International Journal of Mathematics, Statistics, and Computer Science
Vol. 2, 2024
ISSN: 2704-1077 eISSN 2704-1069, DOI: 10.59543/ijmscs.v2i.9073

Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks

Ali Darch Abed Dawar*
Department of Animation, School of Sciences, Gujarat University, India; aliderch88@gmail.com

Received 09.01.2024, Revised 26.02.2024, Accepted 01.03.2024, Published 09.03.2024

ABSTRACT: The communication network would have potential uses dependent on the infrastructure once the fifth generation (5G) network is fully commercialized. Subscriber Identification Module (SIM) authentication is a well-known mechanism for safeguarding the confidentiality of wireless device users. Fifth-generation computer technologies are very advanced in certification based on geolocation, regular confirmation, and authentication mechanisms. The clonable authentication feature solves the issue of authentication using duplicate modules. In highly dynamic environments, the problem poses a risk to privacy protection, adaptiveness, self-organization, information leakage, and the reliability of services. The article introduces a 2-way identity authentication method (2WIAM) using a Physical Unclonable Function (PUF) to address the issue above. The suggested technique for detecting module clones depends on user-provided authentication and geolocation data. The 2-way mutual authentication used in the suggested technique is a clever way to combine the many wireless technologies accessible to a given network node and enable the creation of wireless on-demand service providers and networks. The initial stage involves immediate passcode authentication, and the second is verifying the identity of the mobile equipment and any shifts or copies in its physical position. A new-cross authentication is then carried out to determine the identity of the clone's physical counterpart. In prior authentication situations, the choice to provide authorization or ban the clone was made fairly and objectively. The experiment results show that the users' privacy is protected, enhanced adaptiveness and the amount of data lost is limited.

Keywords: 5G, Decision-Making, Location-Tracking, PUF, SIM Authentication.

1. INTRODUCTION

Satellite and fifth-generation (5G) networks are integrated to improve wireless and mobile communication. Telecommunication, navigation, and earth imaging satellite networks are integrated into satellite communication networks to provide multimedia connectivity, identifier and weather information services, network positioning, and internet connectivity to mobile users [1]. 5G technology features provide ultra-fast internet access for smart homes, cities, and villages. 5G technology modifies defense applications, space technology, sea-to-space communication, mind-to-mind communication; 5G can control natural calamities, etc. [2, 3] The performance of information transmission is enhanced by 5G. The 5G service classes are ubiquity Mobility Ultra-Broadband (uMUB), ultraHigh-Speed Low-Latency Connectivity (uHSLLC), and ultraHigh-Data-Density (uDD). THz communication, visible light communication, modular communication, blockchain for decentralized security, quantum communication, intelligent and flexible materials, management, and energy harvesting are the encouraging features of 5G [4, 5].

Mobile communication requirements are not satisfied due to limited resources, the original design objective. The main issue of mobile communication is an integrated heterogeneous network. Authentication and roaming are the main problems in a heterogeneous network [6,7]. The RIM (removable identity module) is the SIM card used in mobile devices that support the Global System Of Mobile communication (GSM) and General Packet Radio Services (GPRS) [8,9]. The user authentication, identification, and encryption of messages are stored in SIM as the description-related information. International Mobile Subscriber Identity (IMSI) provides a separate identity for users to find the country network and to find the subscriber within a particular network by MNC (Mobile Network Code) and MSIN (Mobile Subscriber Identification Number) [10,11]. Random numbers, Signed responses, and a Cipher key are the main components of the authentication. Subscriber authentication is done by a separate authentication key provided for users. The general authentication technique is phone-based passcodes. In the authentication procedure, IETF (Internet Engineering Task Force) is used for generating the passcodes, exchanging, and verifying the passcodes by phone-based passcodes [12,13].

Key exposure attacks are prevented by Physical Unclonable Function (PUF). It combines the present cryptographic anthropophagus efficiently and securely. Electric signal delay is used in PUF to alter small variations on-chip during the manufacturing process [14]. Secret keys are covered by the normal mechanism itself PUF does not require any specific mechanism. Device authentication, key generation, and DRM use PUF. For on-chip authentication and identification, PUF with CMOS is used. For PUF authentication, Fuzzy extractors are implemented, and error-corrected data are created, commonly called Helper data [15]. The PUF

and fuzzy extractor generate the key, which is used for authentication. Based on arbitrary string encryption and decryption, the PUF authentication mechanisms are implemented. The PUF-based RFID authentication protocol (MMY) reinforces secret key leakage in NVM (non-volatile memory) and ensures security across key leakage [16]. The RFID authentication protocol is created for the unpredictability of PUF based on secure public-key encryption [17,18].

The main contributions of the articles include:

- The paper offers a 2-Way Identity Authentication Approach (2WIAM) employing a Physical Unclonable Function (PUF) to handle the authentication issue using duplicate modules, which threatens privacy, adaptiveness, self-organization, information leakage, and service dependability.
- The PUF and fuzzy extractor generate the authentication key. The authentication procedures of PUF are based on encrypting and decrypting arbitrary strings.
- Experimental results show that the suggested technique improves upon state-of-the-art solutions regarding authentication success rates, data loss, adaptability, and processing speed.

In the following fashion, the article continues: In section 2, we analyze the existing literature. Section 3 discusses the methodology and data sources used by the 2-Way Identity Authentication Methodology (2WIAM). In Section 4, you will see the results and discussions of your experiments. The recommendations for further research and conclusion are presented in Section 5.

2. RELATED WORKS

Through heterogeneous information bound with USIM cards, Yang et al. [19] achieved M2M (Machine-to-Machine) device authentication. Enhancing the initial authentication through pairing the IMEI (International mobile equipment identification number), device code, IMSI (International mobile subscriber identification number), and hardware modifications are the IMEI-IMSI and ClockSkew-IMSI methods.

In a mobile environment, the evaluation of multifactor authentication (MFA) is done by Krac and Simic [20] through an approach for identifying and fixing problems with the Universal Authentication Framework (UAF). Proposed models are evaluated against previous work regarding user priorities and SUAPCPS (security, usefulness, availability, price intricacy, privacy, and comfort). MFA solutions for users and identifying spots for developers are improved. FES (Fuzzy Expert System) tool is used to develop the fishbone model.

