mechanism.
5) Computation of time delay for the User authentication process to test the acceptability of the proposed system.
6) Development of extended TAM to evaluate the User acceptance of the proposed system using IBM SPSS and Smart PLS.

E. PAPER ORGANIZATION

The remainder of the paper is organized as follows. Section III describes the methodology adopted for automated User identification and authentication. Section IV explains development of WPKI. Section V presents the adopted research method and its design. Section VI describes the formal verification of the proposed algorithm using AVISPA. Section VII gives the details of the test environment and time delay for user authentication. Section VIII gives the data analysis. Section IX provides the inferences.Lesson Learnt is included in Section X and Section XI gives conclusion and future scope.

III. METHODOLOGY

In this section, an automated approach to achieve the User identification and authentication is discussed. Figure 3 depicts the proposed model. The National Identity Number (NIN) of the User is used for identification by using the Aadhar card. QR code scanning of the card is done using the zxing Scanner and encoded user details are sent to the server by public key encryption [37]. A verification email is sent to the User on the email address provided during registration. To the registered mobile number an OTP is sent. The system has a two step authentication mechanism. After the authentication process, the valid User is issued a digital certificate by a CA in WPKI. The WPKI model is explained in the further section.

A. MODELLING OF WPKI COMPONENTS

WPKI based authentication system and associated services play an important role in diversified applications. Modeling of the WPKI and its components helps to remove ambiguity and allows better readability. The WPKI model to manage certificate life cycle is shown in Figure 4. The digital certificate issued to the User is stored in the repository for future use. The published CRL contains a list of revoked certificates which are not in use, and it is useful for certificate verification.

There are mainly two types of modeling techniques:

1) State-based: It is described using 'Z' specification. It models 'backend' operations by capturing the state of the PKI components in the authentication process and the relation between them.
2) Event-based: It is represented in the Algebra of Hoare's Communicating Sequential Process (CSP). It is used to model 'front end' interactions and behavior [38].

In a PKI, the digital certificates are issued by the authorized CA, and it binds the User with the associated public key. The private key of the corresponding User is used for the generation of the digital signature. The CA at the first level is called a root CA, and the certificate for it is generated by itself. The process is called self certification. Each CA is authorized to certify its next subordinate levels. The architecture is called a hierarchical PKI, and it is used in the proposed research work. The public and private key pair for the User can be generated by two approaches. They are:

1) Generation of the key pair by the trusted CA and transmit private key of the User securely.
2) The client generates a key pair and sends a copy of a public key to the CA for certification by ensuring Proof of Possession (POP) of the corresponding private key.

The first approach is incorporated in the proposed research work, and it is discussed in the subsequent sections.

B. FORMAL SPECIFICATION OF WPKI COMPONENTS

The following section describes the method of modeling various elements of a WPKI namely, CAs, digital certificate, a Clients (Users) and Authentication Server for understanding the system and its components. The abstraction of the CA,

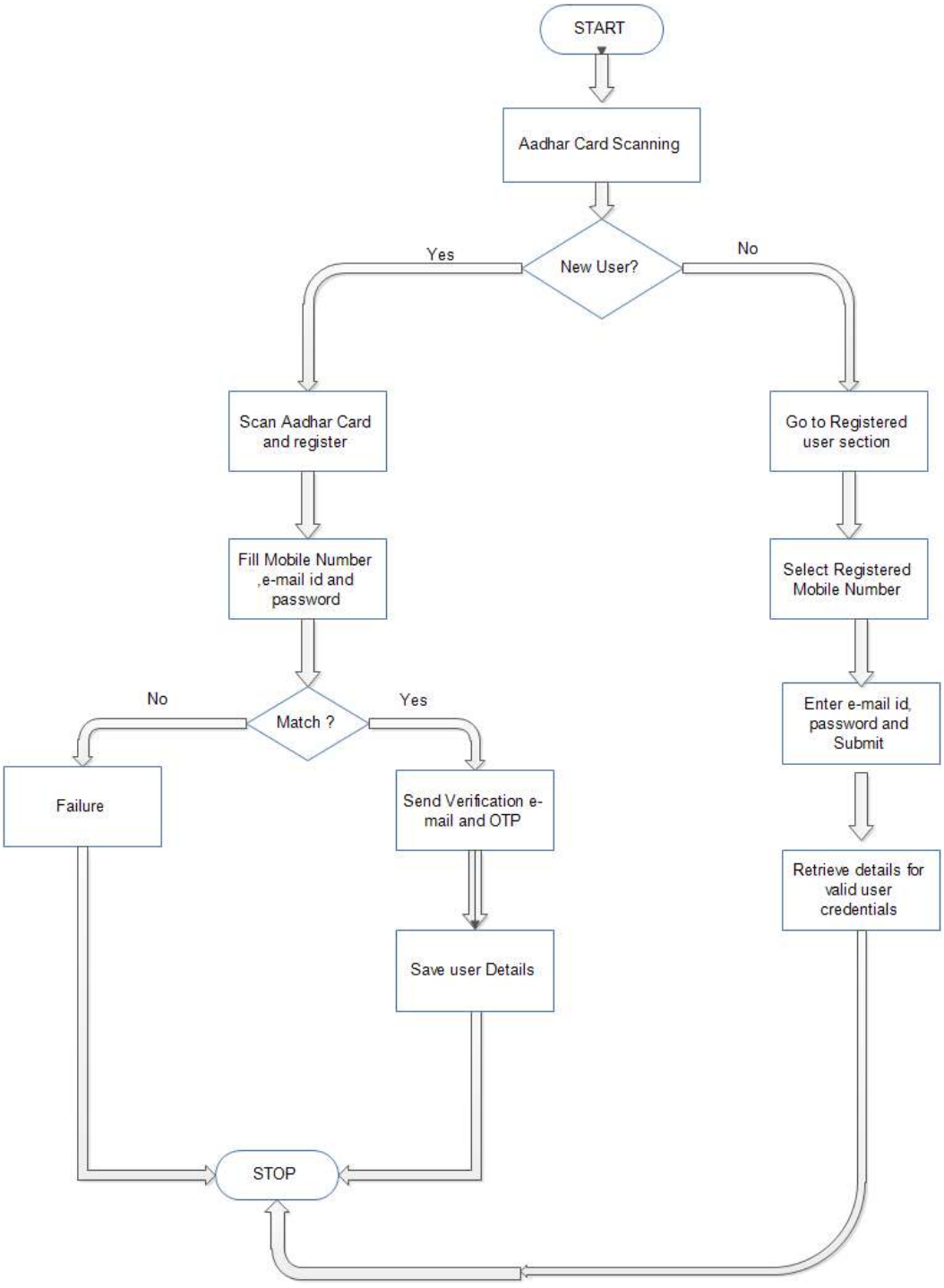

FIGURE 3. User identification and authentication using Aadhar card.

digital certificate, Clients, and Servers are formulated using a state-based model. The state-based model represents the schema, and it explains the various components implemented in the proposed WPKI using OpenSSL and test environment as listed in Table 10 and Table 11 under the Linux environment. The following types are used to represent the model [39].

1) Key: It represents the asymmetric key pairs. A validPKIKeyPair is a relationship that binds a public key to its corresponding private key. It is used to ensure that the key generated for the User is valid.
2) Data: It represents the plain text and the ciphertext data.
3) WPKISerialNb: It represents the serial number of every digital certificate.

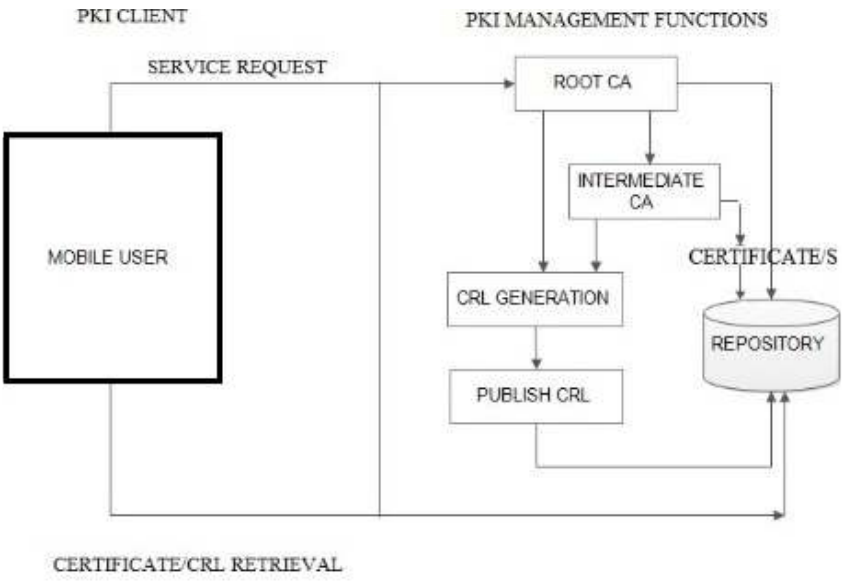

FIGURE 4. WPKI model for digital certificate life cycle management.

4) WPKICipherAlgoName: It represents the cryptographic algorithms used.
5) WPKICertAuthorityName: It represents the names of the CA.
6) Date: It represents the validity dates for which the certificate is useful.

A CA generates a digital certificate and signs it by using a private key. It also maintains a CRL containing revoked certificates. It is made public to verify clients and servers. The WPKI CA can be represented as follows:

$$
\begin{array}{|l}
\textit{PublicCAInfo} \\
\hline
\textit{name} : \textit{WPKICertAuthorityName} \\
\textit{publicKey} : \textit{Key} \\
\textit{ca\_revocationList}\ \mathbb{P}\ \textit{SerialNb} \\
\textit{ca\_SupportedCrypto}\ \mathbb{P} \\
\textit{WPKICipherAlgName} \\
\hline
\end{array}
$$

Here, 'name' is the name of the CA with a unique 'public key' having a set of revocated certificates maintained in 'ca_revocationList.' 'ca_SupportedCrypto' represents the list of the supported cryptographic algorithms for signature generation and verification.

