Hindawi
Security and Communication Networks
Volume 2021, Article ID 9940183, 15 pages
https://doi.org/10.1155/2021/9940183

Research Article

Lightweight Technical Implementation of Single Sign-On Authentication and Key Agreement Mechanism for Multiserver Architecture-Based Systems

Darpan Anand,[1] **Vineeta Khemchandani**,[2] **Munish Sabharawal**,[3] **Omar Cheikhrouhou**,[4] **and Ouissem Ben Fredj**[5]

[1]*Chandigarh University, Punjab 140301, India*
[2]*J.S.S. Academy of Technical Education, Noida, India*
[3]*Galgotias University, Noida, India*
[4]*College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[5]*University of Kairouan, Route Périphérique Dar El Amen 3100, Kairouan, Tunisia*

Correspondence should be addressed to Ouissem Ben Fredj; ouissem.benfredj@gmail.com

Received 21 March 2021; Revised 29 April 2021; Accepted 4 May 2021; Published 17 May 2021

Academic Editor: Vijay Kumar

Authentication is the primary and mandatory process for any Information and Communication Technology (ICT) application to prove the legitimacy of the genuine user. It becomes more important and crucial for public platforms like e-governance platforms. The Government of India is transforming the country into Digital India through various e-governance initiatives based on ICT. For authentication, National e-Authentication Framework (NeAF) was proposed by the Indian government which is a policy framework for authentication. This framework does not provide any technical and unified solution for authentication systems while it is based on centralized verification data. In this paper, we proposed a solution for the authentication which provides the unified authentication solution for the Indian e-governance system with existing infrastructure. This solution also provides the features such as scalability, security, and transparency based on distributed computing and working on multiserver architecture. This solution also fulfills the need of the current Indian government to provide multiple e-governance services through a single smart card.

1. Introduction

Authentication is the primary and mandatory process for any application to prove the legitimacy of the user [1]. It becomes more important and crucial for public platforms. There are many ways to prove the authenticity of the user for any application, software, or service and authentication where ICT has been used. It can be done using various techniques such as password and biometrics [2] and is used in various sectors such a banking [2, 3]. But, due to the increase in Internet coverage, various organizations, groups, companies, and firms started the delivery of their services through Information Communication Technology (ICT). One of the popular examples of this type of service is e-governance. Similar to the other applications, authentication is also required it. The Government of India also took serious steps towards transforming the country to Digital India through various e-governance initiatives based on Information Communication Technology (ICT). In the pace of development, National e-Authentication Framework (NeAF) was proposed by the Indian government. NeAF has been prepared by the National e-Governance Division (NeGD) within the Department of Information Technology (DIT).

NeAF is a policy framework for authentication for the Indian e-governance system. This paper is analyzing the requirements of an authentication protocol for the Indian e-governance system under the boundaries of NeAF.

Further, the paper extends up to the implementation, its concepts, and architecture to overcome the authentication issues and provides an integrated and unified view to the whole Indian e-governance system. The problem arises that individual registration and authentication process is required for each e-governance service. Therefore, a unified single sign-on authentication technique is required for the Indian e-governance system to integrate all e-governance services. The same problem is reflected in the survey conducted by us [4, 5].

Due to the increase in Internet coverage, various organizations, groups, companies, and firms started the delivery of their services through Information Communication Technology (ICT); therefore, authentication is becoming the most important process to provide accessibility of the services only for a legitimate user [6]. The same concept is applying by the government to serve its citizens through various services, which is called e-governance [7–9].

Since the 1970s, the Government of India took serious steps towards transforming the country to Digital India through various e-governance initiatives based on Information Communication Technology (ICT) [5, 10]. The journey of e-governance development in India started in 1970 with the establishment of the Department of Electronics, which is related to ICT development [11]. Then, National Information Center (NIC) was established in 1977, NICNET which is a satellite-based computer network was established in 1987, and District Information System of the National Information Center (DISNIC) was launched in 1990 [12]. Ministry of Information Technology was established to monitor Information Technology-related issues in 2000, the government formally launched its National e-Governance Plan (NeGP) [13], a guideline for all types of governments under the federal structure to implement e-governance in 2000 [14], e-Authentication framework was launched for user authentication for e-governance under NeGP in 2012 [15], next version of National e-Governance Plan e-Kranti is launched to improve and strengthen the existing NeGP in 2013, and finally, Digital India was established in the year 2014. In the pace of development, National e-Authentication Framework (NeAF) was proposed by the Indian government. NeAF has been prepared by the National e-Governance Division (NeGD) within the Department of Information Technology (DIT). NeAF is a policy framework for authentication to prove the legitimacy of the citizens to access various services of/from the Indian e-governance system [16].

There is no provision to access various services through single sign-on. User needs to register at every portal of government service, and the architecture of these services is different. There are various authentication techniques adopted by the respective department on their own, such as biometric, Q&A, OATH, OTP authentication, and LDAP. It creates a problem for integration and intercommunication. The second issue is the scale of the users. How can the government offer to access huge services at every point for billions of people? This paper found a solution to install the thin service over the ATM and other kiosks to access government services along with the existing financial services. Later, the architecture to implement thin service is also explained in this manuscript. Therefore, the UIAP is secure, multiserver architecture-oriented, based on distributed computing, using smart card, and able to integrate the existing system and fulfill the need of billions of people to access the government services to provide a unified view to the Indian e-governance system.

The available authentication framework and developments are explained at the outset of this paper which includes the National e-Authentication Framework and then e-Pramaan. Then, the working of these projects is explained, and in the next section, the proposed protocol has explained its implementation process. The performance parameters are explained along with the conclusion of the work [17]. In Section 3, related work has been discussed. The existing Indian e-governance authentication system has been discussed in Section 4. The UIAP protocol proposed to integrate the Indian e-governance system has been proposed in Section 5. Section 6 explains the process to implement the UIAP for the existing Indian e-governance system. Finally, Section 7 concludes the paper.

The Government of India expressed its interest to provide a smart card for authentication for various e-governance services. The e-governance environment is working on a multiserver architecture-based environment and using distributed computing. Many researchers presented different authentication protocols both for two-layer and for multilayer architecture-based systems. The authentication schemes for multiserver architecture are available in the literature [18–23]. It has been observed that the hash-based authentication schemes are the most efficient techniques [18, 22, 24–26]. In 2014, Hu [27] proposed a technique [19], which claims anonymity and traceability with all necessary security properties as in Li. et al.'s protocol [19]. Gaharana and Anand presented a security analysis of various multiserver authentication techniques [28]. These techniques are based on two-way and three-way factor-based authentication [29–34]. Generally, authentication schemes are dependent on a central server that stores the verification data. Because of centrally stored verification data, these schemes are vulnerable. Therefore, a new authentication scheme is required to overcome the vulnerabilities due to centrally stored verification data such as reflection attack, insider attack, and smart card loss attack, and Anand D. and Khemchandani V. proposed a technique to overcome this weakness [35, 36].

2. Motivation of This Work

The available authentication solutions are not capable of giving a unified authentication view for the e-governance services in India. Citizens need to register themselves for each service and then the services are integrated using the ADHAAR number which is a unique identification number for citizen which is centralized. Therefore, there is a requirement for an authentication technique that can give a unified view to the authentication process to access e-governance services at geographically distributed servers and departments. Along with this unified view, there is also a

requirement for this authentication process that it should not depend on any centralized storage and should be able to store the related information at distributed storage.