Jaing et al. [21] proposed an efficient authentication protocol for mobile internet users with anonymity and key protection. Based on SDH, a zero-knowledge protocol is used to achieve anonymity. The proposed model is secure for qs–mSDH and linear assumption in the random oracle model. The proposed model is efficient and achieves stronger anonymity compared with other schemes. The proposed work is suitable for real-time applications.

In [22], privacy and ease of use of a novel smartphone authentication process are offered. The subscriber identity module and open ID connects describe the proposed method. User perspective and security viewpoint are used for evaluating the proposed authentication method based on the questionnaire method. Compared with a static password and SMS one-time password (OTP) and risk, the result is analyzed and reduced by security analysis.

In keystroke dynamics authentication, Chang et al. [23] designed new soft biometrics for a limited resource. The proposed work consists of both data mining and statistical prediction. The proposed classifier considers the outlier's problem and measures the difference between the clustering distributions. The accuracy is improved for free text authentication in case of a limited resource.

Zhang et al. [24] suggested T2FA: Translucent Two-Factor Authentication. PUF (physical unclonable function) and specific performance are the foundation of T2FA. The second method verifies the user's mobile device, while the third uses the user's voice print to identify the user's mobile device and access the interface in an exact location. The proposed work provides high satisfaction and security. Transparency of the authentication eliminates fraud.

In an Edge computing environment, a PUF-based anonymous authentication scheme is recommended by Long et al. [25] for hardware devices and IPs. This scheme avoids modeling and replaying attacks in the PUF circuit to improve security and reduce complexity. Extracted fingerprints are used to trace the trusted device vendor and infringement behavior.

The behavioral model of text input is considered by Galkov et al. [26] in the authentication of mobile devices. The user model is built by keystroke pressure and key hold time. A user-adapting algorithm is used to construct a feature vector of a freely typed text. Following standardization, values are used to seek and correct the outliers. The pro Galkov et al. [26] consider the behavioral model of text input blem of classification is solved by potential function-based fuzzy search. The resulting software proves the efficiency of the proposed model.

User silicon entangled mobile identity authentication is used by Dee et al. [27]. Sensors in the mobile device touchscreen detect a human biometric for tracing the shape and silicon foundry process. An authentication

mechanism based on robust user device biometric is designed to achieve gesture accuracy in complex geometric gestures. User profiles exhibit PUF properties for reducing gesture hamming distance.

In [28], identity authentication method based on trajectory (TIAM) characteristics, mobile devices are introduced. TIAM has a registration phase to create template trajectories, stay point, and authentication phase for calculating the trajectories data and authenticate it and detect the stay points. Data are updated to the library with authenticated new sample trajectories and accommodate in a changed user route. Tests are carried out to demonstrate the adaptability and precision of the planned work.

Parne et al. [29] proposed ESAP- efficient and secure authentication protocol in mobile communication networks for roaming users. BAN logic verify the proposed method. AVISPA tool analyzes the possible attacks on the communication network and provides security. A fluid flow mobility model based on performance analysis is used to reduce overhead and congestions and compare existing protocols.

In mobile equipment, Abazi et al. [30] described applying the biometric models of authentication. The proposed method is used to increase phone access security. The biometric modules used for sharing the process and authentication are explained. Potential attacks are detected, and the problem in mobile devices is overcome.

Fast authentication and key agreement on commodity mobile devices are suggested by Xie et al. [31]. GeneWave achieves initial bidirectional authentication by thwarting Time uncertainty to provide accurate intervals. The initial acoustic channel response does device authentication. The efficiency, security, and increased key generation rate are obtained as constructive features of the proposed method.

Cao et al. [32] proposed a lightweight and secure access authentication (LSAA) scheme for administering security in 5G user devices and machine-type communications. This scheme exploits mutual authentication, identity-based privacy, and reliable key sharing for robust security. The proposed scheme is reliable in reducing computation and communication costs with controlled storage utilization.

3. PROPOSED METHOD

Authentication and verification are conducted, with the verification and security deployed, to ensure user privacy across all wireless mediums. The goal of the study is to enable a timely 2-way authentication procedure between the client and the service supplier. The choice is taken to either deliver the information or service to the authorized user, implement the use authorization, and prevent the clone. Here, manual and location-based authentication is performed to identify the clones in the devices. Fig. 1 illustrates the function of the proposed method.