A generic representation of a cryptographic algorithm to achieve a digital signature or encryption (for authentication or confidentiality) is as shown below:

The CA also maintains few secret information, which can only be known to the CA management. The secret information includes the private key corresponding to the public key of the CA and a list of issued certificates. It can be captured by defining a 'secretKey' and 'issued,' where 'issued' is a function that relates a serial number to a digital certificate as shown below.

$$
\begin{array}{|l}
= [\textit{WPKICipherAlgName}, \textit{Data}, \textit{Key}]] = \\
\textit{validPKIKeyPair} : \textit{Key} \leftrightarrow \textit{Key} \\
\textit{pkiAlgoName} : \textit{WPKICipherAlgName} \\
m : \textit{Data} \\
pk, sk : \textit{Key} \\
\hline
(pk)\textit{validPKIKeyPair}(sk) \Leftrightarrow \\
[\,[\,\textit{pkiAlgoName}\,]\,]\,pk \\
([\,[\,\textit{pkiAlgoName}\,]\,]\,skm) = m \wedge \\
[\,[\,\textit{pkiAlgoName}\,]\,]\,sk \\
([\,[\,\textit{pkiAlgoName}\,]\,]\,pkm) = m \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\textit{PrivateCAInfo} \\
\hline
\textit{PublicCAInfo} \\
\textit{issued} : \textit{SerialNb} \rightarrow \textit{Certificate} \\
\textit{secretKey} : \textit{Key} \\
\hline
\end{array}
$$

The conjunction of private and public CA information models the CA. It is shown as follows:

$$\text{WPKICertAuthority} \mathrel{\widehat{=}} \text{PublicCAInfo} \wedge \text{PrivateCAInfo}$$

The digital certificate issue by a CA contains the following components:

1) issuer: It is the name of the CA that issued the User certificate;
2) serial: It is the serial number of the certificate;
3) subject: It is the name associated with the public key of the certificate (User);
4) public key: It is the public key of the User;
5) validity: It is the validity date of the certificate;
6) WPKIAlgoName: It is the name of the public key algorithm to be used with the public key; and
7) caSignatureAlgo: It is used by the CA to generate a digital signature on the certificate.

The WPKICertificateData is represented as below:

WPKICertificateData

$issuer : WPKICertAuthorityName$
$serial : SerialNb$
$subject : Subject$
$publicKey : Key$
$validity : Date \times Date$
$pkiAlgoName : WPKICipherAlgName$
$caSignatureAlgoName :$
$WPKICipherAlgName$

The data type WPKI certificate is represented as follows:

WPKICertificate

$WPKICertificateData$
$WPKIcaSignature : Data$

The 'Public_UserDetails' possesses the information needed for the authentication. It is comprised of a digital certificate issued by CA and a list of cryptographic algorithms supported for key generation and encryption. The User data known publicly is represented below:

Public_UserDetails

$cert : WPKICertificate$
$UserSupportedCrypto : \mathbb{P}$
$WPKICipherAlgName$

$cert.caSignatureAlgoName \in$
$UserSupportedCryptoAlgo$
$cert.pkiAlgoName \in$
$UserSupportedCryptoAlgo$

In an open system environment, the server administrator authenticates the Users by validating their digital certificates and verifying that the corresponding private key exist along with the User.

WPKIAuthenticationServer

$registered\_Users : \mathbb{P}\, Subject$
$trustedCA : \mathbb{P}\, WPKICertAuthorityName$
$key\_association : Subject \nrightarrow Key$
$caKey : CertAuthorityName \nrightarrow Key$
$revoked : \mathbb{P}\, SerialNb$
$today : DateserverSupportedCrypto :$
$\mathbb{P}\, WPKICipherAlgName$

$domkey\_association =$
$registered\_Users \lhd trustedCA$
$\subseteq domcaKey$

CertValidaionOK and VerificationOk are used to validate and verify the issued digital certificates. The result of validation and verification will result in either authentication success or authentication failure status of the digital certificates as shown in schemas Success and Failure.

CertValidationOk

$\Xi AuthenticationServercert? :$
$CertificatecertData :$
$Certificate \nrightarrow Data$

$cert?.issuer \in trustedCA \land cert?.serial$
$\notin revoked \land$
$today \text{validDate} cert?.validity \land [\,[$
$cert?.caSignatureAlgoName\,]\,]$
$(caKeycert?.issuer)cert?.caSignature =$
$certData(cert?)$

VerificationOk

$\Xi AuthenticationServer$
$cert? : Certificate$
$nonce? : Data$
$signed\_nonce? : Data$

$cert?.subject \in$
$registered\_Users \land [\,[\,cert?.pkiAlgoName\,]\,]$
$cert?.publicKeysigned\_nonce? = nonce?$

Success

$resp! : Report$

$resp! = Auth\_Success$

Failure

$resp! : Report$

$resp! = Auth\_Failure$

IV. DEVELOPMENT OF A WIRELESS PUBLIC KEY INFRASTRUCTURE

The Components of WPKI are constructed as discussed in the formal modeling by using the OpenSSL package. Figure 5 demonstrates a hierarchical PKI with 'CITY' as root CA, 'UDP,' and 'MPL' as subordinate CAs in level 1 and 'MNG' as level 2 subordinate CA used for the proposed system. The Algorithm 1 discusses the automated User identification and authentication process and issuance of digital certificate and key transfer after successful authentication. The Algorithm 2 and Algorithm 3 explain the fast certificate verification in the developed WPKI using ECRL [3].

A. PROCEDURE: AUTHENTICATION AND SYMMETRIC KEY EXCHANGE BETWEEN THE USER AND THE CA

The pseudo-code to achieve authentication and symmetric key exchange is given in Algorithm 1 and the notations used in the algorithm are listed in Table 1.

PREMISE: User knows the Public key, 'k_{PU}' of the Authentication Server (AS). User and CA share a Symmetric Key with the help of AS and Token Grant Server (TGS).

GOAL: User and CA achieve mutual entity authentication and agree on a shared secret key. The CA also issues digital certificate to the User and securely transmits digital signature generation key.

Algorithm 1 Authentication and Symmetric Key Exchange

procedure Authentication AND KEY EXCHANGE
  User⇒AS: $E_{Asym}[k_{PU}$,'{NIN || ID_{TGS}||MAC|| TS || Nonce}']
  AS:
  if (Verification(NIN)==TRUE) **then**
    Retrieve NIN_Mobile#, NIN_E-Mail
    if (NIN_E-Mail == FALSE) **then**
      NIN_E-Mail ⇐ Input(E-mail)
    end if
    NIN_Mobile# ⇐ Generate_OTP()
    if Input(Hashvalue)== HASH(OTP, MAC) **then**
      Verification Success
    else
      Verification Failure
    end if
  end if
  if (User_Authentication == TRUE) **then**
    TGS ⇐ User details + $K_{U,TGS}$
    $Ticket_{TGS}$ =$E_{sym}[k_{(AS,TGS)}$, '{$k_{(U,TGS)}$ || NIN || MAC || ID_{TGS} || ID_{AS} ||TS || TGS details}']
    User ⇐ ($Ticket_{TGS}$)
    User ⇐ $E_{sym}[k_{(MAC+OTP)}$,'{$k_{(U,TGS)}$ || TS}']
  else Failure_Message
  end if
  Client _Validator= $E_{sym}[k_{(U,TGS)}$, '{NIN || MAC || ID_{AS} || TS}']
  User ⇒ TGS: ID_{CA} || $Ticket_{TGS}$ || Client_Validator
  TGS:
  if (Client _Validator == TRUE) **then**
    User ⇐ ($Ticket_{CA}$)
    User ⇐ $E_{sym}[k_{(U,TGS)}$,'{$k_{(U,CA)}$ || Nonce}']
  else Failure_Message
  end if
  $Ticket_{CA}$ =$E_{sym}[k_{(TGS,CA)}$, '{$k_{(U,CA)}$ || NIN || MAC || ID_{AS} || ID_{TGS} || TS || CA details}']
  Client_Validator= $E_{sym}[k_{(U,CA)}$, '{ NIN || MAC || ID_{AS} || ID_{TGS} || TS}']
  User⇒ CA: $Ticket_{CA}$ || Client_Validator
  CA:
  if (Client _Verification == SUCCESS) **then**
    Diffie_Hellman(Global_Public_Elements, $K_{U,CA}$)
    Generate(K_{Sym})
    Share(K_{Sym})
  else Failure_Message
  end if
  User ⇒ CA: $Ticket_{CA}$ || Request(Key,Certificate || Request(OTP) || E(k_{Sym},['{NIN || MAC || Nonce}']
  X ⇐ $E_{sym}[k_{Sym}$'{*PRIVATEKEY*}']
  CA ⇒ User: $E_{sym}[k_{(MAC+OTP)}$, '{X}']
end procedure

The User generates an encrypted message, which is comprised of a NIN or Aadhar card number, ID_{TGS}, a Timestamp and MAC address using 'k_{PU},' as the encryption key and sends it to the AS.

Figure 6 depicts the components involved in the constructed WPKI. One of the identified challenges in the proposed work is fast certificate verification. ECRL is built to speed up the certificate validation. The Algorithm 2 and Algorithm 3 explains the ECRL construction process. The proposed system is built with three layers of safety. Three entities involved are AS, TGS, and a CA. The AS identifies and authenticates the User based on NIN and Aadhar card credentials. The User credentials are validated against the stored entries in Aadhar repository. The AS performs two-step verification of the User with the help of registered email address, and the mobile phone number supplied during the Aadhar card registration carried out by government agencies. After successful User identification and authentication,

Algorithm 2 Revoked Certificate Serial Numbers for ECRL Generation

```
1: procedure Identify REVOKED certificates
2: Initialization: Let 'p' be a WPKI and 'q' be number of CAs in 'p' and 'R' be revoked certificate.
3:     for each 'q' in 'p' do
4:         fp1 ← Pointer to CertificateRevocationList
5:         fp2 ← Pointer to Certificate_Serial_NumberFile
6:         c ← fgetc(fp1)
7:         while c≠EOF do
8:             if c = 'R' then
9:                 read SerialNo
10:                write SerialNo in Certificate_Serial_NumberFile
11:            end if
12:            c ← fgetc(fp1)
13:        end while
14:    end for
15: end procedure
```