The novel authentication mechanism is the requirement of the time for the Indian e-governance system and this is the motivation for this work. Motivated by this, the paper proposes a robust and efficient user authentication scheme. The major contributions of this paper are smart card-based authentication scheme for a multiserver environment with the following selected features:

Secure: all the major security threats and goals are tested

Light-weighted: distributed parameters are used in place of centralized storage

Single sign-on: single registration may work for all the departments as per the existing e-governance architecture

Efficient: light-weighted and secure protocol which is capable of handling big amount of requests for a huge population through existing resources

3. Related Work

Various authentication schemes have been proposed to handle the security threats specifically for e-governance projects. Roy and Karforma proposed a secure and smart system for e-governance which is using ECDSA (Elliptic Curve Digital Signature Algorithm) based on UML [79]. In this technique, they proposed the e-governance system model dependent on Multipurpose Electronic Card (MEC). In other work, Roy et al. proposed another approach in which ECDSA was replaced with the RSA approach for object-oriented modeling of RSA digital signature. Mutual authentication is the basic security requirement that needs to incorporate in the e-governance system as in 2006. Liao et al. proposed a mutual authentication scheme. Yoon and Yoo [38] analyzed the scheme of Liao et al. and proved that it is unable to resist playback threats and offline password guessing. Other techniques have been proposed by Ku and Chen [39] and Yoon et al. [40]. Wang et al. [41] analyzed these schemes in 2007 and found the security threats such as forgery and DoS threats. To overcome these threats, Wang et al. proposed another scheme with all the security functionalities available in Ku and Chen [39] and Yoon found during the analysis such as insider attack, reflection attack, and parallel session attack [42–44].

Chung et al. [45] analyzed the scheme of Wang et al. [41] in 2009 and observed that the scheme is unable to resist impersonation and password guessing attack. The further author proposed a technique providing security services such as offline password guessing attack, impersonation attack, insider attack, the stolen smart card attack, and the modification of account-database attack. Additionally, the scheme was able to achieve the perfect forward secrecy [46, 47]. Xu et al. [47] analyzed the Lee et al. [46] and Lee and Chiu [48] schemes and proved that these techniques are not able to resist forgery attack. Then, Xu et al. [47] promulgated an improvised scheme to remove security weakness. Song [49] proposed a better scheme in which the drawback of the scheme of Xu et al. [47] has been improvised to overcome the existing impersonation attack. Chen et al. [50] analyzed the scheme of Wang et al. [41]. It has been observed Wang's technique is not able to resist the security attacks such as parallel sessions and forgery attacks. Further, Chen et al. proposed a better technique. Chen et al. [50] analyzed the techniques of Sood et al. [51] and Song [49] in 2012. According to Chen et al. [50], the improvements recommended by Song [49] and Sood et al. [51] are very sensitive to many known attacks. In this method, Chen et al. recognized security defects in the enhanced smart card-based password authentication and key agreement schemes of Sood et al. [51] and Song [49]. The technique of Sood et al. does not support an important security requirement of mutual authentication, and Song's technique was susceptible to offline guessing attacks and stolen card and thus enhanced the technique of Chen et al., which eradicated these security weaknesses, and the technique achieved mutual authentication, withstands various attacks, and is efficient. He also exposed that the technique of Sood et al. [51] has two drawbacks. Firstly, the technique is in a one-way authentication mechanism as the server verifies the authenticity of the entity and has no reciprocal mechanism of authentication. The second is erroneous input detection. Chen et al. [50] also determined the offline password guessing attack concerning Song's scheme, which led to the lack of security. Additionally, Chen et al. [50] presented an authentication mechanism to overcome the security flaws. In 2013, Li et al. [52] found that Chen et al. failed to satisfy forward secrecy and proposed an improved scheme. Jiang et al. [30] analyzed the scheme of Chen et al. [50] and found that the scheme is insecure to password guessing attack.

4. Authentication System for Indian e-Governance System

The journey towards authentication system for the Indian e-governance system started in 1970 with the establishment of the Department of Electronics since then many milestones have been achieved. In 1977, NIC was established. In the year 2006, the government launched NeGP (National e-Governance Plan), a guideline for all types of governments under the federal structure to implement e-governance.

4.1. National e-Authentication Framework. This project has an objective to develop an online service delivery mechanism to authenticate the user's identity electronically to prove their legitimacy to access each government service securely. Therefore, the Department of Information Technology, Government of India, has proposed the National e-Authentication Framework (NeAF).

The objective of NeAF is to provide a guiding framework to all central ministries, state departments, and other government agencies for the implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy. The overall objective is to

provide a trusted electronic environment where the users can transact easily and securely with the government. The framework first defines the principles of e-Authentication along with its various components such as Identity Management, Authentication, Authorization, Credential Registration, Permission Assignment, Deregistration, and Single Sign-on. The framework then defines a layered approach towards e-Authentication along with a six-step methodology to determine the business and assurance requirements of government applications, the user registration process, the implementation model, and the assessment of the chosen authentication model. It is also recommending the procedure to define the sensitivity level of the respective application for National Service Delivery Gateway (NSDG), State Service Delivery Gateway (SSDG), and Mobile Service Delivery Gateway (MSDG). Further, the framework is followed by the technical architecture of "e-Authentication" as well as the roles and responsibilities of stakeholders towards acceptance and execution of this framework [5, 53–55].

Implementation of the authentication is depended on the available technologies, mechanisms, and interfaces. These are incorporated in NeAF as illustrated in Figure 1. The following sections are describing these components.

4.2. Authentication Protocols. The organizations build Information and Communication Technology- (ICT-) based systems to provide quality services to their end-users. Several interconnected servers are required for the efficient and effective use of these services. The user legitimacy test is very important for ICT-enabled services. Different authentication protocols to test are adopted by the various departments for their projects. For authentication, identification is important because, ultimately, the identity of the user will be proved in the authentication [37, 56].

The proposed protocols and methods identified in NeAF are as follows:

(1) Biometric: biometric authentication is simply the process of verifying the user's identity using measurements or other unique characteristics of his/her body and then logging in to the system, an app, a device, and so on [57]. For these body measurements (such as iris, fingerprints, palm design, face detection, and voice), specific hardware is used to extract the features and match them with already recorded features [58, 59].

This technique has some disadvantages as follows:

Unable to update or change because biometrics is last a lifetime
"Master fingerprints" can trick many phones and scanners
Vulnerabilities in biometric authentication software
Creating a fake identification such as finger (spoofing the fingerprint)
Hacking the biometric sensor and stealing the data

(2) QnA: in this mechanism, the user can either set their own set of questions and answers during the QnA creation stage, or the application can choose to ask predefined questions to the user. It can be used as a secondary, second factor of two-factor authentication or in the password change process. It cannot be used as a primary authentication process because the vulnerability is very high and the probability to break it is also very high [60, 61].

(3) OATH: this mechanism is the initiative of industrial collaboration and combined efforts to develop a strong and secure authentication scheme that is open to use. It uses open standards to endorse the implementation of strong authentication [62, 63]. The objective of this scheme is to make the authentication process independent from the vendor or development platform. In this way, the development cost of the product will decrease and the use of the product will become simple [64]. There are various levels of the OATH standard. For the basic level, OATH is using the following credentials for authentication:

One-time password- (OTP-) based authentication
Public key infrastructure- (PKI-) based authentication (using X.509.v3 certificate)
Subscriber identity module- (SIM-) based authentication (using GSM/GPRS SIM)

However, OATH is very useful, but some disadvantages are also identified as phishing, centralized, anonymity issue, etc.

(4) OTP authentication: automatically generated, an alphanumeric, fixed-length string of characters used to authenticate the legitimacy of the user for a single transaction or a specific session is called a one-time password (OTP). OTP is more secure in comparison with the static or user-created password due to its randomness and single-time use. The OTPs may use as authentication login information, but generally, it is used as a second-factor authentication credential for the multifactor authentication mechanism [65, 66].

(5) Kerberos, X.509 certificates: the X.509 is a type of digital certificate that uses a widely accepted public key infrastructure (PKI) standard for the verification of the identity of the user/computer/service claimed at the remote location. The X.509 certificate was firstly issued as a part of the International Telecommunications Union's Telecommunication Standardization Sector (ITU-T) and X.500 Directory Services Standard in 1988. Later, it has been identified that it is not secure against attacks and also requires a huge hierarchy. The maintenance of Kerberos is also costly as it required maintaining various lists and status of the certificates such as Certificate Revocation List (OCR) and Online Certificate Status through Online Certificate Status Protocol (OCSP) [67].