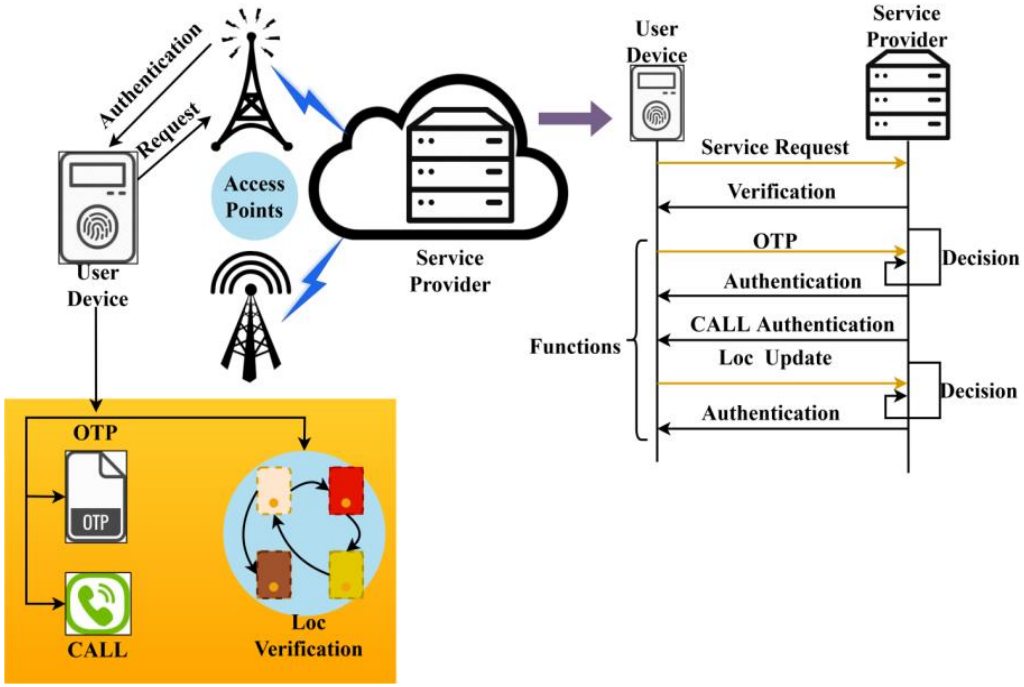

Fig. 1—Functions of the Proposed Method

The user device interacts with the service provider through the access points. The user device is verified using a one-time password (OTP), or calls or both, and location-based mobile internet protocol (MIP) matching. The service provider performs decision-making based on the above verification methods for providing security.

Manual and location-based authentication

In this work, the 2WIAM method verifies the SIM's location and manual activation and avoids information loss. It addresses user privacy and information leakage and avoids the threat in 5G computing. The 2WIAM is used along with the PIF method to overcome the mentioned issues reliably. The identification of manual authentication is carried out by equating the following equation.

$$\partial(a') = \left(\frac{1}{u_n}\right) * \prod_{\varphi}^{s'} \quad \left(v' - \frac{f_m}{\frac{e_q}{\omega}}\right) + \left[(x_0 - v') * \delta(f_m)\right] + r_d \tag{1a}$$

Manual authentication is identified in the above equation (1a). It acquires the appeal from the user that is denoted as $e_{q,}$ and the provider validates the data to guarantee authenticity. The information/ service is denoted as f_m, the user access the services are termed as u_0, whereas; the number of a user is referred to as u_n. The identification represented as ∂ are performed to raise the total amount of user requests and to supply the service.. Here, the service provider is denoted as r_d that is produced as the response to the user on time, and it is termed as v', for this periodic monitoring is done, and it is represented as ω

The manual authentication is represented as a', and the acknowledgment is sent back from the user as the one-time password $s'$to set the SIM in 5G. In this case, the acknowledgment is represented as x_0, and it is acquired on time is denoted as $[(x_0 - v') * \delta(f_m)]$ thus, the verification is carried out that is referred to as δ for every incoming appeal from the user. Here the analysis is done for the number of appeal information from the user, denoted as φ. Thus, the verification is done for the information and provides the service that decreases the data loss. The following equation evaluates the service provider's verification to set up manual authentication for the user.

$$\delta = \left(f_m + e_q\right) * s' \left[\left(\frac{\frac{x_0}{\delta}}{s'}\right) + \left(\frac{\varphi}{v' + \sigma}\right)\right] * \left[(\sigma + \pi) + \left(\frac{\varphi}{o_e}\right)\right] - v'(x_0 - r_d) \tag{1b}$$

The verification is done for the manual authentication that deploys the one-time password verification, and it is linked to the user's information and attractiveness. The acknowledgment is given to the service provider and, in turn, receives the information on time; for this processing, the verification phase is necessary. It deploys the periodic monitoring and analysis of the authentication that is termed as σ, from this verification is performed, and it is represented as $s'\left[\left(\frac{\frac{x_0}{\delta}}{s'}\right) + \left(\frac{\varphi}{v' + \sigma}\right)\right]$.

The analysis is done for the varying devices in 5G and processed with the manual authentication, which is done by designing the security model, and it is denoted as π. Thus, both authentication and security are provided to the user. This is achieved by relying on the clone of information, and it is represented as o_e. It is carried out on time; in this, the acknowledgment and service provider deploys to analyze the information and avoids information leakage. Thus, the verification phase is used in manual authentication to activate the SIM in 5G on time, and the upcoming equation is used to identify the location-based authentication.

$$\partial(l_t) = \sum_{f_m}^{\omega} \quad (x_0 - u_0) * \left(\frac{q'}{a'}\right) + \left(\delta * e_q\right) + \left(v' - g_0\left(q' + \sigma\right)\right) * r_d(v') \tag{1c}$$

The identification of location-based authentication is calculated in the above equation, and the service is delivered to the user via constant review, localization of mobile IP addresses, and identification. The mobile IP for the device is the same for varying instances, and it is denoted as q', and the manual setup is used to find the user's location termed as a'. The verification is done for the appeal that deploys the authentication. It is performed by mapping denoted as $\left(\delta * e_q\right) + \left(v' - g_0(q' + \sigma)\right)$, the location-based authentication is termed as l_t. In Fig. 2, the mapping and location-based authentication processes are illustrated.