Algorithm 3 Construction of ECRL for Fast Certificate Verification

```
1: procedure insertSerial
2:     initialize a input[] char array to 0
3:     while fp1≠null do
4:         f ← 0
5:         fp1 ← file pointer of Certificate_Serial_NumberFile
6:         c ← fgetc(fp1)
7:         while c≠newline do
8:             input[f] ← c
9:             f ← f + 1
10:            c ← fgetc(fp1)
11:        end while
12:        dec ← hextodec(input))
13:        root ← avl.insert(root,dec)
14:    end while
15:    end while
16: end procedure
```

the User is issued with a ticket to consult the TGS. The AS also supplies a symmetric key, '$k_{U,TGS}$' to the User for secure communication with TGS by encrypting it with the key derived from user credentials (MAC address of the device and OTP). Same key '$k_{U,TGS}$' is also kept as the part of the ticket by encrypting it with '$k_{AS,TGS}$.' Since AS and TGS trust each other and share a symmetric key '$k_{AS,TGS}$,' when the User produces the ticket issued by AS to TGS containing symmetric key '$k_{U,TGS}$' issued by AS, the TGS trusts the User. The user also produces Client Validator to prove himself the possession of key '$k_{U,TGS}$' by encrypting its credentials and sending to TGS. The TGS can verify the genuine User by matching these credentials encrypted by shared key '$k_{U,TGS}$.' After successful verification of the User with the User's credentials and ticket issued by the AS, the TGS generates a symmetric key and issues a ticket to consult CA. The usage of symmetric key and ticket is similar to above description in the context of CA and User. The symmetric key encryption is used for fast computation by considering the limitation of the mobile device. With the issued ticket, the User contacts CA for a digital certificate. After User verification, on behalf of the User, the trusted CA generates public and private key pairs. The digital certificate request issued by User is verified, and the certificate is issued for a subject public key. The private key of the User is sent to the User by encrypting it with symmetric which is already shared between CA and the User.

B. EFFICIENT CERTIFICATE REVOCATION LIST (ECRL) FOR FAST VERIFICATION OF DIGITAL CERTIFICATES

With the help of the hosted CA and OpenSSL, a hierarchical WPKI is created. Each CA is loaded with a valid private and public key pair. A CRL file is generated from the set of revoked certificates. After extracting the serial number of the revoked certificates, an ECRL is built, where every node has the serial number of a revoked certificate. The incorporation of ECRL for fast verification of digital certificates improved the performance of the system.

TABLE 1. Notations used in the authentication and key exchange algorithm.

Symbol	Description
U	User.
MAC	MAC Address.
OTP	One Time Password.
TS	Time Stamp.
AS	Authentication Server.
TGS	Token Grant Server.
CA	Certificate Authority.
ID_X	ID of entity X.
V	Validity of the message.
$k_{(AS,TGS)}$	Shared symmetric key between AS and and TGS.
$k_{(U,TGS)}$	Shared symmetric key between User and and TGS.
$k_{(U,CA)}$	Shared symmetric key between User and and CA.
$k_{(TGS,CA)}$	Shared symmetric key between TGS and and CA.
k_{PU}	Asymmetric Key used in public key encryption.
$E_X[\ k_Y,'\{Z\}']$	Using the encryption method 'E_X' and the key 'k_Y', the String 'Z' is encrypted.
Client_Validator	Attested token possessed by the User to prove identity.
HASH	Hash Function.
E_{sym}	Symmetric Encryption.
E_{Asym}	Asymmetric Encryption.
NIN	National Identity Number.
NIN _X	X is linked with NIN.
$Ticket_X$	Ticket issued to the User to contact the entity 'X.'

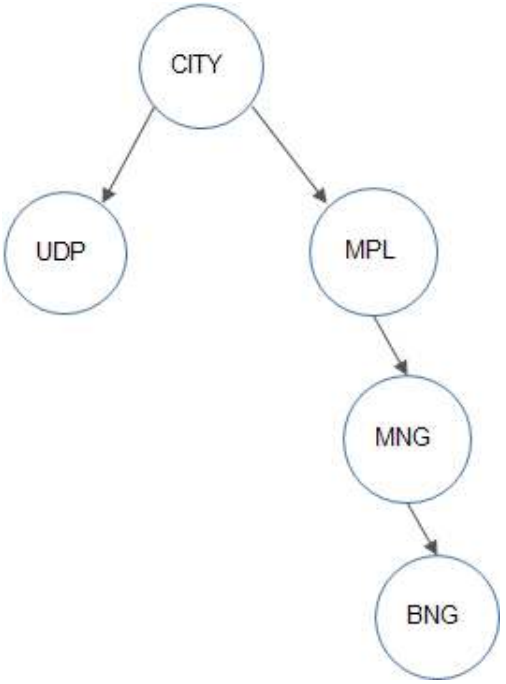

FIGURE 5. Hierarchical certificate authorities used for proposed research work.

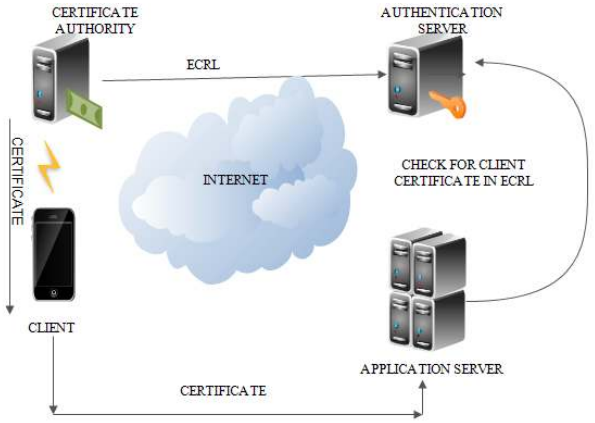

FIGURE 6. WPKI with integrated ECRL.

C. TAM FOR USER ACCEPTANCE OF THE PROPOSED METHOD OF USER IDENTIFICATION AND AUTHENTICATION BY USING A MOBILE APPLICATION

The TAM is extended to get a better understanding of the user behavior on a proposed automated system [40]. The following internal variables were included in the proposed work by extending TAM [41] as shown in Figure 7.

i. PUS: PUS is defined as the degree to which a User trusts using a particular system improves the job performance. The parameters measured are listed in Table 2.
ii. PEU: PEU is the measure of easiness that is felt while using the product. It is the degree to which User trusts that using the mobile application will improve the performance. Table 3 lists the parameters used for the study.
iii. User Satisfaction (US): US is a measure of usage of the new system by fulfilling the User requirements. The US is a result of a clear understanding of the developed system. It is also a measure of performance of the system to see if it meets or exceeds perceived expected outcomes. It is personal assessment parameter and directly related to the User expectations. Table 4 lists the parameters used for the study.

TABLE 2. Perceived usefulness items.

Construct	Operational Definition	Measured Item
PUS	PUS is a feeling that smart phone Users hold while using the developed technology with a new product	PUS1: Usage of mobile application for automated User identification enables the User to accomplish task quickly and efficiently. PUS2: Usage of Mobile application for automated User identification saves a lot of time energy and improves job performance. PUS3: The usage of proposed system improves productivity. PUS4: The usage of proposed system would enhance the effectiveness of the job and make things easier.

TABLE 3. Perceived ease of use.

Construct	Operational Definition	Measured Item
PEU	PEU measures level of easiness experienced by the User while using the application	PEU1: Learning to operate the Mobile application system is easy for the User PEU2: It is found easy to make the system do what the User want to do by the mobile application without much assistance PEU3: The interaction with the proposed system is flexible, clear and understood PEU4: Overall system performance is good and found easy to use

TABLE 4. User satisfaction.

Construct	Operational Definition	Measured Item
US	US measures the level fulfilling User requirements through system performance.	US1: The system works the way the User want it to work US2: The mobile application is pleasant to use and wonderful US3: Using the system gives satisfaction by meeting requirement US4: System usage gives confidence and it is a good alternative for traditional system

TABLE 5. Attitude towards use.

Construct	Operational Definition	Measured Item
ATU	Positive Attitude towards the use of the system is influenced by the satisfaction obtained after the usage of the proposed system.	ATU1: Usage of mobile applications save time ATU2: Usage of mobile applications is secure ATU3: Usage of mobile applications will consume less man power and saves money ATU4: System is useful and User friendly

iv. Attitude Towards Use (ATU): ATU is an individual positive or negative feeling, while doing some task using the target system. Table 5 lists parameters used for the study.

v. Attribute Of Usability (AOU): The AOU helps to get feedback on the working and non-working components of the system. It provides a broader understanding of what Users are doing and how they interact with the system by using a mobile application. Table 6 lists the parameters used for the study.

D. RESEARCH OBJECTIVE IN THE PROPOSED TAM MODEL TO VALIDATE THE USER ACCEPTANCE OF THE DEVELOPED SYSTEM

The User acceptance of the proposed User Identification and Authentication model is validated using modified TAM model. Figure 7 shows the proposed TAM model to validate the developed model. The sub objective is to study to what extent the exogenous variables (PSA, PEU, PUS, US, and ATU) influences and affects the endogenous variable AOU in the automated User

TABLE 6. Attribute of usability.

Construct	Operational Definition	Measured Item
AOU	The AOU helps to get feedback about the system after rigorous usage	AOU1: Interacting with the new application is easy AOU2: The purpose can be served easily AOU3: Functionalities are well integrated and self-understood AOU4: Overall System is useful and meets requirement

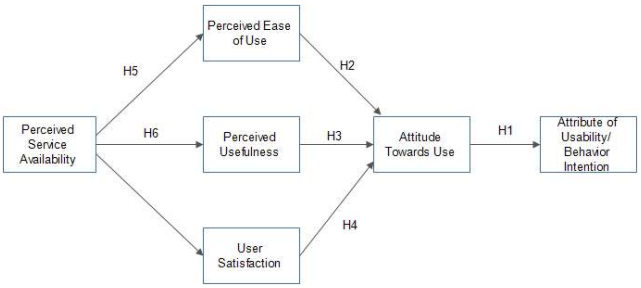

FIGURE 7. Proposed extended Technology Acceptance Model for User Acceptance Test.

identification and authentication process using the mobile application.

E. SUB RESEARCH QUESTIONS

- H1: There is a significant influence of the ATU over the AOU of the proposed TAM Model.
- H2: The association between the PEU and the ATU of the proposed TAM Model is considerable.
- H3: The relationship between the US and the ATU of the proposed TAM Model is significant.
- H4: The linkage between the PUS and the ATU of the proposed TAM Model is influencing.
- H5: There is a positive relationship between the PSA and the PEU of the proposed TAM Model.
- H6: The association between the PSA and the US of the proposed TAM Model is considerable.
- H7: There is a positive relationship between the PSA and the PUS of the proposed TAM Model.