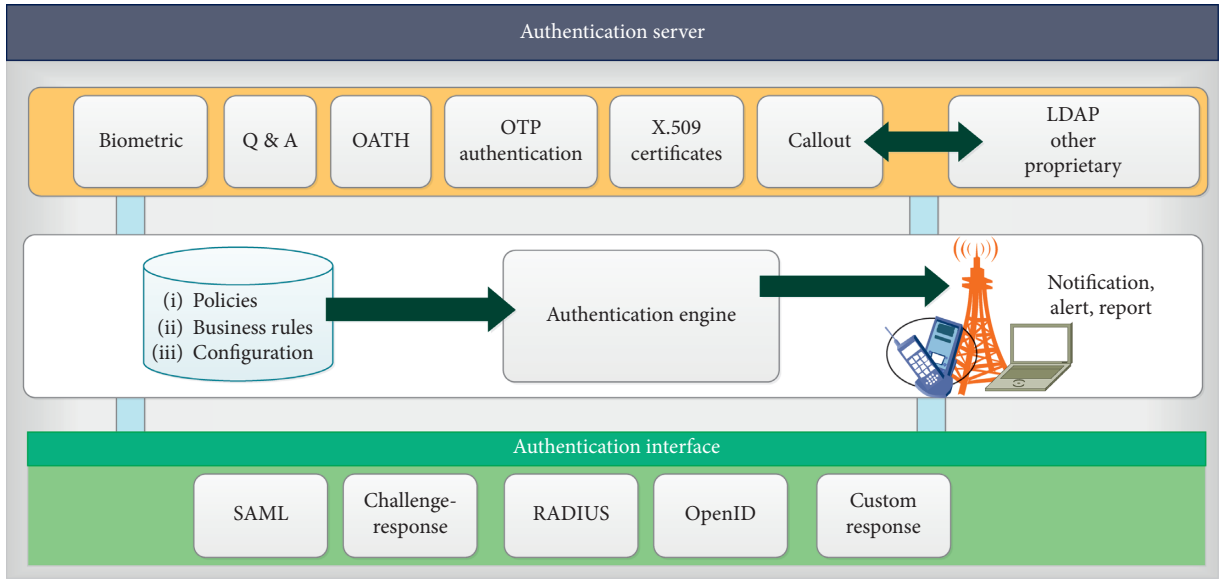

Figure 1: Block diagram for NeAF system.

(6) The Lightweight Directory Access Protocol (LDAP): the protocol was developed for directory services in which distributed lists of information are systematized into a tree of directory information, which are stored within an LDAP database. If the user wants to access the information from an LDAP database, then he/she has to prove his/her identity. In this way, it is quite consuming. The problem with LDAP and its type of solution is the integration of the active directory at the cloud [68]. Additionally, the support for Mac and Linux platforms can be extremely burdensome. Due to these problems, drawbacks, challenges, and cons, there is a serious need for innovation within the directory realm [69, 70].

4.3. Authentication Interface. An authentication interface is one of the most core interfaces to provide a platform for the user to connect with the security framework. NeAF has announced the following authentication interfaces.

4.3.1. Security Assertion Markup Language (SAML). Current software and services are working on the distributed environment in which there is a need to pass on the identification credentials from one node to another node. In this regard, SAML is very useful to open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). The major benefit of the SAML is that a set of credentials is sufficient to access various websites/services as one site pass on the credentials to another node.

4.3.2. Challenge-Response. Two friends are only the persons known the secrets of each other. The same concept is applied for challenge-response authentication. It is an interface for authentication where one entity provides a challenge (a secrete question, etc.) and at the other end, the second entity provides the corresponding response to complete the authentication process successfully. If a second entity fails to provide a valid response, then the authentication process fails with fail status and denies the second entity to access services, computer, network, or another network resource at the first entity [71].

4.3.3. Remote Authentication Dial-In User Service (RADIUS). This protocol is developed for the Network Access Servers (NAS) which requires authenticating its links and a shared authentication server along with authorization, and configuration. Therefore, this protocol is working as AAA protocol, i.e., authentication and authorization protocol for specific applications such as Network Access or IP Mobility. To authenticate the user, this protocol uses Password Authentication Protocol (PAP), Extensible Authentication Protocol (EAP), or Challenge Handshake Authentication Protocol (CHAP) and accesses text file, Database, and LDAP servers for authentication [1]. The authentication credentials are accessed from the above-said storage entities, and after completion of the authentication process, the credentials are returned back to the respective NAS [72].

4.3.4. OpenID. Nowadays, every user is required to access various services available on the Internet using a computer or using mobile. It is very tough to manage the authentication credentials for all the services as all the services are deployed on different platforms and the authentication of each service is different. Therefore, it is a requirement to sign in at one website and access any service without creating new passwords. This objective is achieved by the OpenID which allows the user to use an existing account to sign in to multiple websites. For OpenID authentication, the associate information with OpenID is passing to the other websites like name or email address. This information can be controlled and configured for the amount which can be shared

with other websites. The password or authentication credentials are taking care of by the primary website which is responsible to prove the legitimacy of the user and confirm the authentication of the user and the rest websites are not able to access these authentication credentials. Hence, a user does not need to worry about an unscrupulous or insecure website compromising your identity.

4.4. e-Pramaan. It is a framework standard for authentication of the users and also provides security for various government services on the Internet or mobile platform. It is based on the National e-Authentication framework. The e-Pramaan authentication framework is providing the exclusive unified login service for national and state-level e-governance applications. The services of e-Pramaan are implanted through SAML 2.0-based single sign-on (SSO) and provide multifactor authentication using various authentication parameters such as OTP, password, biometrics, and a digital certificate. e-Pramaan is also providing chaining of user's authentication through various government legitimate verification methods such as Aadhaar-based user identity verification and PAN-based identity verification. The details and analysis of the e-Pramaan have been provided in the next section [5].

The e-Pramaan has been proposed in 2012 and deployed in India in 2015. It is implemented on the web for the citizens. The citizen has to get registered for this service. After successful registration and authentication, the user can access the services through the given links.

4.4.1. Workflow of e-Pramaan. The workflow of e-Pramaan is shown in Figure 2. To access selected e-governance services, the Government of India provides a platform through a web portal, i.e., https://epramaan.gov.in. Before accessing any authorized e-governance service, the user needs to get registered on this site. This registration process requires the user's Aadhaar information. Figure 2 illustrates the e-Pramaan workflow which requires registration followed by the login process. After successful login, the e-Pramaan website redirects the users to the specific departmental server.

4.4.2. Information Flow of e-Pramaan. The information flow is illustrated in Figure 3. The process is started with two options, either the user is already registered or he/she is a new user to register. If the user is already registered, then he/she is redirected to the login page and provides authentication credentials. These credentials are used for the purposes of authentication at the central repository. If the user's legitimacy is proved through the mentioned process, then the system redirects the request to a user's specific page. User can then access the e-governance services for which he/she is authorized. Once, the work is completed he/she can log out from the system.

However, in the case of registration, the user has three options as follows:

(i) Registration using base number/voter ID

(ii) Registration using driving license

(iii) Registration without identity verification

The registration process is successful once the information provided by the user is verified. After registration, the user can log in and access the desired services.

4.4.3. Sequence Flow of e-Pramaan. To understand the sequence of intercommunication of various processes/servers of the e-Pramaan, a sequence diagram is illustrated in Figure 3. The e-Pramaan layer is intermediate between user and department's services, i.e., e-governance services. To access the information, a user requests for authentication to the e-Pramaan layer. Based on the user's credentials, the authentication process verifies the user's legitimacy through the stored information. If the user proves its legitimacy, then the e-Pramaan website redirects the request to the requested server.

The flow of information of the e-Pramaan is illustrated in Figure 4. This flow diagram explained the flow of information for "already registered user" and also for "new user".

4.4.4. Analysis of NeAF and e-Pramaan. To make the system better, it is necessary to analyze the existing authentic system of India. The observations are as follows:

(i) There is a centralized data store for authentication credentials.

(ii) The whole authentication process depends on the single and centralized authentication credentials.

(iii) The e-governance services are individually accessed through their authentication system.

(iv) The registration process for each e-governance service is existing along with e-Pramaan registration. User is to get registered for each e-governance service individually.

(v) The multiple registrations for the services of a single organization (i.e., the registration process for various e-governance services) are a redundant process. These repetitions of the same process make citizens uncomfortable. The same results were highlighted by us in other works where government officials are also agreed on it [4, 5, 53, 73].