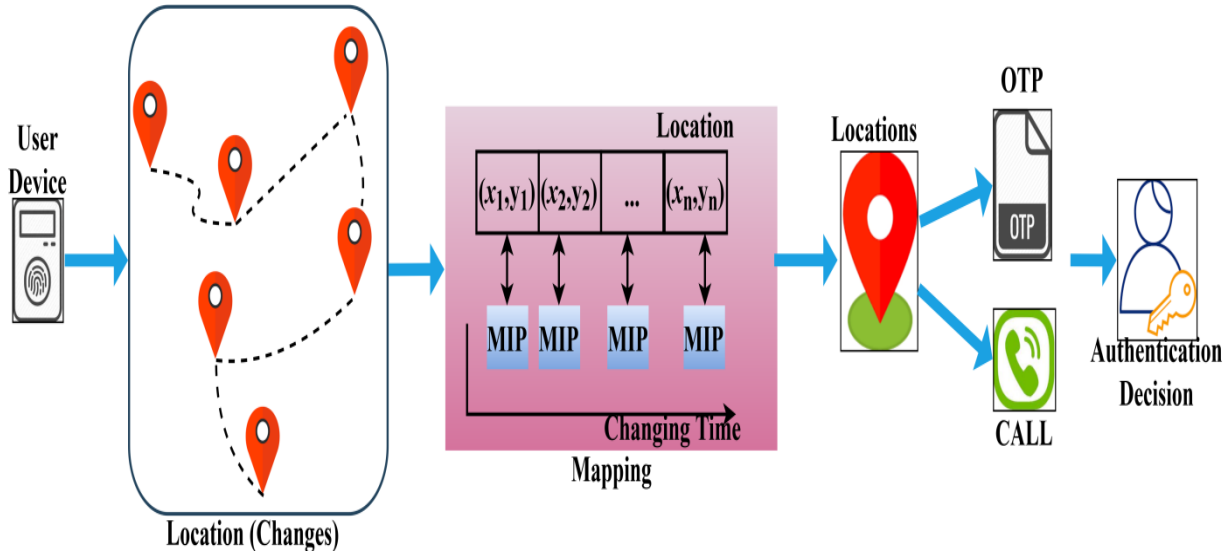

Fig. 2—Mapping and Location-based Authentication

Mobile IP addresses and authentication protocols are mapped for various use cases, and the service is delivered based on the user's preference. The mapping is referred to as g_0; it is processed to find the device's accurate location and performs the 2- step of authentication by verifying the information. In this manner, the location-based authentication is monitored by mapping mobile IP and mutual authentication in 5G and promptly forwarding the service. Thus, the identification of the location for the device is computed in the above equation (1c). The following equation is used to identify the clones from the information.

$$\partial(o_e) = \{[(f_m + \pi) + g_0(q' + \sigma)] * s' + \omega = \left(\frac{f_m + e_q}{\sum \pi}\right) * q'(s') - v'(r_d) \quad (2)$$

Identifying the clone is done by equating the above equation from the previous state of authentication and security and maps the mobile IP and authentication. The security is provided to the number of information from the mapping, and it is represented as $[(f_m + \pi) + g_0(q' + \sigma)]$ that deploys the manual and location-based authentication. Here, the periodic monitoring is performed on time associated with the varying devices to ensure security by performing authentication. The security of the appeal information is provided based on the manual and mobile IP of the device. This process is denoted as $\left(\frac{f_m + e_q}{\sum \pi}\right) * q'(s')$.

This cloning is identified by mapping the service with the preceding state of the devices' mobile IP, and mutual authentication is carried out on time. In a time- and effort-saving manner, the attractive user is given the information related to the 2-way identification, which guarantees safety. Thus, the identification is performed on time and provides the authentication on time, and it relates to finding the clone of information that leads to information loss in 5G.

Authentication for location-based service

The suggested work uses a three-way hashing algorithm with a cryptographic function to ensure privacy and authenticate users. The information is converted to a fixed length and deploys n-bits of information; here, the service distribution is allocated to the appealing user. The result is mapped with the mobile IP and authenticated, and service is provided promptly by the service provider; It employs both first and second pre-image resistance.

The pre-image resistance is used to monitor the threats in 5G computation and overcome this in the preliminary step; here, the hash function generates the hashes to the appealing user. The threats are detected by deploying the hash function, identifying the clone information, and information leakage, for this 2-step verification process is utilized. If the hashing is used, the subsequent pre-image barrier a is created for the input information f_m and it is denoted as $a(f_m)$, it is difficult to find another set of input information by consideringa(x). Let x is the unknown variable that is an appeal from the user in this

manner; the threats are detected and provides security, avoids information leakage. The 2-factor authentication is provided by the following equation, which uses the 3-way hash technique.

$$\sigma(l_t) = \left(\frac{1}{u_n}\right) * e_q + \prod_{k_g} \quad f_m(a) + \left[(r_d - v') + \left(\frac{g_0}{x_0 + q'}\right)\right] * p' + e_q(u_0) + \left[\sum_{j_s} \quad (f_m + \varphi) * \omega(v')\right] - \partial \tag{3}$$

In the above equation, the authentication for the location-based service is given from the service provider by deploying a hash function associated with the input and output. Here, the information loss and privacy of the user is addressed, and it is denoted as j_s and p' for the varying appeal of the user. This mapping is performed on the location-based service, and the service provider is responsible for the appeal of the service by deploying the hash function. This security algorithm is used to distribute the information into bits. It is then forwarded to the device, and from that, the verification is carried out reliably. Fig. 3 illustrates procedure of smart phone and network operator authentication.