V. RESEARCH METHOD AND DESIGN

The framed hypotheses are tested using the developed research model shown in Figure 8. The measurement of the AOU is done using a linear regression. Regression is a type of supervised learning problem in which the response is continuous [42]. Linear regression is one such machine learning model that can be applied for regression problems. In applied machine learning, algorithms are adapted from many different domains such as statistics and used according to the needs and requirements. However, linear regression was initially developed for use in the field of statistics. It has since then undergone an expansion in its application and is now widely used as a machine learning model for understanding the relationship between input and output numerical variables [43]. It is mostly used to predict a continuous response rather than a categorical one. The model is built using the Artificial Neural Network (ANN). They are formed by the simple clustering of the artificial neurons. It contains three layers namely input, hidden and output. The input layer receives the input, the output layer sends the information to the outside world, and the hidden layers produce an output using the activation function [44]. The research work is aimed at examining the effect of extended TAM on the usage of the mobile application for User identification and authentication process. A self-assesable questionnaire is prepared and responses are received from the potential target Users. For the proposed research using mobile phones and mobile applications, young generation population sample is prominent, and various studies proved that primary mobile application Users belong to the young generation [45].

A. LINEAR REGRESSION

The regression equation used for analysis is given in equation 1.

$$y_i = \beta_{(0)} + \beta_{(1)}x_{(1)} + \beta_{(2)}x_{(2)} + \beta_{(3)}x_{(3)} \ldots + \beta_n x_n + \epsilon \tag{1}$$

where, y_i is the response, β_0 is the intercept, β_1 is the coefficient for x_1, similarly β_n is the coefficient for x_n, and ϵ is random error component, used to measure the actual observation of variable y.

The beta values are known as the model coefficients. These coefficients or values are learned during the model fitting stage using the ''least squares'' principle. Then, the fitted model is used for making predictions. Linear Regression is applied to exogenous variables to understand the relationship between ATU, PUS, US, PEU to measure the AOU.

B. SAMPLE DEMOGRAPHICS

A total population of 175 people participated in the study. 70% of the total population (121 respondents) were males, and 30% of the total population (54 respondents) were females. All the respondents selected for the research study were familiar with the usage of smartphones, mobile application and mobile banking technology, which constituted a good sample for the proposed research work [46]. The experimental dataset details are tabulated in Table 7.

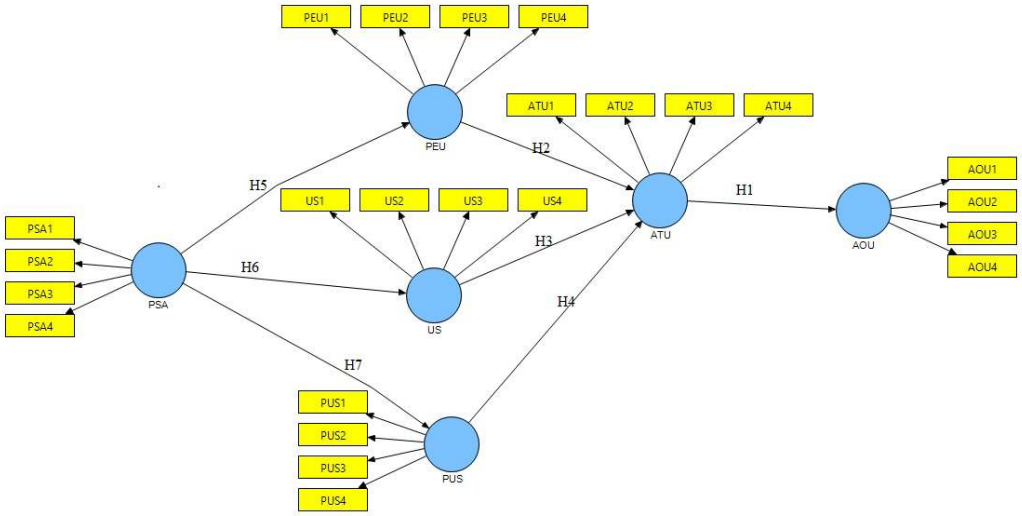

FIGURE 8. Research model to test the proposed hypotheses.

TABLE 7. Demographics details used to test the user acceptance of proposed research work.

Demographics	Details	Frequency	Percentage
Gender	Female	121	70
	Male	54	30
Age	18 to 25	79	45.14
	25 to 40	62	35.42
	40 to 60	34	19.44
Domain	IT background	63	36
	Non IT background	74	42.28
	Others	38	21.7
TOTAL		175	100

C. MEASURES FOR RESEARCH

A questionnaire is designed and developed based on the TAM model proposed by Davis. A five-point Likert scale ranging from (1) for ''Strongly disagree'' to (5) for ''Strongly agree'' is used to operationalize the parameters included in the proposed research model. Most of the questionnaire elements were adopted from the relevant prior research work with validation and terminology changes [46].

D. VALIDITY AND RELIABILITY OF THE MEASURES AND INSTRUMENT USED

The measures adapted and instruments used for the proposed study needs to be evaluated before testing the theory. Davis *et al.* [47] suggested finding the content validity through a panel consisting of experts to verify how well the instrument meets the required criteria. Thus, an independent interview is conducted with two professors and two engineers to evaluate if the research study covers relevant constructs. The suggestions were later incorporated. A pretesting with the instrument through interviews with different people helped to assess whether the instrument is functioning in the right way without excluding the desired phenomenon as suggested by [48].

VI. FORMAL SECURITY VERIFICATION OF THE PROPOSED ALGORITHM USING AVISPA TOOL

The simulation result of the proposed algorithm 1 using a formal security approach is discussed in this section. The most widely used and accepted modeling tool for building, analyzing and simulating the security protocol, AVISPA is used to verify and validate the security of the proposed scheme.

1) AVISPA OVERVIEW

AVISPA is a tool used for the validation of security protocols with the following capabilities.

- The support of a formal language to state the security system, their security capabilities, and vulnerabilities.
- The tool facilitates automatic analysis techniques with the help of different back ends.

AVISPA uses modular and expressive formal languages for specifying security protocols and their properties [23], [24]. The tool provides four different back ends namely, On–the–Fly Model–Checker (OFMC) [49], Constraint Logic based Attack Searcher (CL-Atse) [50], SAT-based model checker and tree automata based on an automatic approximation of security protocols to support security analysis [23]. The AVISPA uses HLPSL (High Level Protocol Specifications Language) based on different roles. Each participant role is represented using primary roles and scenarios of primary roles are denoted using composition roles [51]. All roles are independent of each other and exchange information using various parameters with the help of the channel.

In HLPSL, every participant plays a role during the execution of the protocol. The AVISPA uses dolev and yao's (dy) model to design the intruder [23] and it helps to play

TABLE 8. Symbols and keywords used in AVISPA to execute the proposed protocol.

Symbols	Descriptions
.	Associative concatination
,	Element seperation
;	Sequential composition in roles
:=	Local variable intialization
xor	XOR operation
^	Parallel composition in roles
=|>	Immediate transition
{ }_	Digital signature or Encryption
agent	Data- type for agents
Channel(dy)	Intruder channel
const	Constant data type
def=	Beginning of role body
hash_func	One way hash function
public_key	Public key for encryption
secret	Used to check the secrecy
witness	Check for authentication (with request)
request	Check for authentication (with witness)

the legitimate roles in the developed protocol. The translator hlpsl2if is used by AVISPA to convert the protocol to Intermediate Format (IF) during the execution. The IF is analyzed by the back end to examine the security goals are met or not. If all the identified and mentioned goals are satisfied by the protocol, the AVISPA simulator outputs ''SAFE''. If any vulnerabilities identified during the protocol execution results in ''UNSAFE'' output by the AVISPA with details and statistics. The Symbols and keywords of HLPSL used to represent the proposed scheme in AVISPA are tabulated in Table 8.

A. SIMULATION AND SECURITY ANALYSIS OF THE PROPOSED SYSTEM

The proposed protocol performs automated User authentication and secure key exchange between mobile User and CA as discussed in Algorithm 1. There are mainly four primary roles in the proposed protocol, namely the User, authentication server, token grant server, and the certificate authority. The role User is shown in Figure 9. The start signal initiates the process and triggers the state change from 0 to 1. The Snd() and Rcv() functions are used to send and receive parameters between different roles using ''dy'' channel. The role authentication server is shown in Figure 10. The role token grant server is shown in Figure 11.

The role Certificate Authority is shown in Figure 12. The role specifications for the session and environment are shown in Figure 13 and Figure 14 respectively. In the session role, all the basic roles are included for composition. The environment role resembles actual environment, where the intruder has access overall system resources. The environment role comprises of all global constants included in one or more session, where an adversary can play genuine user roles. The goals of the proposed scheme are mentioned in the goal environment.