(vi) Through e-Pramaan, all the suitable e-governance services are made available at a single window. But it is not the integration of all the services as claimed. It infers that there are two ways to access the system, either to access a particular e-governance service directly from the department's server or through the e-Pramaan. It means there are two authentication processes for the same service, and therefore, redundant data have to be stored for authentication of a citizen for a service.

The unified and integrated authentication system means all the e-governance services are accessible only through a single authentication system. Whether users may access through the portal of service or from the platform

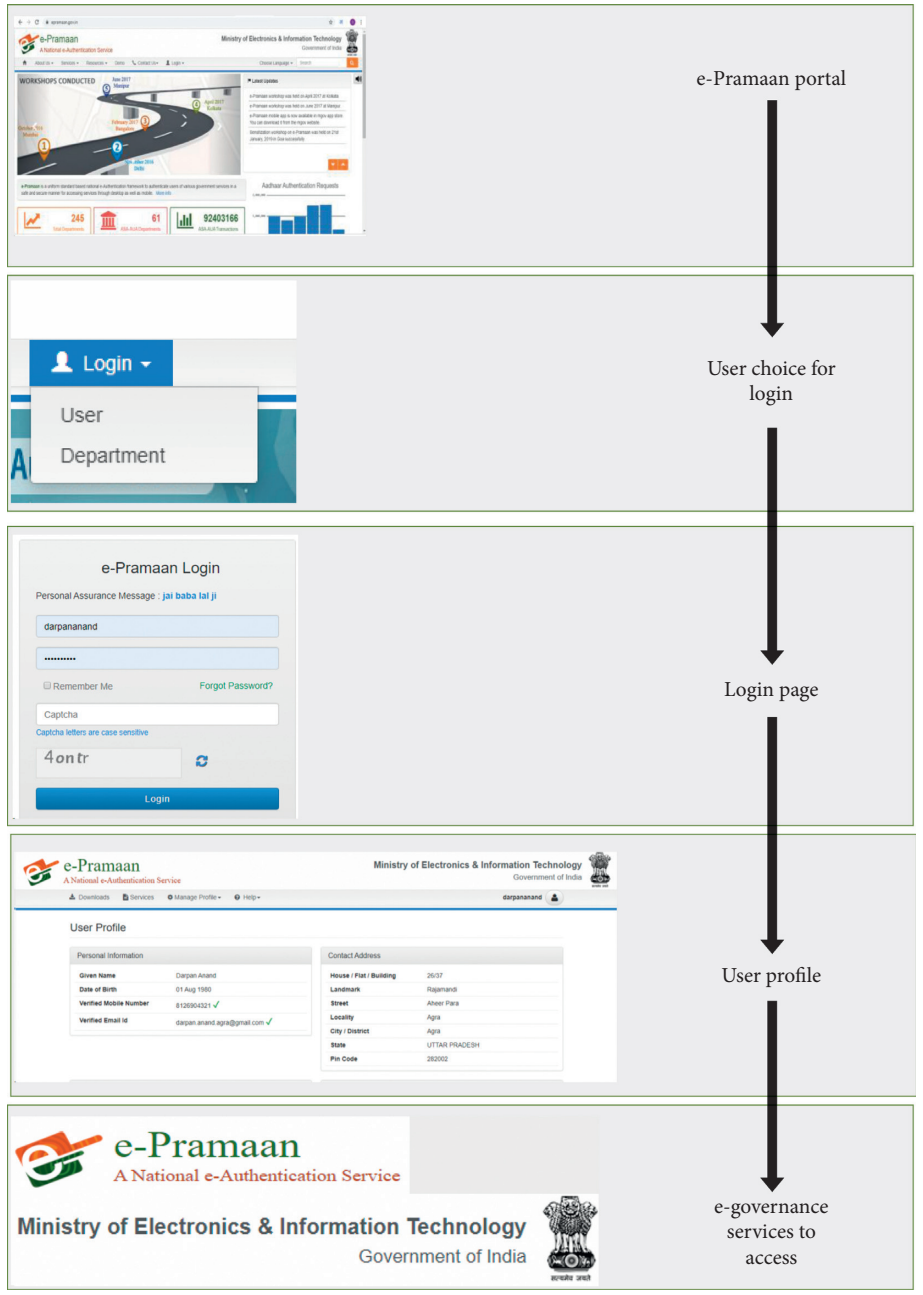

Figure 2: e-Pramaan live working flow.

government provides to access their services (as in the case of e-Pramaan). To make the system more secure and safe, the authentication should not be dependent on the central authentication store; therefore, the process should be distributed and not storing data on the central data store [35]. To solve these issues, Anand and Khemchandani propose a UIAP which is explained in the next section.

5. Unified Integrated Authentication Protocol (UIAP)

This section explains the proposed Unified and Integrated Authentication Protocol (UIAP), which is developed not only for authentication on multiserver architecture but also provides the facility of secrecy for communication among various involved servers and layers. Because of this, the protocol can integrate the existing isolated system in a unified manner. In UIAP, once a user gets registered for any service, he/she can be authenticated to access a particular service provided by a server other than the server on which registration has been done. If the user wants to access the services from service-providing server (other than service providing server, where a user got registered), the session key will be shared between all the involved servers including service providing server where users got registered. In this way, the data required for registration are stored at the service providing server and central authentication server in a distributed manner during the registration process. This

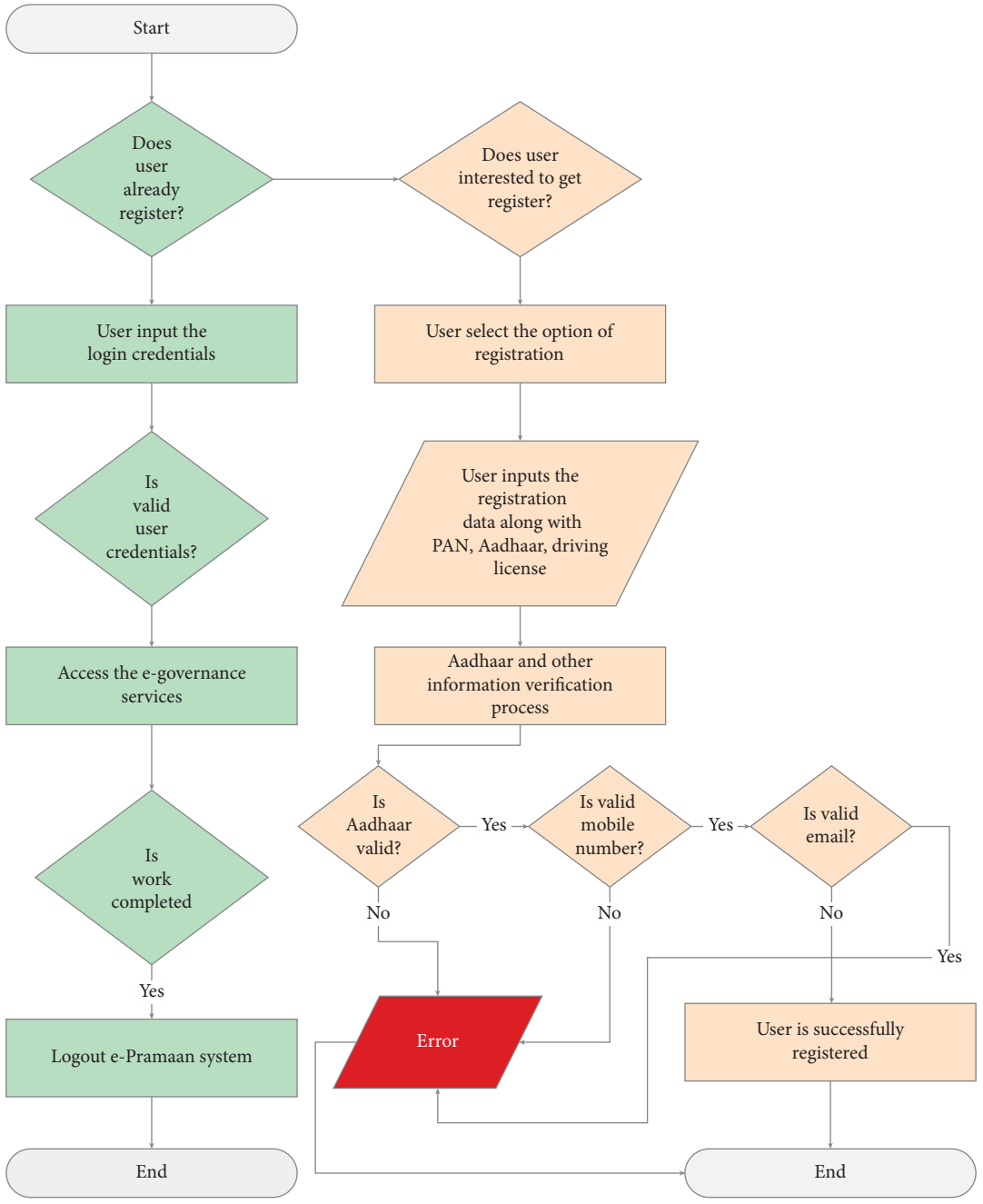

Figure 3: Process flow for e-Pramaan.

proposed protocol contains three kinds of layers for the authentication process as a Common Service Center (CSC), the Department Service Providing Server (DS)/Department Service Used for Registration Server (DSO), and the Central Authentication Server (CAS).