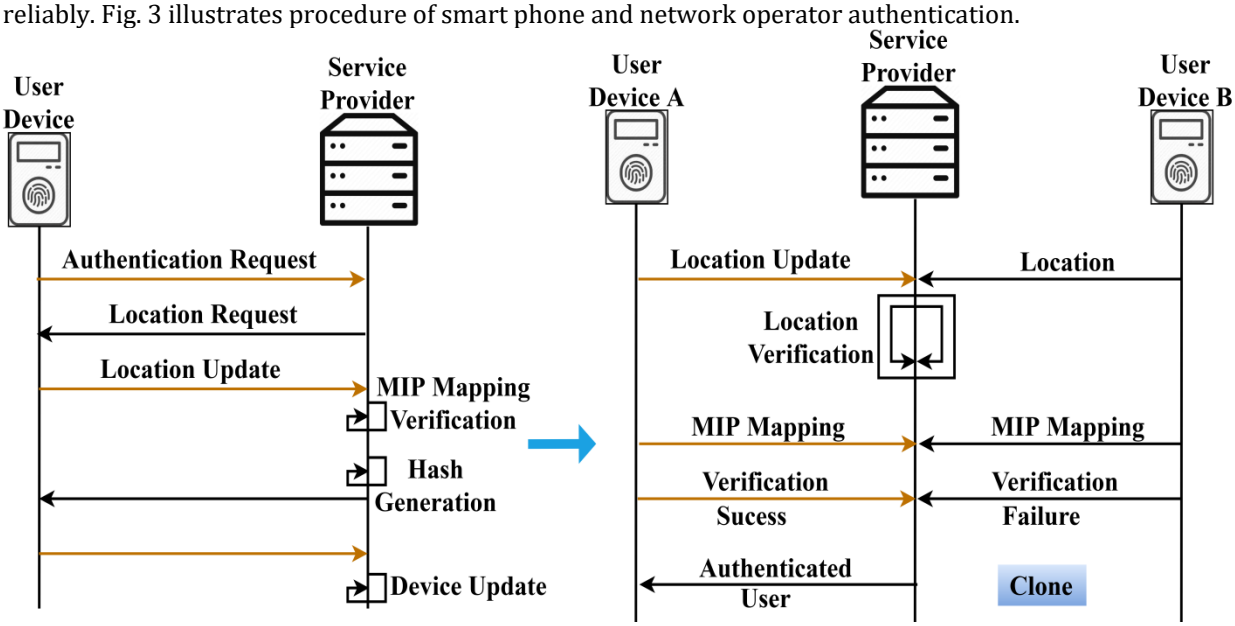

Fig. 3—Authentication Process between Mobile Device and Service Provider

In this authentication process, the MIP verification is the key factor for identifying the clones using the generated hash. The update is performed if the user device is verified through CALL or OTP or both, and location. The information loss and leakage is identified by verifying the device by tracking the location with the mobile IP, with the user location is detected by the periodic manner, and it is represented as $\left[\sum_{j_s} \quad (f_m + \varphi) * \omega(v')\right]$. In this information, leakage is identified by deploying the hash code function for the number of inputs and provides the authentication for the device to activate the SIM. Thus, the above equation is used to provide authentication to the device by performing the hash function and securely distributes the service. For addressing the information leakage and user privacy, the security model is developed.

Security model

Hash functions, which employ bits to capture information, are used by the security model, and the service is provided promptly to the user after authentication. Here, the authorised user performs an evaluation of the security framework using a cryptographic mechanism, and then transmits the results to the network operator. A hash function is then used to assess the dispersion of hash codes to the input, which speeds up the calculation time, and the service provider confirms the authentication. The attractive user is afforded heightened protection against data loss and leakage as a result of external threats. Estimating the security model that uses the hash function and generates the corrected hash value may be done with the help of the following equation.. It is represented as the information provided to the appealing user promptly by n-bits of information in an authenticated manner.

$$\pi = \sum_{\varphi}^{\sigma} \quad f_m(a' + l_t) + \left[(e_q * x_0) + \left(\frac{\delta + f_m}{\frac{g_0}{\omega}}\right)\right] * a(f_m) - r_d + \left(\left[\prod_{k_g}^{q'} \quad \left(\delta * \frac{j_s + \sigma}{u_n}\right)\right] * (o_e(\partial) - l_t + p')\right) - v' \tag{4}$$

The security model is designed in the above equation using the hash function. It is associated with the periodic monitoring, and the acknowledgment is provided on time, and it is represented as $\left[(e_q * x_0) + \left(\frac{\delta + f_m}{\frac{g_0}{\omega}}\right)\right]$. In this, the hash function is responsible for producing the fixed-length of information that relates to identifying the clone in the information for this processing PUF is used. This security model is used to map the preceding state of the information appeal with the service provider and produces the result.

In this information, leakage is addressed, and it is avoided by using a hash function provided to the inputs; here, it is referred to as information appeal. Thus, the hashing is done for the number of inputs deployed to identify the clones in the information that represents the mutual authentication process for the location-based identification. The tracking of user location is done by evaluating and providing privacy. It is associated with the verification, and it is denoted as $\left[\prod_{k_g}^{q'} \quad \left(\delta * \frac{j_s + \sigma}{u_n}\right)\right]$.

For every instance, the verification is performed to address the information leakage; in this hash function, all the inputs are coded so the upcoming information appeal cannot access the current information. In this manner, the clone is detected using the PUF method associated with 2WIAM and promptly tracks the location. Here, the location-based detection is performed in a reliable manner deployed by a 3-way hash function and provides the appeal information security.

Physical Unclonable Function

In this work, the 2WIAM method is processed to resolve the security issues and privacy for the user and efficiently track devices' location. This method is associated with the hash code that produces the fixed information length by performing 2-step verification that tracks the location. Here, the security model is used to map the information appeal, and the hash function codes the information to secure the information from the threat. If the data is appealing, the information is sent to the supplier; otherwise, it is disseminated as the n-bit of data for the authorized devices. The following equation is used to monitor the security that decreases information loss and ensures user authentication.

$$\omega(\pi) = \left(\frac{u_n}{\partial}\right) + l_t * \left[\sum_{g_0} \quad (q' + \varphi) + \left(\frac{n_0 + c'}{\delta(l_t)}\right) + \sigma\right] - \left(v' + \frac{f_m(e_q)}{a}\right) \tag{5}$$

The n-bit hash code is coupled with a time interval that is monitored periodically for the user appeal service. The analysis is done for the number of information. It is used to track the location of the device by deploying the authentication for the appealing user promptly, and here the mapping is done, and it is represented as $\sum_{g_0} \quad (q' + \varphi)$. Here, the information change and replication of information is addressed, and it is denoted as n_0 and c', it is used to provide security reliably. Fig. 4 presents the authentication method for secure monitoring of the user device.