AVISPA execution results are shown in the Figure 15 and Figure 16. The back ends OFMC and CL-Atse are used for simulation. Once new cryptographic protocols developed, they should be tested with already existing standards and compatibility. Formal analysis help and speeds up standardization by finding flaws and give evidence of security if no faults found. OFMC performs the job of protocol falsification and bounded session verification by adopting demand

```
role user (Ui, As, Tgs, Ca : agent,
        Ks, Kct, Ktg, Kcc, Kca : symmetric_key,
        H : hash_func,
        KP: public_key,
        Snd, RCV :channel(dy))
played_by Ui
def=
 local State : nat,
 Ai, TID, MAC, TS, Nn, OTP1, OTP2, IDs, IDc, Qms, Qms1, Qms2, Qms3, Nin,Z,Ski,PK: text
       const  subs1,subs2,subs3,subs4 :protocol_id
init State:=0
              transition
1.            State=0 /\ RCV(start)=|>
              State':=1 /\ TS':=new()
              /\ Nn':=new()
              /\ Snd({Nin.TID.MAC.TS'.Nn'}_KP)
 2. State = 1 /\RCV({Kct.Nin.MAC.TID.IDs.TS}_Ktg, {Kct}_Ski.TS, {Nin.MAC.IDs.TS}_Kct) =|>
       State' := 2 /\ Snd(IDc.{Nin.MAC.IDs.TS}_Kct, {Kct.Nin.MAC.TID.IDs.TS}_Ktg)

 3. State = 3 /\RCV({Kct.Nin.MAC.TID.IDs.TS}_Ktg, {Kct}_Ski.TS, {Nin.MAC.IDs.TS}_Kct) =|>
       State' := 4 /\ Snd(IDc.{Nin.MAC.IDs.TS}_Kct, {Kct.Nin.MAC.TID.IDs.TS}_Ktg)


 4. State = 5 /\RCV ({Kcc.Nin.MAC.IDs.TID.TS}_Kca, {Nin.MAC.IDs.TID.TS}_Kcc, {Kca.TS}_Kct)
=|>
 State' := 6 /\ Snd({Kcc.Nin.MAC.IDs.TID.TS}_Kca. {Nin.MAC.IDs.TID.TS}_Kcc)

 5. State = 7 /\ RCV({Qms}_Kcc)=|>
       State' :=  8 /\Snd({Qms1.Qms2.Qms3.Nn.Nin.MAC}_Kcc)
              /\secret({OTP1, OTP2, Nn, Qms, Qms1, Qms2}, subs2, Ui)
end role
```

FIGURE 9. User role specification of the proposed scheme.

driven method, the transition system resulting from ''IF'' specification. It allows analyzing protocols with respect to an algebraic theory of employed cryptographic operations which are part of the input [49]. The two techniques deployed are lazy intruder and constraints differentiation [24], [52]. Both the methods reduce the search space associated with a given protocol specification without excluding attacks or introducing new ones. The OFMC simulation results show that the protocol is ''SAFE'' from any flaws. The contract executed for a bounded number of sessions with 1432 visited nodes having a depth of 8 plies with a parse time of 0.009 seconds and search time of 5.10 seconds. The ''Goal As specified'' in the output format indicates that the purposes specified in the environment are considered during the protocol execution and the intruder has full access to all resources in public channel. The simulation result shows that the proposed scheme is secure from all vulnerabilities as defined in the goals.

Cl-Atse is a constraint logic based attack searcher for security protocols and services. Cl-Atse runs the protocol or set of services in all possible ways by representing the family of traces with positive or negative constraints on the intruder knowledge and variables [50]. Each run of a service step consists of adding new restrictions on the intruder and environment state. It reduces the constraints down to a normalized form and decides some security property has been violated. Cl-Atse does not limit the services in any way except bounding the maximum number of times the function to be iterated otherwise the analysis might be non terminating on secure services, and only heuristics, approximations, or restrictions on the input language could lift this limitation [23]. Cl-Atse is a typed model, where protocol description in the IF is equipped with a signature section describing the type of message between agents. If a security property is violated, then Cl-Atse outputs a warning ''UNSAFE'' with details of the analysis, property that was violated(secrecy for example), statistics on the number of explored states and an ATTACK TRACE giving details of the attack scenario. If no attack found, then Cl-Atse outputs a message ''SAFE'' showing no vulnerabilities in the protocol. The Cl-Atse output shows that the protocol named ''*END_TO_END_SECURE*'' with a bounded number of sessions having typed model with specified goals in the environment is executed. The statistics show that the protocol is ''*SAFE*'' with no attacks analyzed(Analyzed: 0 states) and no states with attacks reachable(Reachable: 0 states) [53]–[57]. The translation and computation time taken is 0.05 seconds and 0.0048 seconds (rounded off) respectively.

VII. TEST ENVIRONMENT AND TIME DELAY FOR USER AUTHENTICATION

The system is built to overcome the indefinite time delay occurred in the manual method where the user is

```
role asa(Ui, As, Tgs, Ca : agent,
        Ks, Kct, Ktg, Kcc, Kca : symmetric_key,
        H : hash_func,
        KP: public_key,
        Snd, RCV :channel(dy))

played_by As
def=
 local State : nat,
 Ai, TID, MAC, TS, Nn, OTP1, OTP2, IDs, IDc, Qms, Qms1, Qms2,
Qms3,Nin,Z,Ski,PK: text
        const  subs1,subs2,subs3,subs4 :protocol_id

init State := 0
        transition

1.              State = 0 /\ RCV({Nin.TID.MAC.TS'.Nn'}_KP) =|>
                State' := 1 /\ OTP1':= new()
                /\ OTP2':= new()
                /\Z':=H(xor(Nn, 1).OTP1'.OTP2'.MAC).TS
                /\Ski':= (MAC.OTP1.OTP2)
        /\Snd({Kct.Nin.MAC.TID.IDs.TS}_Ktg, {Kct}_Ski.TS,
{Nin.MAC.IDs.TS}_Kct)
        /\secret({OTP1, OTP2, Nn}, subs3, As)
```

FIGURE 10. Authentication Server role specification of the proposed scheme.

TABLE 9. Time delay for user authentication.

Sl.No	Operation	Number of operation	Time/operation in seconds	Total Time in seconds
1	Asymmetric Encryption (RSA)	3	9.99	29.97
2	Symmetric Encryption (AES256-CBC Mode)	9	2.88	25.92
3	Hash Operation (SHA-512)	2	3.1	6.3
4	Symmetric Key Generation	3	1.89	5.67
5	Scanning Aadhar Card Using Mobile Phone	1	5	5
TOTAL TIME FOR USER AUTHENTICATION				72.86

authenticated through confrontation by the physical movement to registered offices. The time delay occured for User authentication due to various operations are shown in Table 9. The test environment consists of smart phone and laptops. The specification of the User (mobile client) is shown in Table 10. The Server and CA details are given in Table 11.

From Table 9, the total time consumed for user authentication in the described set up is 72.86 seconds which is very very less than the time consumption by the claimant to physically move for confrontation to the registered office and it is acceptable with high efficiency.

TABLE 10. Test environment (client specification).

Device	Samsung galaxy ON5 Pro (Mobile Phone)
OS	Android 6,Marshmallow
RAM	2 GB
Processor	Cortex,1.3 GHz,quadcore
Software	Android studio 2.3

VIII. DATA ANALYSIS AND RESULTS

In this section, the reliability analysis of the proposed study is performed. Seven hypotheses (H1 to H7) are formulated

```
role tgsa (Ui, As, Tgs, Ca : agent,
        Ks, Kct, Ktg, Kcc, Kca : symmetric_key,
        H : hash_func,
        KP: public_key,
        Snd,RCV :channel(dy))

played_by Tgs
def=
 local State : nat,
        Ai, TID, MAC, TS, Nn, OTP1, OTP2, IDs, IDc, Qms, Qms1, Qms2,
Qms3,Nin,Z, Ski,PK: text
       const  subs1,subs2,subs3,subs4 :protocol_id
init State := 0
       transition
1.              State = 0 /\ RCV(IDc.{Nin.MAC.IDs.TS}_Kct,
{Kct.Nin.MAC.TID.IDs.TS}_Ktg) =|>
                State' := 1 /\Snd({Kcc.Nin.MAC.IDs.TID.TS}_Kca,
{Nin.MAC.IDs.TID.TS}_Kcc, {Kca.TS}_Kct)
       /\secret({OTP1, OTP2, Nn}, subs4, Tgs)
end role
```

FIGURE 11. Token Grant Server role specification of the proposed scheme.

TABLE 11. Test environment (servers and CA specification).

Device	HP Probook 440 G4 (Laptop)
OS	Windows 8.1 Enterprise and Ubuntu 16.04
RAM	4 GB
Processor	Intel R(Core),TMi5-52000 cpu @2.2 GHz
Softwares	OpenSSL,JDK,Python

and tested as a part of a research study. A stepwise regression analysis is performed on the exogenous and endogenous variables. It is done using the IBM SPSS software. The SmartPLS software is used for generating consolidated path model. The reliability measure is shown to check whether the test consistently measures what it is expected to measure. The internal consistency or reliability is measured using the computed Chronbach's alpha value. Reliability test such as Chronbach's alpha is usually used to measure if the questionnaire with multiple Lickert scale questionnaire items is reliable. The questions are developed to estimate the latent variable (hidden/unobservable), and Chronbach's alpha is used to tell whether the test generated accurately measures interested latent variable. Table 12 shows results of the reliability analysis. The rule of thumb for interpreting Chronbach's alpha with a Likert scale data is shown in the Table 13.

The Composite Reliability of reflective constructs are shown in Table 14 and Figure 17. The Composite Reliability

TABLE 12. Reliability analysis among variables.

Cronbach's Alpha	Number of items
0.920	6

TABLE 13. Internal consistency measure with Chronbach's Alpha.

Chronbach's Alpha	Internal Consistency
α >0.9	Excellent
0.9 >α >= 0.8	Good
0.8 >α >= 0.7	Acceptable
0.7 >α >= 0.6	Questionable
0.6 >α >= 0.5	Poor
0.5 >α	Unacceptable

TABLE 14. Composite reliability of reflective constructs.

Reflective constructs	Composite reliability
AOU	0.959
ATU	0.945
PEU	0.952
PSA	0.931
PUS	0.903

of all reflective constructs is above the threshold value. It implies that high level of internal consistency reliability exists for all five reflective constructs.