U_i is ith user from a set of users U, $h(.)$ is expressing a hash function, E is expressing the ciphering/encryption algorithm, k is denoting the concatenation (bitwise), $\oplus$ is expressing XOR operation for bit values, UID_i is users U_i identity, $r1$, $r2$, and $r3$ are denoting the random numbers at CSC, DSO, and CAS, respectively, key1 is symmetric key for encryption between CSC and DSO, key2 is symmetric key for encryption between DSO and CAS, ID_{DSO} is used to express the ID of DSO, ID_{DS} is used to express the ID of DS, TS_1, TS_2, and TS_3 and N_1, N_2, and N_3 are denoting the timestamps and nuances generated at CSC, DS, and CAS, respectively, PIN is used to encrypt the data read from smart card for further processing, $\Delta\text{TS}_{\text{DSTV}}$, $\Delta\text{TS}_{\text{CASTV}}$, and $\Delta\text{TS}_{\text{DSOTV}}$ are acceptable time duration between the timestamp values generated at DS with TS_1, CAS with TS_1, and DSO with TS_1, respectively, and SessKey is the final session key deduced at each layer which is used for communication after authentication.

The detailed working of the UIAP is illustrated in Figure 5. The responsibilities of each layer are as follows. This section explains the proposed Unified and Integrated

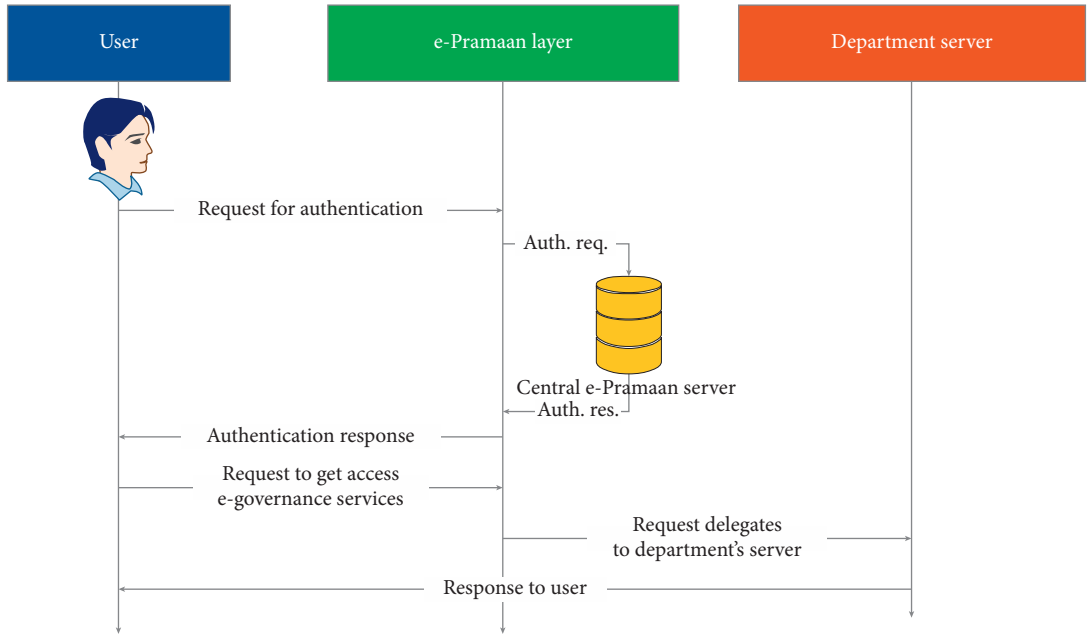

Figure 4: Sequence diagram of e-Pramaan.

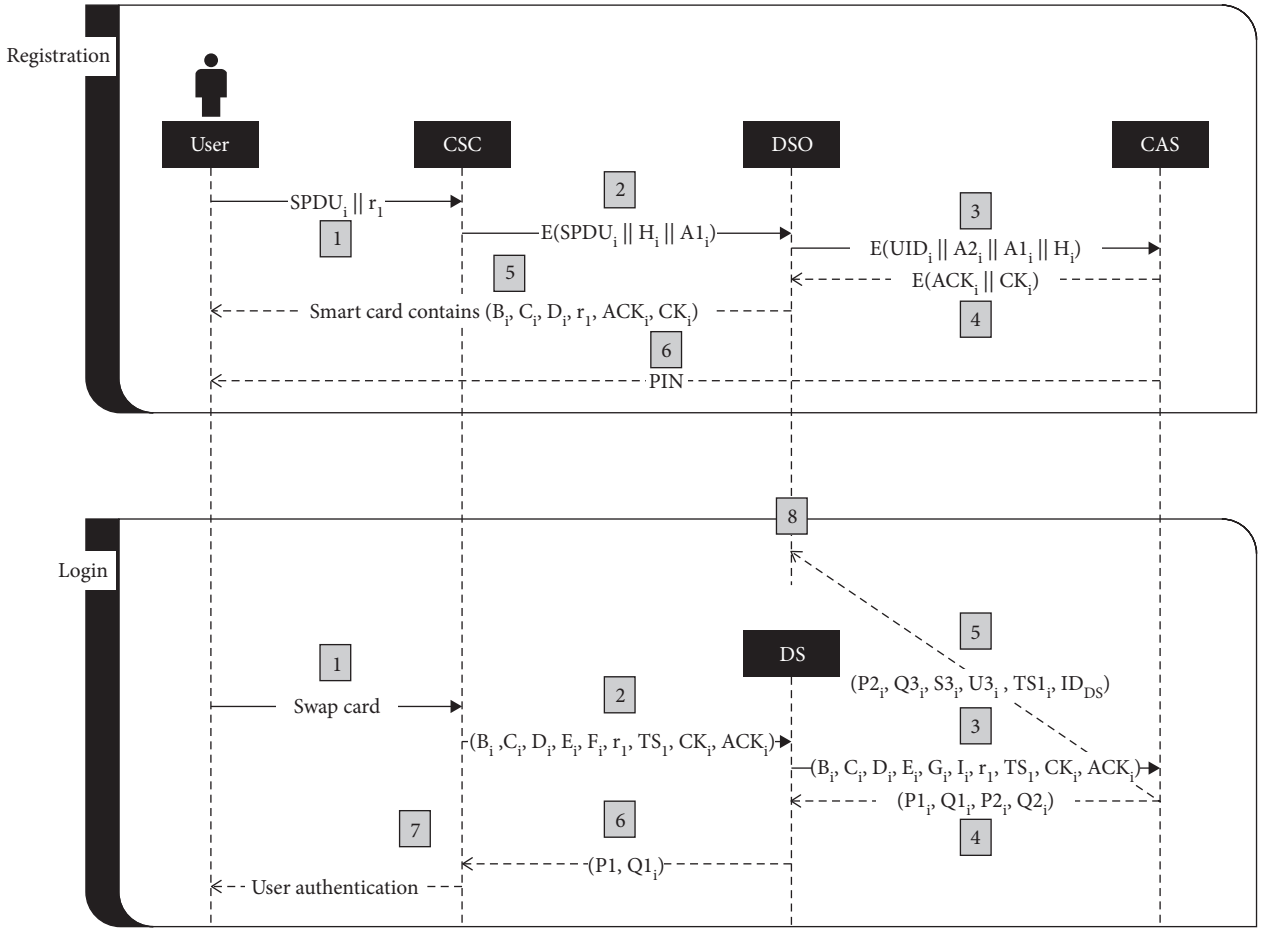

Figure 5: Communication phases of UIAP.