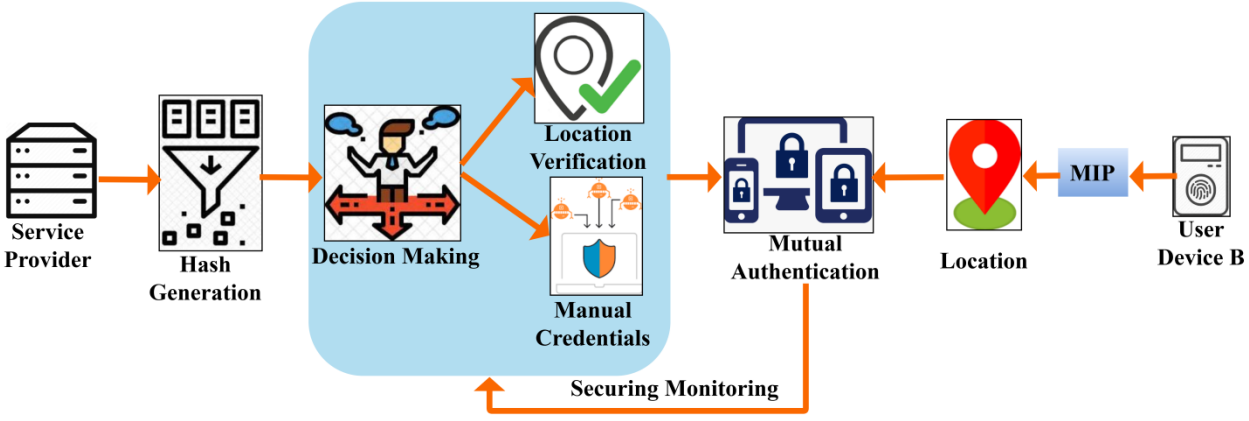

Fig. 4—Authentication for Secure Monitoring

The authentication is delivered to the user, and the service provider sends the user the decoded, hash-fixed information. The time is associated with the information, and the appeal is acknowledged by evaluating the hash function denoted as $\left(v' + \frac{f_m(e_q)}{a}\right)$. For every instance, the user's appeal varies in this manner; the location change or replication is done. For identifying the location, the PUF based 2WIAM method is developed in this proposed work. Thus, the periodic monitoring is done and resolves the information loss for the varying devices and keeps track of location in every instance.

Mutual authentication

Mutual authentication is used to detect the device's location and provides access to the user from the service provider; thus, it utilizes the hash function for security. If the device appeals for the service, the security check is carried out for every instance of time, and then it verifies the authentication. In this manner, the mutual authentication is performed to analyze the change or replication of location; it is a step-2 verification of mobile equipment. Thus, the following equation is used to analyze the change or replication of location. It is performed by using a hash function associated with the periodic monitoring and verification of location. It satisfies the mutual authentication for the change or replication of location that identifies the clone by deploying this.

$$u_h = \{(p' * \omega) + \left(\frac{u_n}{\sum q'+g_0}\right) - v' \in n_0 \left(\delta + \frac{x_0}{\varphi}\right) * \prod_{l_t} \quad (f_m + \pi) * o_e \in c' \qquad (6a)$$

The following equation is used to achieve the mutual authentication (6a), where it differentiates the change and replication of location, and it is represented as n_0 and c'. The first derivation is associated with the change of location, which utilizes the number of users to analyze the device's change, but the mobile IP relies on the same. Here, it evaluates the mobile IP and mapping that is performed on time, and it is represented as $\left(\frac{u_n}{\sum q'+g_0}\right) - v'$For every instance, the change of location is monitored. The mutual authentication is denoted as u_h. And the second derivation deploys the replication, and it determines the same mobile IP for 5G and tracks the location by utilizing the hash function. Fig. 5 presents the replication (clone) detection process.

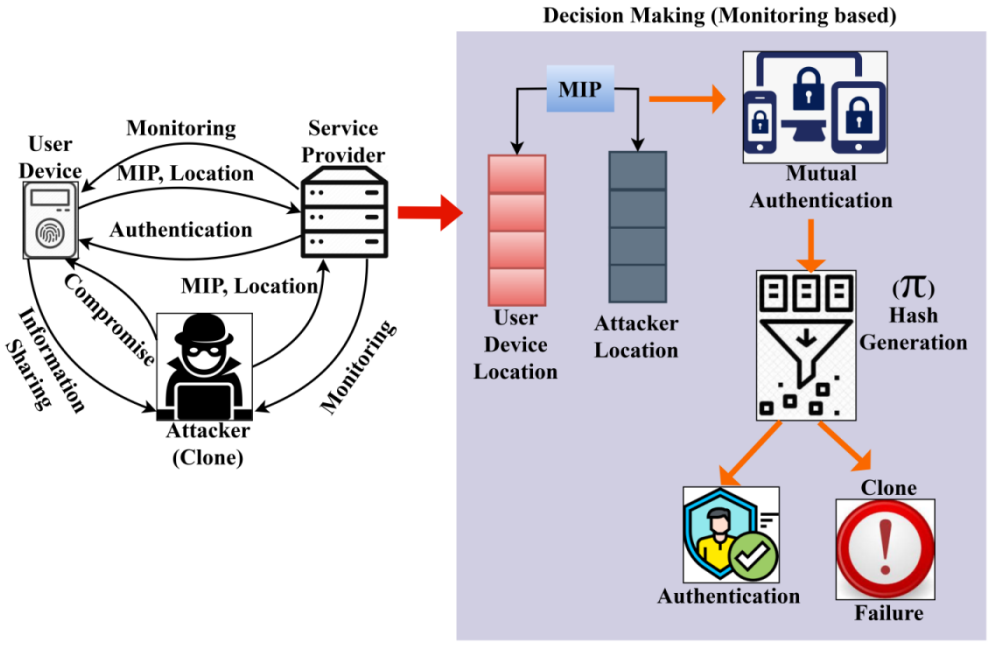

Fig. 5—Replication (Clone) Detection Process Illustration

The replication is analyzed by identifying the clone in the location and blocks them for further processing; this security method is used, and it is denoted as $\left(\delta + \frac{x_0}{\varphi}\right)$. Thus, the clone is detected in the replication stage, avoids leakage of information, and provides user privacy by using 2-way identification. This mutual authentication is done periodically and deploys the hash function to monitor the security

for the number of devices and reliably track the location. The identification of clones is necessary to analyze the replication in 5G mobile devices. For this, the following equation is computed.

$$\omega = \prod_{f_m}^{u_n} \quad (a' + l_t) * \left(\frac{g_0 + q\prime}{\sum \quad i_0 + p\prime}\right) + \left(e_q + \delta\right) * \left(\frac{\partial + f_m}{r_d}\right) * o_e(l_t - v') \tag{6b}$$