Convergent Validity is assessed by Average Variance Extracted (AVE). The AVE value is tabulated in Table 15

```
role caa (Ui, As, Tgs, Ca : agent,
        Ks, Kct, Ktg, Kcc, Kca : symmetric_key,
         H : hash_func,
        KP: public_key,
        Snd, RCV :channel(dy))

played_by Ca
def=
 local State : nat,
  Ai, TID, MAC, TS, Nn, OTP1, OTP2, IDs, IDc, Qms, Qms1, Qms2,
Qms3,Nin,Z,Ski,PK: text
        const  subs1,subs2,subs3,subs4 :protocol_id
init State := 0
        transition


1.              State = 0 /\ RCV({Kcc.Nin.MAC.IDs.TID.TS}_Kca,
{Nin.MAC.IDs.TID.TS}_Kcc) =|>
                State' := 1 /\Snd({Qms}_Kcc)

2.              State = 2 /\ RCV({Qms1.Qms2.Qms3.Nn.Nin.MAC}_Kcc) =|>
                State' := 3 /\Ski':= MAC.OTP1.OTP2
                /\Snd({{PK}_Kcc}_Ski)
                /\secret({PK}, subs1, Ca)

end role
```

FIGURE 12. Certificate Authority role specification of the proposed scheme.

```
role session(Ui, As, Tgs, Ca : agent,
        Ks, Kct, Ktg, Kcc, Kca : symmetric_key,
        H : hash_func,
        KP: public_key)
def=
local SA, SB, RA, RB, SC, SD, RC, RD: channel (dy)
composition
        user(Ui, As, Tgs, Ca, Ks, Kct, Ktg, Kcc, Kca, H,KP, SA, RA)
        /\ asa(Ui, As, Tgs, Ca, Ks, Kct, Ktg, Kcc, Kca, H,KP, SB, RB)
        /\ tgsa(Ui, As, Tgs, Ca, Ks, Kct, Ktg, Kcc, Kca, H,KP, SC, RC)
        /\ caa(Ui, As, Tgs, Ca, Ks, Kct, Ktg, Kcc, Kca, H,KP, SD, RD)
end role
```

FIGURE 13. Role specification for the session of the proposed scheme.

and plotted in Figure 18. The AVE values for all reflective constructs are above 0.5, which means the measure of all reflective constructs have high level of convergent validity.

```
role environment()
def=
const ui, as, tgs, ca: agent,
ks, kct, ktg, kcc, kca : symmetric_key,
h : hash_func,
kp: public_key,
subs1, subs2,subs3,subs4 : protocol_id
intruder_knowledge = {ui, as, tgs, ca, h}
composition
session (ui, as, tgs, ca, ks, kct, ktg, kcc, kca, h,kp)
/\session(ui, as, tgs, ca, ks, kct, ktg, kcc, kca, h,kp)
/\session(ui, as, tgs, ca, ks, kct, ktg, kcc, kca, h,kp)
/\session(ui, as, tgs, ca, ks, kct, ktg, kcc, kca, h,kp)
end role
goal

secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
secrecy_of subs4

end goal
environment()
```

FIGURE 14. Role specification for the goal and environment of the proposed scheme.