Authentication Protocol (UIAP), which is developed not only for authentication on multiserver architecture but also provides the facility of secrecy for communication among various involved servers and layers. Because of this, the protocol can integrate the existing isolated system in a unified manner. In UIAP, once a user gets registered for any service, he/she can be authenticated to access a particular service provided by a server other than the server on which registration has been done. If the user wants to access the services from service providing server (other than service providing server, where a user got registered), the session key will be shared between all the involved servers including service providing server where users got registered. In this way, the data required for registration are stored at the service providing server and central authentication server in a distributed manner during the registration process. This proposed protocol contains three kinds of layers for the authentication process as a Common Service Center (CSC), the Department Service Providing Server (DS)/Department Service Used for Registration Server (DSO), and the Central Authentication Server (CAS). The detailed working of the UIAP is illustrated in Figure 5. The responsibilities of each layer are as follows:

(1) Common Service Center (CSC): the user interacts with the whole system through this layer. Generally, organizations installed various ICT kiosks, i.e., CSC to access the services. These kiosks will be enabled with all the required resources such as computer systems, Internet, scanner, power backup, and installed nearby the residences of remote users. These centers are useful for remote residents and also for busy persons who are unable to reach the office physically for any service. The registration can be done only from a legitimate CSC or from any legitimate office of the organization. The request for login goes from the CSC layer. CSC layer validates the registration, standardizes and formats the information, and then forwards to the next layer for further processing.

(2) Department Service Providing Server (DS): there are various departments to handle a specific type of service. These services (such as road transportation office, passport office, banks, and income tax office in case of e-governance) are only accessible by the legitimate and registered users. This layer is the set of servers, which are collectivity called as Department Service Providing Layer or DS. This layer is responsible to provide the services after validating the legitimacy of the users through CSC.

(3) Department Service Used for Registration Server (DSO): this type of servers is the members of the set of DS layer, but the primary responsibility of it is to register user and store the registration data. The stored data will be used for authentication to prove the legitimacy of the user by passing messages among CSC, DS, and CAS. This layer is also responsible to serve the users by providing services as by the DS layer.

(4) Central Authentication Server (CAS): this layer has a responsibility to authenticate the users. At the time of login, this layer will identify the user's DSO server where detailed information is stored at the time of registration. Therefore, there is no need to store the whole data on a central server or central cloud.

There are three processes to implement UIAP for authentication:

(i) Initialization and registration phase: this phase is responsible to register the citizens who approach to access any e-governance service. In this phase, various parameters are shared between the various communication entities and some of them are stored on these layers for the further authentication process in a distributed manner.

(ii) Login phase: this main process is used to prove the legitimacy of the genuine user. If the user is unable to prove its legitimacy, then the user cannot allow accessing the system.

(iii) Authentication and key agreement phase: after successful login, through the same parameters which are shared in the login phase, a session key is deduced and used for secure communication.

6. Lightweight Technical Implementation of UIAP

There are several existing projects which are running on various servers to provide various services to citizens. For these services and servers, citizens have registered for individual services at a specific server. To implement the UIAP, the following components of the system are required:

(i) UIAP implementation architecture: this is a framework that comprised of the relationships and interactions between application components, such as middleware systems, user interfaces, and databases.

(ii) Data structure: How do we represent, organize, manage, and store the information that enables efficient access and modification for UIAP communication.

(iii) Communication services: there are various standardized ways or media to propagate communication between the various layers engaged in UIAP.

(iv) Integration with other e-governance services: the most challenging task to integrate the existing services with UIAP.

6.1. UIAP Implementation Architecture. The average Internet user gets to see a specific page on his/her system, through a series of interactions between various components of

applications, user interfaces, middleware systems, databases, servers, and the browser. The framework which ties up this relation and interaction together is the project implementation architecture. The project implementation architecture for UIAP is illustrated in Figure 6.

The user can access the e-governance services through three mediums as follows:

Government kiosks (Common Service Center): under the NeGP, the government began a venture CSC to encourage the citizens for e-governance by a stand adjacent to his/her home in farther regions of anywhere in the region of the country [74]. The CSC guidelines conceive a wide variety of substances and services that could be offered as training and education, health, insurance, banking (rural and urban), entertainment, agriculture, business, skill development, etc.

Web applications (HTTP-based application for laptop, desktop, or smartphone): the Government of India initiated the facility to access the various e-government services through web portals. As technology grows, the services are also provided for smartphones through Android or iOS apps. These services are responsive and based on web application architecture [75, 76]. This is also very useful as a major population is using smartphones and the Internet. Therefore, it is very much mandatory to facilitate citizens with an open platform to access e-governance services.

Through existing infrastructure like bank ATMs: there is a big challenge to deploy CSC to provide the reach to the citizens to access the e-governance services. To make it available to the citizens, apart from CSC and web application platforms, the bank ATMs can be another option. There are about 2.2 million ATMs including 15,626 WLAs working in India to serve the citizens and it is expected to 4 million in the next couple of years. The primary objective of these machines is related to money, basic bank operations, etc. Some of the ATMs are also working for income tax filing and other government-related tasks. The working of these ATMs can be extended to serve various existing e-governance services. This idea, to provide e-governance to all the citizens through exiting the ATM network, is useful to enhance the reach [77, 78].

6.2. UIAP Data Format. To exchange data among different servers involved during the authentication process, the lightweight data-interchange format JavaScript Object Notation (JSON) can be used to reduce communication overhead. It can be considered as of the best solutions to represent the data because the JSON objects are an open-standard file format that uses human-readable text to transmit data objects consisting of attribute-value pairs and array data types or any other sterilizable value. It is a very common data format, with a diverse range of applications. So, it is useful to integrate the existing e-governance services, whether they are working on any platform and technology [79, 80].

6.3. UIAP Deployment. Scalability is important for keys (used for authentication and establishment of keys) and services. To scale the authentication service for a billion people, there are two general technical options:

(i) Multiple servers with proper integration and synchronization

(ii) Cloud-based e-governance services can be implemented

The first option is not considered efficient as it is required to develop and deploy multiple services for an effective and efficient outcome like load balancing, security, backup services, and integration synchronization. The second option is suitable to deploy the proposed authentication service for e-governance services. The Government of India deployed its cloud platform for various e-governance services, i.e., MeghRaj (https://cloud.gov.in/). This cloud service is open for all e-governance services. The security concern can be addressed by efficiently implementing the following services:

(i) PaaS (Platform as a Service)
(ii) IaaS (Infrastructure as a Service)
(iii) SaaS (Software as a Service)
(iv) Storage (Storage as a Service)
(v) Load Balancer (Load Balancer as a Service)
(vi) Antivirus (Antivirus Service)
(vii) IP (Public IP Service)
(viii) RM (Resource Monitoring as a Service)
(ix) VA (Vulnerability Assessment Service)
(x) WAF (Web Application Firewall (WAF) Service)
(xi) Backup (Backup Service)
(xii) APM (Application Performance Management)
(xiii) DA (Data Analytics (DA) as a Service)

Many of these services are already deployed on the MeghRaj platform. The NIC National Cloud (MeghRaj) is presently hosting several critical applications on over 16,000 virtual servers supporting 480+ e-governance projects and 900+ user departments under Digital India. Therefore, MeghRaj is the prominent, efficient, secure, and effective option to deploy the proposed authentication service UIAP.