The monitoring is performed by evaluating the above equation (6b). It deploys the device's mapping with its services, which is associated with the user's appeal, and acknowledgment is provided on time. Here, it relates to both manual and location-based device tracking and identifies the clone promptly, and it is denoted as $\left(\frac{\partial + f_m}{r_d}\right) * o_e(l_t - v')$. When a clone has been identified, the service is sent on to the device that will be responsible for enforcing security measures. Thus, the clone is identified using the PUF method associated with 2WIAM and provides privacy, and addresses the information leakage. The decision is made to analyze the usage permission or block the clone in the initial stage and protect the information and privacy. It is formulated in the following equation.

$$\varphi = \left(\frac{1}{f_m(u_n)}\right) + e_q * \left(\frac{\prod \quad r_d * v\prime}{n_0 + c\prime}\right) + \gamma[i_0 + \omega(l_t) + (b_z)] \tag{7}$$

In the above equation, the decision is made to analyze the usage permission and block the clone information in the device, leading to information loss. Thus, the decision is performed for every appeal from the user and provides the information promptly. This process is associated with the change or replication process. It is used to track the device's location and provides the service provider's results by deciding on the appeal. The service is not forwarded to the device if it detects a clone or privacy issue. In this manner, it blocks the service and is given as b_z. Here, usage permission is termed as i_0, and the monitoring is done periodically, representing it as $\gamma[i_0 + \omega(l_t) + (b_z)]$. In this manner, the decision is made efficiently for the number of users. Their appeal and user privacy are done by integrating the security and decision-making process. It is derived in the below equation.

$$\pi(\partial) = \sum_{x_0}^{u_0} \quad \left(v^{'} - k_g\right) * \left(\frac{\omega}{q^{'} + u_0}\right) + \left(\gamma * \frac{\delta}{u_h}\right) + f_{\,m} - v' \tag{8}$$

The security is analyzed by equating the above equation (8), and it is denoted as $\pi(\partial)$, here it is associated with the decision-making approach that is performed on time. Here, the monitoring is done for the mobile IP to track the device's location by evaluating the 2WIAM method that relies on PUF. This verification is performed for the varying device to track the location and provides security for the number of users in the 5G environment. In this manner, mutual authentication is used to analyze the device's state and deploys the hash function to provide security reliably. Thus, the proposed objective is satisfied by introducing 2WIAM that relies on the PUF method, provides privacy for the user, blocks the clone in the device, and addresses the information loss.

4. RESULTS AND ANYLSIS

The authentication failure varies for OTP, CAL, OTP+CAL, and LOC. It is monitored periodically to address the leakage. The authentication failure for OTP+CAL decreases compared to the OTP and CAL method. It shows higher authentication failure for LOC than the other three processes (Refer to Fig. 6). The location change is done for the varying authentication failure that deploys the OTP, CAL, OTP+CAL, and LOC (Refer to Fig. 7). The authentication failures show low to wavy and lesser location change for OTP+CAL. Compared to OTP, CAL, and OTP+CAL, the LOC shows better location change and lesser authentication failure.