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/END_TO_END_SECURE.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 5.10s
 visitedNodes: 1432 nodes
 depth: 8 plies
```

FIGURE 15. On-the-fly model checker (OFMC) simulation result.

IX. INFERENCES FROM THE TABULAR DATA

The following section discusses model summary and coefficients for each exogenous variable to measure the corresponding endogenous value. The R value gives the correlation between observed value and the predicted value. R^2 is the coefficient of determination and explains about

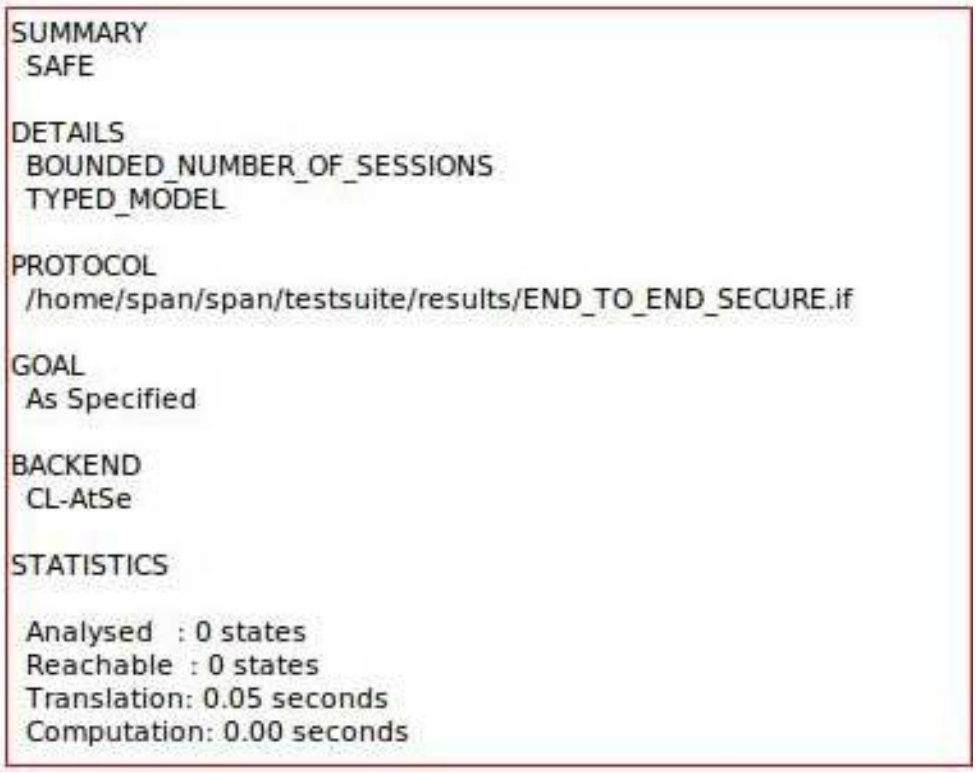

FIGURE 16. Constraint logic based attack searcher (CL-AtSe) simulation result.

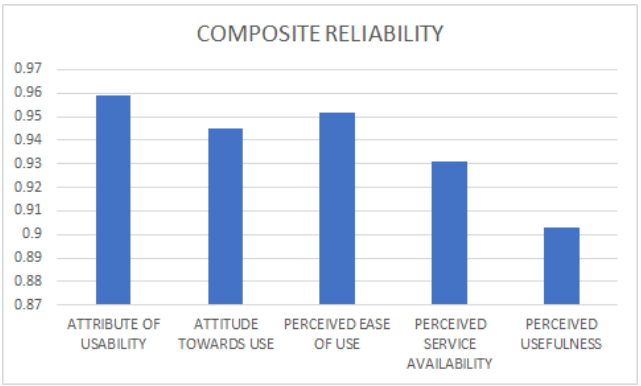

FIGURE 17. Plot of composite reliability.

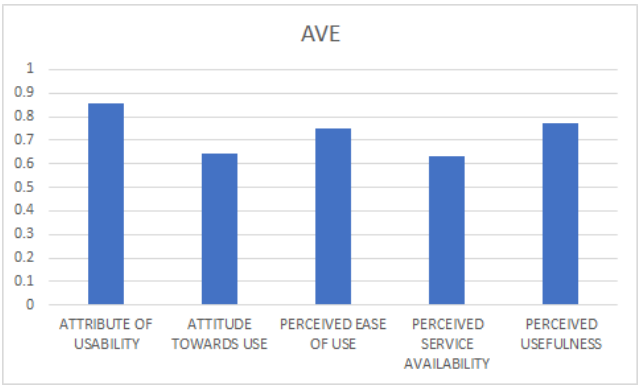

FIGURE 18. AVE of reflective constructs chart.

TABLE 15. Average variance extracted (AVE).

Reflective Constructs	AVE
AOU	0.859
ATU	0.645
PEU	0.752
PSA	0.631
PUS	0.770

what percentage of endogenous variable is defined by the exogenous variable. R^2 is the basic matrix and tells how much variance is described by the model. For example in Table 16,

TABLE 16. Model Summary (Predictor: PSA and dependent variable: PEU).

Model	R	R^2	Adjusted R^2
1	0.989	0.989	0.988

the R^2 value is 0.989 which implies that the exogenous variable PSA explains 98.9% of the endogenous variable PEU. If we add more variables to the model, the R^2 value will increase, but the adjusted R^2 value does not increase unless the added variable is significant.

The Coefficient table has unstandardized and standardized coefficients. The unstandardized coefficient is helpful to

TABLE 17. Model summary of PSA to PEU coefficients.

Model	Unstandardized Coefficients		Standardized Coefficients	t	sig.
	B	Std. Error	Beta		
1{Constant}	-1.278	0.124		-10.288	0.000
PSA(AVG)	0.983	0.008	0.994	122.739	0.000

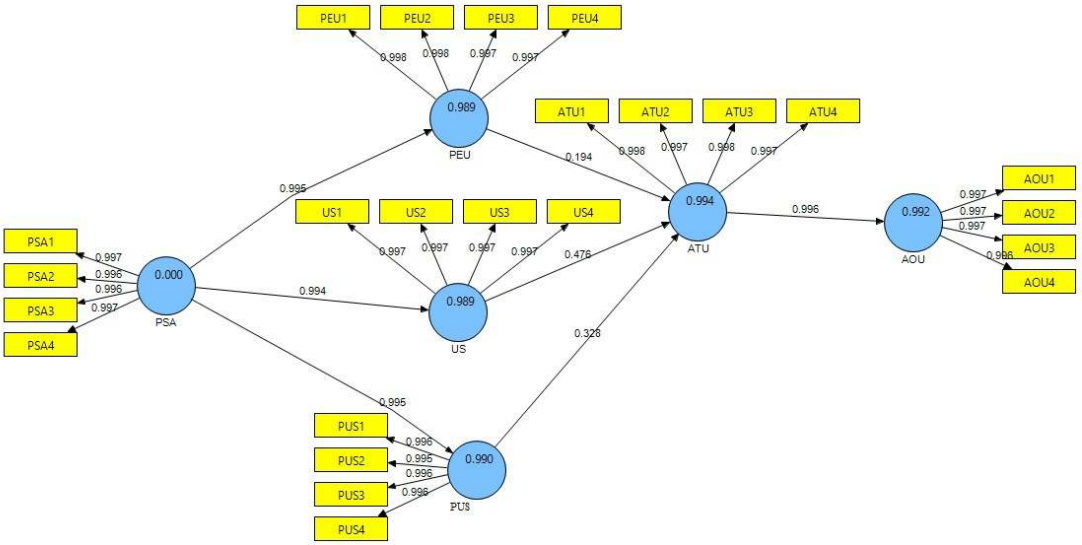

FIGURE 19. Execution of PLS algorithm in SmartPLS.

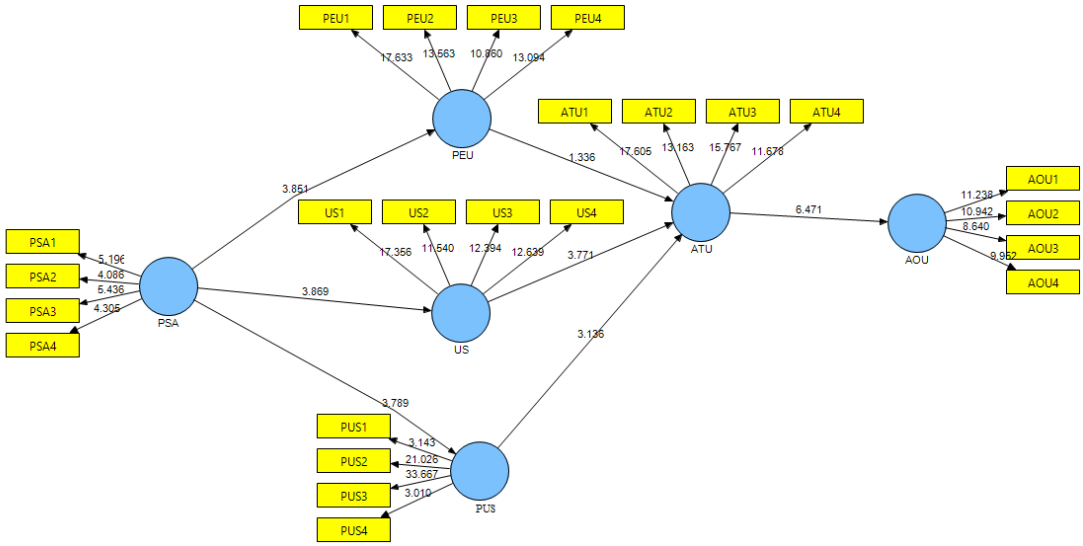

FIGURE 20. Execution of PLS BOOTSTRAP algorithm in SmartPLS.

TABLE 18. Model summary (predictor: PSA and dependent variable: PUS).

Model	R	R^2	Adjusted R^2
1	0.990	0.986	0.989

predict the things in the real world, whereas the standardized coefficients are helpful to compare between different predictors based on the standard deviation. For example in Table 25, the Beta value is 0.996, which means that with one standard deviation increase in ATU, we can expect 99.6% increase in AOU. It implies a strong influence of ATU over AOU. With a significance level (sig.) of 5% (or confidence level of 95%), the path coefficients are significant if the $|t|$ value is higher than 1.96. It is clear from the coefficients table that both $|t|$ value and sigma are in the accepted range. Similarly, other coefficient table values can be interpreted.

TABLE 19. Model summary of PSA to PUS coefficients.

Model	Unstandardized Coefficients		Standardized Coefficients	t	sig.
	B	Std. Error	Beta		
1{Constant}	-0.930	0.121		-7.657	0.000
PSA(AVG)	0.988	0.008	0.995	125.941	0.000

TABLE 20. Model summary (predictor: PSA and dependent variable: US).

Model	R	R^2	Adjusted R^2
1	0.989	0.988	0.988

TABLE 21. Model summary of PSA to US coefficients.

Model	Unstandardized Coefficients		Standardized Coefficients	t	sig.
	B	Std. Error	Beta		
1{Constant}	-1.020	0.127		-8.024	0.000
PSA(AVG)	0.986	0.007	0.994	120.171	0.000

TABLE 22. Model summary (predictor: PUS, PEU and US and dependent variable: ATU).

Model	R	R^2	Adjusted R^2
1	0.994	0.993	0.993

TABLE 23. Model summary of PUS, US, PEU to ATU coefficients.

Model	Unstandardized Coefficients		Standardized Coefficients	t	sig.
	B	Std. Error	Beta		
1{Constant}	-0.025	0.88		-0.282	0.000
PEU(AVG)	0.202	0.092	0.201	1.87	0.031
US(AVG)	0.486	0.085	0.487	5.701	0
PUS (AVG)	0.311	0.067	0.311	4.629	0

TABLE 24. Model summary (Predictor: ATU and dependent variable: AOU).

Model	R	R Square	Adjusted R Square
1	0.992	0.990	0.991

TABLE 25. Model summary of ATU to AOU coefficients.

Model	Unstandardized Coefficients		Standardized Coefficients	t	sig.
	B	Std. Error	Beta		
1{Constant}	-0.151	0.100		-1.515	0.132
ATU(AVG)	0.994	0.007	0.996	152.361	0.00

The execution of PLS algorithm in ANN is shown in Figure 19. It is used to construct correlations. The factor loadings are also displayed in the diagram. Factor loadings close to 1 indicate that the factor strongly influence the variable. Inside each node, the corresponding R^2 values are shown.

Figure 20 explains the execution of PLS Bootstrap algorithm. The execution results in the production of path weights and Regression weights to identify significant paths. The path between two different nodes has the $|t|$ value displayed in it. It can be observed from the ANN model that, the path from PEU to ATU is not significant because the t value is 1.336 which is not in an acceptable range.

From Table 23, it can be observed that, effect of PEU on ATU is not significant because of the $|t|$ value being 1.87.

Using regression, the AOU can be computed with the help of equation 2.

$$\text{AOU} = -0.151 + 0.994 * \text{ATU} \tag{2}$$

where, ATU is stated as shown in equation 3.

$$\text{ATU} = -0.025 + 0.202 * \text{PEU} + 0.486 * \text{US} + 0.311 * \text{PUS} \tag{3}$$

The PEU, US and PUS can be estimated using equations 4, 5 and 6.

$$\text{PEU} = -1.278 + 0.983 * \text{PSA} \tag{4}$$

$$\text{PUS} = -0.930 + 0.986 * \text{PSA} \quad (5)$$

$$\text{US} = -1.020 + 0.986 * \text{PSA} \quad (6)$$

X. LESSONS LEARNT

The proposed scheme addresses the issue of manual confrontation involved in User identification and authentication. It eliminates the indefinite time engaged in direct manual intervention by using Aadhar card based automated system. The validity of the proposed protocol is verified using the AVISPA tool. The results demonstrate that the delegation of the computational task to abundant resource devices will not hamper the system. It also shows that it is safe and secure. The user behavior while using the system is captured and learned using extended TAM. The result is consolidated in the form of Attribute of Usability, and it shows that the potential target Users accept the system. The study and experimentation also show that the implementation of an automated mechanism can save a significant amount of time.

XI. CONCLUSION AND FUTURE SCOPE

User identification and authentication is a process of verification of the credentials to confirm the validity of the User. It plays a vital role as it provides access to system resources and confidential data. In the proposed work, the drawback of the manual procedure to achieve a User authentication is overcome by employing an automated process. The credentials to validate the User is encoded NIN and it is obtained from the Aadhar card. The mobile devices are resource constrained and computationally inefficient compared to traditional high-performance computers and servers. The cryptographic operations such as key generation, encryption, and digital signature generation and verification involve complex mathematical operations. In the proposed authentication and symmetric key exchange algorithm, the complex mathematical operations are delegated to resource abundant and computationally efficient devices to reduce the workload of resource-constrained mobile devices. The safety and security of the proposed scheme are validated using AVISPA formal verification technique. The simulation results demonstrate that the scheme is safe and secure. The acceptance of the model is verified using experimental results achieved using the extended TAM. The relationship between the exogenous and the endogenous variables is studied using the regression model. The influence of the independent variable on the dependent variable is proved using the ANN. The ANN shows that the PEU has no significant influence over the ATU. The model developed explains the strong relationship between the ATU and the AOU. The $|t|$ value shown in the path between the ATU and the AOU is above the standard normal deviation which implies its acceptance. The ANN model also indicates the US has highest influence over ATU and it in turn influences AOU. The experiment results show that the time consumption for the User authentication is also in the acceptable range compared to the manual process. The study proves that the automated User identification system is accepted by potential target Users.

In the future, the protocol can be optimized to increase the efficiency of the proposed model. The system performance can be improvised by incorporating higher efficient encryption and digital signature algorithms. The proposed scheme can be further applied to IoT and wireless sensor networks to achieve the authentication and secure transmission of messages. The model can also be extended to a distributed environment.

REFERENCES

[1] S. Agrawal, S. Banerjee, and S. Sharma, "Privacy and security of Aadhaar: A computer science perspective," *Econ. Political Weekly*, vol. 52, no. 37, pp. 93–102, 2017.

[2] Y. Lee, J. Lee, and J. Song, "Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce," *Comput. Commun.*, vol. 30, no. 4, pp. 893–903, 2007.

[3] K. Prakasha, B. Muniyal, V. Acharya, S. Krishna, and S. Prakash, "Efficient digital certificate verification in wireless public key infrastructure using enhanced certificate revocation list," *Inf. Secur. J., Global Perspective*, vol. 27, no. 4, pp. 214–229, 2018. [Online]. Available: https://doi.org/10.1080/19393555.2018.1516836

[4] K. N. Mishra, "AAdhar based smartcard system for security management in South Asia," in *Proc. IEEE Int. Conf. Control, Comput., Commun. Mater. (ICCCCM)*, Oct. 2016, pp. 1–6.

[5] P. G. Schierz, O. Schilke, and B. W. Wirtz, "Understanding consumer acceptance of mobile payment services: An empirical analysis," *Electron. Commerce Res. Appl.*, vol. 9, no. 3, pp. 209–216, 2010.

[6] Y. Liu, H. Li, and C. Carlsson, "Factors driving the adoption of m-learning: An empirical study," *Comput. Educ.*, vol. 55, no. 3, pp. 1211–1219, 2010.

[7] K. Chen, J. V. Chen, and D. C. Yen, "Dimensions of self-efficacy in the study of smart phone acceptance," *Comput. Standards Interfaces*, vol. 33, no. 4, pp. 422–431, 2011.

[8] B. Šumak, M. Heričko, and M. Pušnik, "A meta-analysis of e-learning technology acceptance: The role of user types and e-learning technology types," *Comput. Hum. Behav.*, vol. 27, no. 6, pp. 2067–2077, 2011.