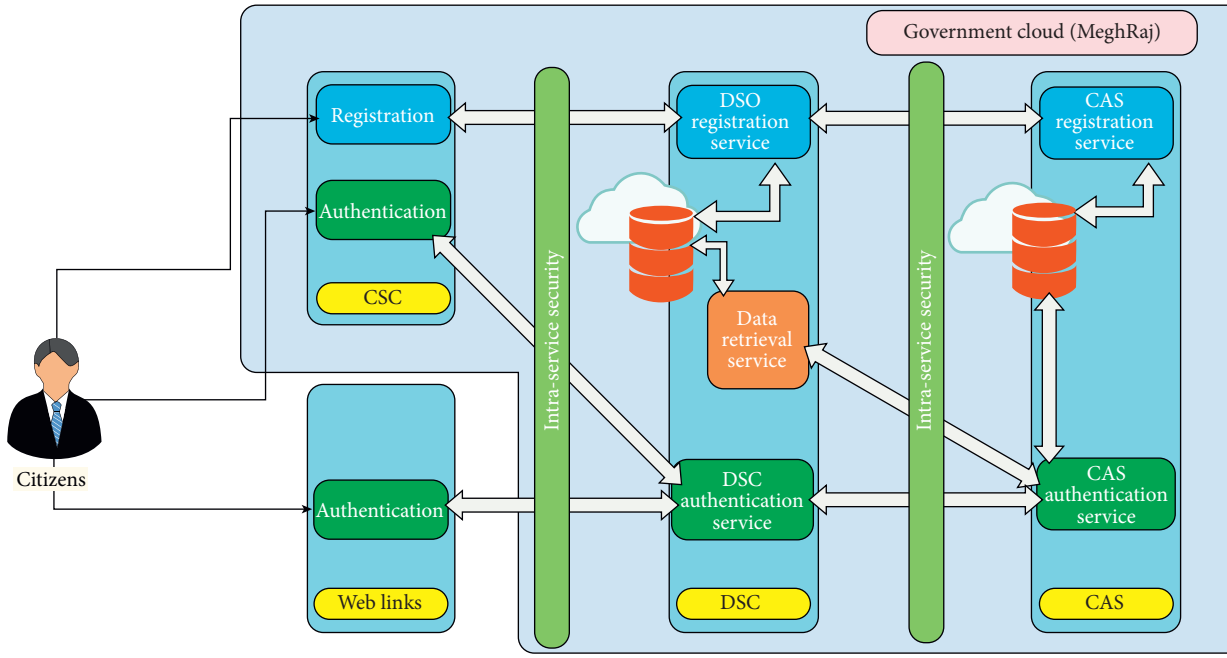

Figure 6: Proposed implementation architecture for UIAP.

7. Conclusion

The authentication process is very crucial and important for the highly scalable system providing multiple services through different servers. The same will apply to the e-governance system. The Government of India is also taken it seriously e-governance services, and therefore, NeAF and e-Pramaan projects are proposed. e-Pramaan just redirects the user to a specific departmental server to access the corresponding server after authentication. In this setup, the user has to authenticate himself/herself separately to access a specific service. Therefore, to access any service (which is not read-only), he/she has to execute two authentication processes with separate credentials. To provide a single authentication service to access all services, we propose the lightweight technical implementation of single sign-on authentication and key agreement mechanism based on UIAP. This paper also explains the implementation of the authentication mechanism using lightweight SOAP services deployed over a cloud-based platform. Further, the work will be extended to make the technique able for authorization of the e-governance services.

Data Availability

The data used to support the findings of the manuscript are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Dr. Omar Cheikhrouhou thanks Taif University for its support under the project Taif University Researchers supporting project number TURSP-2020/55, Taif University, Taif, Saudi Arabia.

References

[1] O. Cheikhrouhou, M. Laurent, A. B. Abdallah, and M. B. Jemaa, "An EAP-EHash authentication method adapted to resource constrained terminals," *Annals of Telecommunications - Annales des Télécommunications*, vol. 65, no. 5-6, pp. 271–284, 2010.

[2] M. Sabharwal, "The assessment of concerns, opinions and perceptions of Customers to find the significant metrics for deployment of Biometrics in E-banking," *International Journal of Computer Applications (IJCA)*, vol. 138, no. 14, pp. 28–41, 2016.

[3] M. Sabharwal, "Multi-modal biometric authentication and secure transaction operation framework for E-banking," *International Journal of Business Data Communications and Networking*, vol. 13, no. 1, pp. 102–116, 2017.

[4] D. Anand and V. Khemchandani, "An analytical method to audit indian e-governance system," *International Journal of Electronic Government Research*, vol. 13, no. 3, pp. 18–37, 2017.

[5] D. Anand and V. Khemchandani, "Study of e-governance in India: a survey," *International Journal of Electronic Security and Digital Forensics*, vol. 11, no. 2, pp. 119–144, 2019.

[6] S. Lauriks, A. Reinersmann, H. G. Van der Roest et al., "of ict-based services for identified unmet needs in people with dementia," *Ageing Research Reviews*, vol. 6, no. 3, pp. 223–246.

[7] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.

[8] B. Gupta, M. Tiwari, and S. Singh Lamba, "Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.

[9] R. Heeks, "Understanding e-governance for development," *I-Government Working Paper Series*, vol. 11, 2001.
[10] N. Yadav and V. Singh, "E-governance: past, present and future in India," 2013, https://arxiv.org/abs/1308.3323.
[11] L. Kant and S. K. Krishnan, "Information and communication technology in disease surveillance, India: a case study," *BMC Public Health*, vol. 10, no. 1, p. S11, 2010.
[12] S. Bhatnagar, "Information technology and development: foundation and key issues," 2000.
[13] R. Chauhan, *National E-Governance Plan in india*, United Nations University–International Institute for Software Technology, Macau, China, 2009.
[14] D. G. Chandra and R. S. Bhadoria, "Cloud computing model for national e-governance plan (negp)," in *Proceedings of the International Conference on Computational Intelligence and Communication Networks*, pp. 520–524, Mathura, Uttar Pradesh, India, November 2012.
[15] D. Mathur, P. Gupta, and A. Sridevi, "e-governance approach in India the national e-governance plan (negp)," *Transforming Government*, vol. 3, 2009.
[16] H. Goswami, "Opportunities and challenges of digital India programme," *International Education and Research Journal*, vol. 2, no. 11, pp. 78-79, 2016.
[17] A. Dubey, Z. Saquib, and S. Dwivedi, "Electronic authentication for egovernment services-a survey," in *Proceedings of the 10th IET System Safety and Cyber-Security Conference*, IET, Bristol, UK, October 2015.
[18] T. Hwang, Y. Chen, and C. J. Laih, "Non-interactive password authentications without password tables," in *Proceedings of theIEEE TENCON'90: 1990 IEEE Region 10 Conference on Computer and Communication Systems*, pp. 429–431, Hong Kong, China, June 1990.
[19] C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-I. Fan, "A secure dynamic identity based authentication protocol with smart cards for multi-server architecture," *Journal of Information Science and Engineering*, vol. 31, no. 6, pp. 1975–1992, 2015.
[20] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, "A novel smart card and dynamic id based remote user authentication] scheme for multiserver environments," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 85–5, 2013.
[21] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.
[22] Y.-P. Liao and S.-S. Wang, "A secure dynamic id based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.
[23] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609–618, 2011.
[24] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.
[25] C.-C. Nugent, T.-H. Lin, and R.-X. Chang, "A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13863–13870, 2011.
[26] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key greement using smart cards," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 2, pp. 793–800, 2009.
[27] W. Hu, K. Xue, P. Hong, and C. Wu, "Atcs: a novel anonymous and traceable communication scheme for vehicular ad hoc networks," *IJ Network Security*, vol. 13, no. 2, pp. 71–78, 2011.
[28] S. Gaharana and D. Anand, "Dynamic id based remote user authentication in multi server environment using smart cards: a review," in *Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks*, pp. 1081–1084, Jabalpur, India, December 2015.
[29] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390–1397, 2010.
[30] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383–393, 2015.
[31] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: a comparative evaluation of two-factor Authentication schemes," in *Proceedings of the 11th ACM on Asia Conference on Computerand Communications Security*, New York, NY, USA, September 2016.
[32] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2014.
[33] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity," *Information Sciences*, vol. 321, pp. 162–178, 2015.
[34] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Networks*, vol. 20, pp. 1–15, 2014.
[35] D. Anand and V. Khemchandani, "Unified and integrated authentication and key agreement scheme for e-governance system without verification table," *Sadhana*, vol. 44, no. 9, p. 192, 2019b.
[36] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.
[37] A. Roy and S. Karforma, "Authentication of user in e-governance: a digital certificate based approach," *International Journal of Scientific Research and Management (IJSRM)*, vol. 2, no. 8, pp. 1212–1221, 2014.
[38] E.-J. Yoon and K.-Y. Yoo, "Drawbacks of liao et al's password authentication scheme," in *Proceedings of the International Conference on Next Generation Web Services Practices*, pp. 101–108, Seoul, South Korea, June 2006.
[39] W.-C. Ku and S.-M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204–207, 2004.
[40] E.-J. Yoon, E.-K. Ryu, and K.-Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 612–614, 2004.
[41] X.-M. Wang, W.-F. Zhang, J.-S. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 29, no. 5, pp. 507–512, 2007.
[42] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "CyberSecurity attack prediction: a deep learning

approach," in *Proceedings of the 13th International Conference on Security of Information and Networks*, pp. 1–6, Merkez, Turkey, November 2020.

[43] I. Jemal, O. Cheikhrouhou, H. Hamam, and A. Mahfoudhi, "Sql injection attack detection and prevention techniques using machine learning," *International Journal of Applied Engineering Research*, vol. 15, pp. 569–580, 2020a.

[44] I. Jemal, M. A. Haddar, O. Cheikhrouhou, and A. Mahfoudhi, "ASCII embedding: an efficient deep learning method for web attacks detection," *Pattern Recognition and Artificial Intelligence*, vol. 1322, pp. 286–297, 2021.

[45] H.-R. Chung, W.-C. Ku, and M.-J. Tsaur, "Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 863–868, 2009.

[46] S.-W. Lee, H.-S. Kim, and K.-Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 27, no. 2, pp. 181–183, 2005.

[47] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[48] N.-Y. Lee and Y.-C. Chiu, "Improved remote authentication scheme with smart card," *Computer Standards & Interfaces*, vol. 27, no. 2, pp. 177–180, 2005.

[49] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, vol. 32, no. 5-6, pp. 321–325, 2010.

[50] T.-H. Chen, H.-C. Hsiang, and W.-K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," *Future Generation Computer Systems*, vol. 27, no. 4, pp. 377–380, 2011.

[51] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of wang et al. sauthentication scheme using smart cards," in *Proceedings of the 2010 National Cnference on Communications (NCC)*, Mumbai, India, May 2010.

[52] X. Li, J. Niu, M. Khurram Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[53] D. Anand and V. Khemchandani, "The challenges for authentication in indian e-governance system (a survey on indian administrative staff)," *International Journal of Control Theory and Applications*, vol. 40, no. 9, pp. 335–346, 2016.

[54] A. Jøsang, K. A. Varmedal, C. Rosenberger, and R. Kumar, "Service provider authentication assurance," in *Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust*, pp. 203–210, Paris, France, July 2012.

[55] M. Kumar and K. S. Vaisla, "Comparative study of e- Authentication framework for e-governance," in *Proceedings of the International Conference on Advances in Computing and Communication*, pp. 140–147, Mumbai, India, January 2014.

[56] V. Jain, R. Kumar, and Z. Saquib, "An approach towards digital signaturesfor e-governance in India," in *Proceedings of the 2015 2nd international Conference on Electronic Governance and Open Society: Challenges in Eurasia*, pp. 82–88, St. Petersburg, Russia, July 2015.

[57] T. Wiens, "Engine speed reduction for hydraulic machinery using predictive algorithms," *International Journal of Hydromechatronics*, vol. 2, no. 1, pp. 16–31, 2019.

[58] A. K. Jain and K. Nandakumar, "Biometric authentication: system security and user privacy," *Computer*, vol. 45, no. 11, pp. 87–92, 2012.

[59] R. K. Rowe, U. Uludag, M. Demirkus, S. Parthasaradhi, and A. K. Jain, "A multispectral whole-hand biometric authentication system," in *Proceedings of the 2007 Biometrics Symposium*, Baltimore, Maryland, September 2007.

[60] B. Bazelli, A. Hindle, and E. Stroulia, "On the personality traits of stackoverflow users," in *Proceedings of the 2013 IEEE.International Conference on Software Maintenance*, pp. 460–463, Eindhoven, Netherlands, September 2013.

[61] M. Yousuf and K. Khan, "A novel cost effective authentication framework for wireless lans in small medium enterprises (smes)," in *Proceedings of the 2011 IEEE 3rd International Conference on Communication Sofware and Networks*, pp. 158–162, Xi'an, China, August 2011.

[62] S. Osterland and J. Weber, "Analytical analysis of single-stage pressure relief valves," *International Journal of Hydromechatronics*, vol. 2, no. 1, pp. 32–53, 2019.

[63] W. Jerbi, A. Guermazi, O. Cheikhrouhou, and H. Trabelsi, "CoopECC: a collaborative cryptographic mechanism for the internet of things," *Journal of Sensors*, vol. 2021, Article ID 8878513, 8 pages, 2021.

[64] R. Wang, H. Yu, G. Wang, G. Zhang, and W. Wang, "Study on the dynamic and static characteristics of gas static thrust bearing with micro-hole restrictors," *International Journal of Hydromechatronics*, vol. 2, no. 3, pp. 189–202, 2019.

[65] Z. Sui, Y. Fang, M. Li, and L.-c. Liu, "Design improvement and implementation of authentication technology based on," *Information and Electronic Engineering*, vol. 4, 2005.

[66] Y. Xijun, W. Gouxin, X. Yong, and S. Kun, "Realization and improvement of otp authentication," *Computer Engineering*, vol. 9, 2000.

[67] M. A. Sirbu and J.-I. Chuang, "Distributed authentication in kerberos using public key cryptography," in *Proceedings of SNDSS'97: Internet Society 1997 Symposium on Network and Distributed System Security*, pp. 134–141, San Diego, CA, USA, March 1997.

[68] R. Chaari, O. Cheikhrouhou, A. Koubâa, H. Youssef, and H. Hmam, "Towards a distributed computation offloading architecture for cloud robotics," in *Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 434–441, IEEE, Tangier, Morocco, June 2019.

[69] T. Howes and M. Smith, "LDAP," in *Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*, M. S. Tim Howes, Ed., Macmillan Technical Publishing, New York, NY, USA, 1997.

[70] W. Yeong, T. Howes, and S. Kille, "Lightweight directory access protocol," *Network Working Group - Request for Comments*, vol. 1, p. 1777, 1995.

[71] M. Boujelben, O. Cheikhrouhou, M. Abid, and H. Youssef, "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks," in *Proceedings of the 2009 Third International Conference on Sensor Technologies and Applications*, pp. 442–448, IEEE, Bejing, China, June 2009.

[72] O. Cheikhrouhou, A. Koubaa, M. Boujelben, and M. Abid, "A lightweight user authentication scheme for wireless sensor networks," in *Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010*, pp. 1–7, IEEE, Hammamet, Tunisia, May 2010a.

[73] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.

[74] K. Datta and A. Saxena, "Developing entrepreneurship and e-government in India: role of common service centers," *Journal of E-Governance*, vol. 36, no. 2, pp. 92–100, 2013.

[75] O. B. Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam, and A. Derhab, "An OWASP top ten driven survey on web application protection methods," in *Risks and Security of Internet and Systems*, J. Garcia-Alfaro, J. Leneutre, N. Cuppens, and R. Yaich, Eds., Springer International Publishing, Cham, Switzerland, pp. 235–252, 2021.

[76] I. Jemal, M. A. Haddar, O. Cheikhrouhou, and A. Mahfoudhi, "M-CNN: a new hybrid deep learning model for web security," in *Proceedings of the 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–7, IEEE, Antalya, Turkey, November 2020b.

[77] O. Cheikhrouhou, A. Koubâa, G. Dini, and M. Abid, "RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 15, no. 8, pp. 783–797, 2011.

[78] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "PetroBlock: a blockchain-based payment mechanism for fueling smart vehicles," *Applied Sciences*, vol. 11, no. 7, p. 3055, 2021.

[79] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "UTM-chain: blockchain-based secure unmanned traffic management for internet of drones," *Sensors*, vol. 21, no. 9, p. 3049, 2021.

[80] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "BMC-SDN: blockchain-based multi-controller architecture for secure software-defined networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9984666, 12 pages, 2021.