[9] T. Zhou and Y. Lu, "The effects of personality traits on user acceptance of mobile commerce," *Int. J. Hum.-Comput. Interact.*, vol. 27, no. 6, pp. 545–561, 2011.

[10] A.-C. Teo, G. W.-H. Tan, K.-B. Ooi, and B. Lin, "Why consumers adopt mobile payment? A partial least squares structural equation modelling (PLS-SEM) approach," *Int. J. Mobile Commun.*, vol. 13, no. 5, pp. 478–497, 2015.

[11] F. J. Zareen and S. Jabin, "Authentic mobile-biometric signature verification system," *IET Biometrics*, vol. 5, no. 1, pp. 13–19, 2016.

[12] A. Fongen, "Optimization of a public key infrastructure," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2011, pp. 1440–1447, doi: 10.1109/MILCOM.2011.6127509.

[13] X. Wang, Y. Bai, and L. Hu, "Certification with multiple signatures," in *Proc. 4th Annu. ACM Conf. Res. Inf. Technol. (RIIT)*, 2015, pp. 13–18, doi: 10.1145/2808062.2808068.

[14] S. Ray and G. P. Biswas, "Design of mobile public key infrastructure (M-PKI) using elliptic curve cryptography," *J. Cryptogr. Inf. Secur.*, vol. 3, no. 1, pp. 25–37, 2013.

[15] S. Ma, Q. Huang, M. Zhang, and B. Yang, "Efficient public key encryption with equality test supporting flexible authorization," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 458–470, Mar. 2015.

[16] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33, 2017.

[17] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017.

[18] K. Park, Y. Park, Y. Park, A. G. Reddy, and A. K. Das, "Provably secure and efficient authentication protocol for roaming service in global mobility networks," *IEEE Access*, vol. 5, pp. 25110–25125, 2017.

[19] W. Tu and L. Lai, "Keyless authentication and authenticated capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3696–3714, May 2018.

[20] W. Luo, Y. Hu, H. Jiang, and J. Wang, "Authentication by encrypted negative password," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 114–128, Jan. 2019.

[21] E. Erdem and M. T. Sandıkkaya, "OTPaaS—One time password as a service," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 743–756, Mar. 2019.
[22] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, "Secure authentication protocol for mobile payment," *Tsinghua Sci. Technol.*, vol. 23, no. 5, pp. 610–620, 2018.
[23] R. Madhusudhan, M. Hegde, and I. Memon, "A secure and enhanced elliptic curve cryptography-based dynamic authentication scheme using smart card," *Int. J. Commun. Syst.*, vol. 31, no. 11, 2018.
[24] R. Madhusudhan and M. Hegde, "Security bound enhancement of remote user authentication using smart card," *J. Inf. Secur. Appl.*, vol. 36, pp. 59–68, Oct. 2017.
[25] W. Ding and C.-G. Ma, "Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards," *J. China Univ. Posts Telecommun.*, vol. 19, no. 5, pp. 104–114, 2012.
[26] R. S. Pippal, C. D. Jaidhar, and S. Tapaswi, "Security vulnerabilities of user authentication scheme using smart card," in *Data and Applications Security and Privacy XXVI*, vol. 7371, N. Cuppens-Boulahia, F. Cuppens, and J. Garcia-Alfaro, Eds. Berlin, Germany: Springer, 2012, pp. 106–113.
[27] A. S. M. Kayes, J. Han, W. Rahayu, T. Dillon, M. S. Islam, and A. Colman, "A policy model and framework for context-aware access control to information resources," *Comput. J.*, to be published, doi: 10.1093/comjnl/bxy065.
[28] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394, Feb. 2014.
[29] A. Kayes, W. Rahayu, T. Dillon, and E. Chang, "Accessing data from multiple sources through context-aware access control," in *Proc. IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 551–559.
[30] A. Castiglione *et al.*, "Hierarchical and shared access control," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 850–865, Apr. 2016.
[31] Q. Liu, H. Zhang, J. Wan, and X. Chen, "An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing Internet of Things," *IEEE Access*, vol. 5, pp. 7001–7011, 2017.
[32] S. A. Nikou and A. A. Economides, "Mobile-based assessment: Investigating the factors that influence behavioral intention to use," *Comput. Educ.*, vol. 109, pp. 56–73, Jun. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0360131517300283
[33] K.-B. Ooi and G. W.-H. Tan, "Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card," *Expert Syst. Appl.*, vol. 59, pp. 33–46, Oct. 2016.
[34] P. Y. K. Chau and P. J.-H. Hu, "Information technology acceptance by individual professionals: A model comparison approach," *Decis. Sci.*, vol. 32, no. 4, pp. 699–719, 2001.
[35] M. Ervasti and H. Helaakoski, "Case study of application-based mobile service acceptance and development in finland," *Int. J. Inf. Technol. Manage.*, vol. 9, no. 3, pp. 243–259, 2010.
[36] G. Müller-Seitz, K. Dautzenberg, U. Creusen, and C. Stromereder, "Customer acceptance of RFID technology: Evidence from the German electronic retail sector," *J. Retailing Consum. Services*, vol. 16, no. 1, pp. 31–39, 2009.
[37] A. Dabrowski, K. Krombholz, J. Ullrich, and E. R. Weippl, "QR inception: Barcode-in-barcode attacks," in *Proc. 4th ACM Workshop Secur. Privacy Smartphones Mobile Devices*, 2014, pp. 3–10.
[38] P. Y. A. Ryan and S. A. Schneider, *The Modelling and Analysis of Security Protocols: The CSP Approach*, 1st ed. Reading, MA, USA: Addison-Wesley, 2001.
[39] A. N. Haidar and A. E. Abdallah, "Formal modelling of PKI based authentication," *Electron. Notes Theor. Comput. Sci.*, vol. 235, pp. 55–70, Apr. 2009.
[40] S. Zhang, J. Zhao, and W. Tan, "Extending TAM for online learning systems: An intrinsic motivation perspective," *Tsinghua Sci. Technol.*, vol. 13, no. 3, pp. 312–317, 2008.
[41] V.-Q. Pan, P.-Q. Chew, A. S.-G. Cheah, C.-H. Wong, and G. W.-H. Tan, "Mobile marketing in the 21st century: A partial least squares structural equation modelling approach," *Int. J. Model. Oper. Manage.*, vol. 5, no. 2, pp. 83–99, 2015.
[42] S.-H. Ho and Y.-Y. Ko, "Effects of self-service technology on customer value and customer readiness: The case of internet banking," *Internet Res.*, vol. 18, no. 4, pp. 427–446, 2008.
[43] D. Balachandran and G.-W.-H. Tan, "Regression modelling of predicting NFC mobile payment adoption in Malaysia," *Int. J. Model. Oper. Manage.*, vol. 5, no. 2, pp. 100–116, 2015.
[44] K. Pikkarainen, "Consumer acceptance of online banking: An extension of the technology acceptance model," *Internet Res.*, vol. 14, no. 3, pp. 224–235, 2015.
[45] N. Pindeh, N. M. Suki, and N. M. Suki, "User acceptance on mobile apps as an effective medium to learn kadazandusun language," *Procedia Econ. Finance*, vol. 37, pp. 372–378, Jan. 2016.
[46] H. M. Abu-Dalbouh, "A questionnaire approach based on the technology acceptance model for mobile tracking on patient progress applications," *J. Comput. Sci.*, vol. 9, no. 6, pp. 763–770, 2013.
[47] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: A comparison of two theoretical models," *Manage. Sci.*, vol. 35, pp. 982–1003, Aug. 1989.
[48] I.-L. Wu and J.-L. Chen, "An extension of trust and TAM model with TPB in the initial adoption of on-line tax: An empirical study," *Int. J. Hum.-Comput. Stud.*, vol. 62, no. 6, pp. 784–808, 2005.
[49] D. Basin, S. Mödersheim, and L. Vigano, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, 2005.
[50] M. Turuani, "The CL-Atse protocol analyser," in *Proc. Int. Conf. Rewriting Techn. Appl.*, vol. 4098. Springer, 2006, pp. 277–286.
[51] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2439–2461, 2015.
[52] S. Mödersheim and L. Viganò, "The open-source fixed-point model checker for symbolic analysis of security protocols," in *Foundations of Security Analysis and Design V*, vol. 5705. Springer, 2009, pp. 166–194.
[53] S. Barman, A. K. Das, D. Samanta, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Provably secure multi-server authentication protocol using fuzzy commitment," *IEEE Access*, vol. 6, pp. 38578–38594, 2018.
[54] N. Ravanbakhsh and M. Nazari, "An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 55–88, 2018.
[55] R. Amin, S. H. Islam, P. Vijayakumar, M. K. Khan, and V. Chang, "A robust and efficient bilinear pairing based mutual authentication and session key verification over insecure communication," *Multimedia Tools Appl.*, vol. 77, no. 9, pp. 11041–11066, 2018.
[56] L. Chengzhe, L. Hui, Z. Yueyu, and C. Jin, "Simple and low-cost re-authentication protocol for HeNB," *China Commun.*, vol. 10, no. 1, pp. 105–115, 2013.
[57] S. K. H. Islam and G. P. Biswas, "A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 26, no. 1, pp. 55–67, 2014.

KRISHNA PRAKASHA received the B.E. and M.Tech. degrees from Viswesvaraya Technological University, Belagavi. He is currently pursuing the Ph.D. degree in network security with the Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, where he is currently an Assistant Professor (Senior) with the Department of Information and Communication Technology. He has more than 23 publications in national and international conferences/journals. His research interests include information security, network security, algorithms, real time systems, and wireless sensor networks.

BALACHANDRA MUNIYAL received the B.E. degree in computer science and engineering from Mysore University and the M.Tech. and Ph.D. degrees in computer science and engineering from the Manipal Academy of Higher Education, Manipal, India. He carried out his M.Tech. project work in T-Systems Nova GmbH, Bremen, Germany. He was deputed to Manipal International University, Malaysia, in 2014. He is currently a Professor and the Head with the Department of Information & Communication Technology, Manipal Institute of Technology, Manipal. He has 25 years of teaching experience in various Institutes. He has more than 30 publications in national and international conferences/journals. His research interest includes network security.

VASUNDHARA ACHARYA received the B.E. degree in information science and engineering from the N.M.A.M. Institute of Technology, Nitte, and the M.Tech. degree in software engineering from the Manipal Institute of Technology (MIT), Manipal Academy of Higher Education (MAHE), Manipal. She plans to pursue her Ph.D in Bioinformatics. She is currently an Assistant Professor with the Department of Computer Science and Engineering, MIT, MAHE. Her current interests include information security, medical image processing, and artificial intelligence. She has been serving as reviewer for various International Journals. She is the Review Board Member of the *International Journal of GEOMATE*, Japan, and an Active Reviewer of *Medical & Biological Engineering & Computing*. She is serving as an Editorial Board Member for *Information and Computer Security*, Enpress publisher.