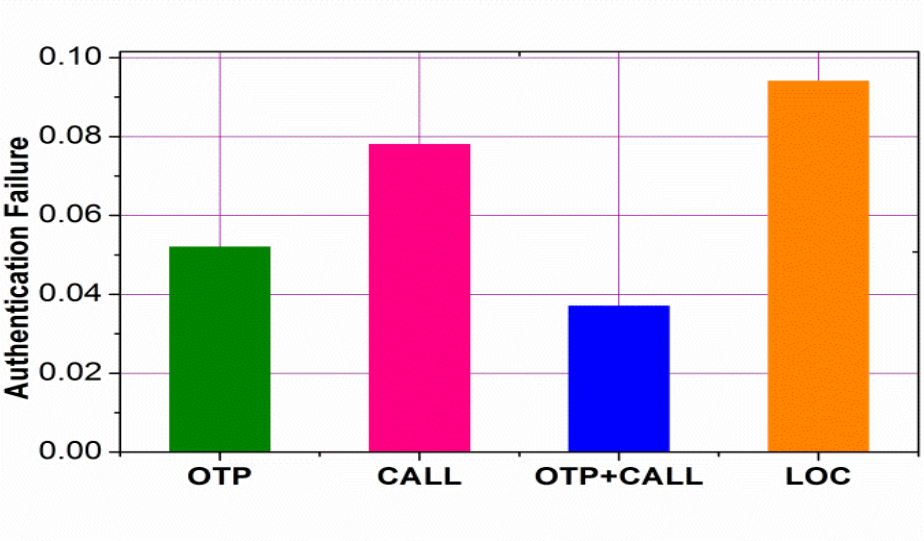

Fig. 6— Authentication Failure

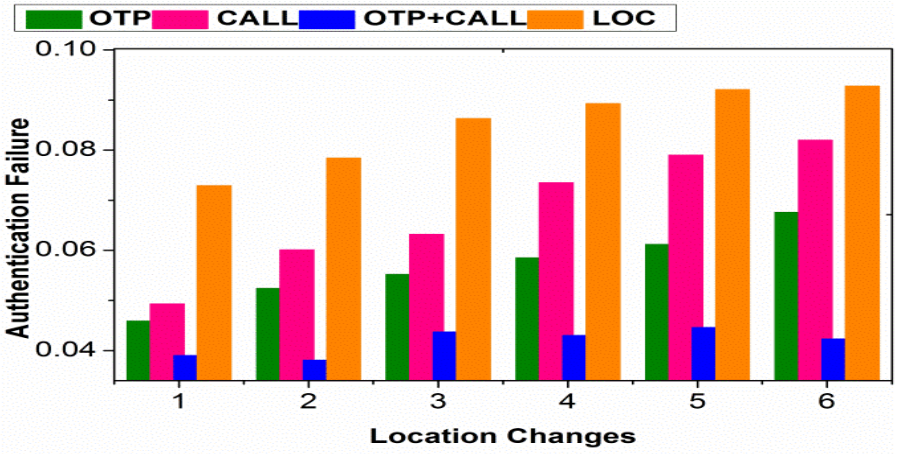

Fig.7—Location Changes

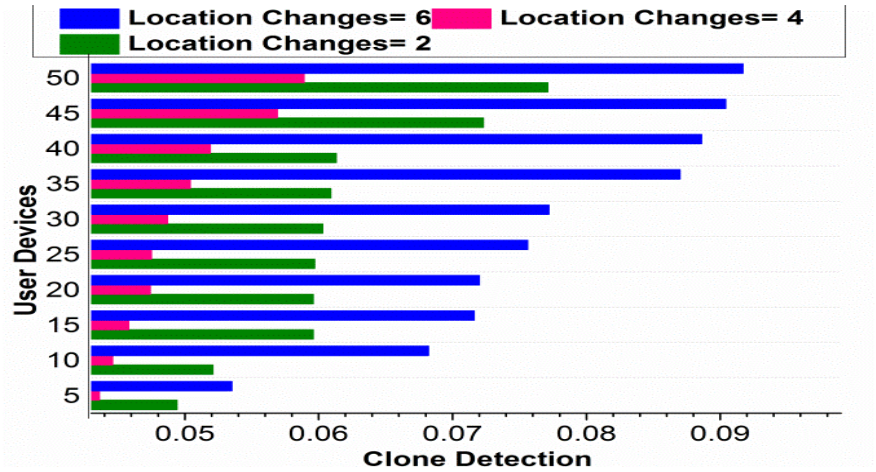

Fig. 8—Clone Detection for User Devices

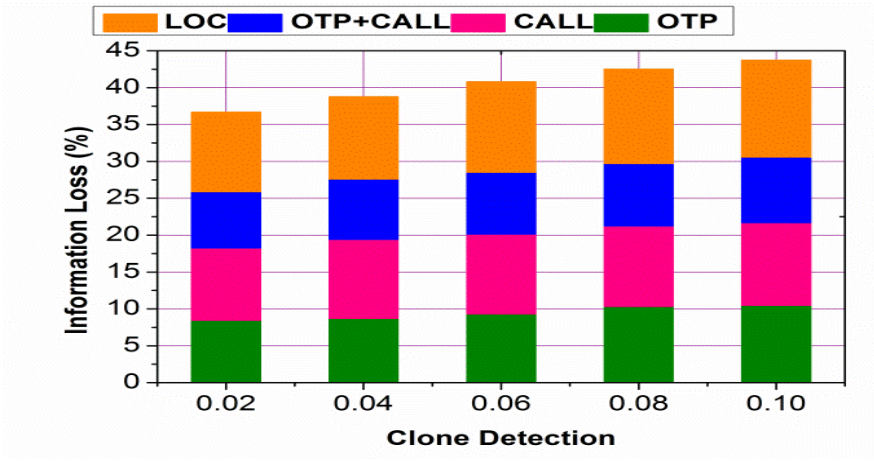

Fig. 9—Information Loss for Clone Detection

The user devices for detecting the clone in the appeal information are done for the varying location changes (Refer to Fig. 8). If the user device varies, the clone for the information is increased, and if location decreases, the detection increases. The location change for 2 shows lesser detection of user devices compared to 6 values. The clone detection is performed for varying information loss percentages, and it ranges from low to high (Refer to Fig. 9). It is evaluated for OTP, CAL, OTP+CAL, and LOC, and the detection process is done reliably. Thus, the clone detection and identification processes for OTP+CAL show lesser information loss than the other three processing.

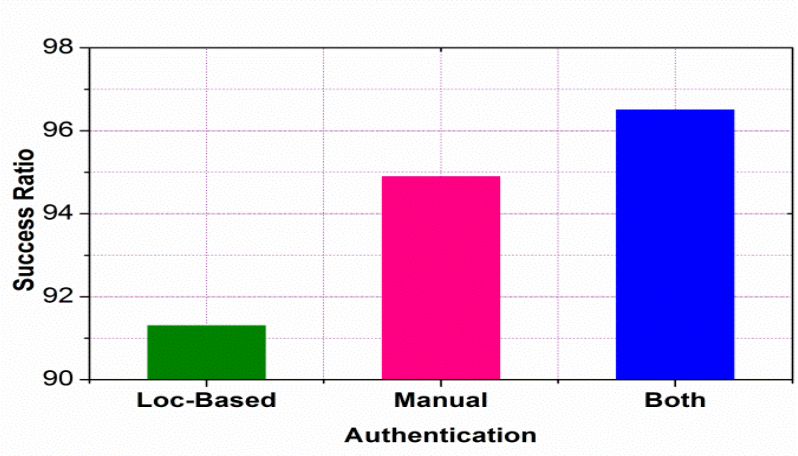

Fig. 10—Success Ratio for Authentications

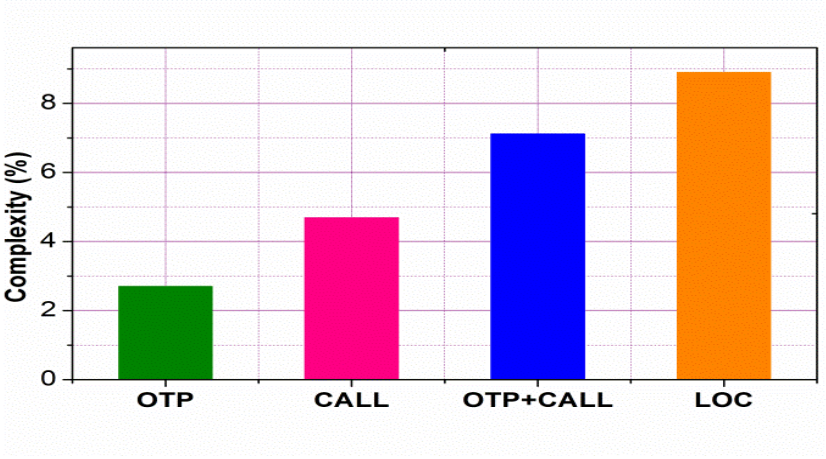

Fig. 11 Complexity (%) for Authentications

The authentication is done on three methods such as manual, location-based, and both the process (Refer to Fig. 10). The computer success rate for these three approaches ranges from low to high values. If the success ratio for both processing and manual process shows, it is a higher value compared to the location-based method. The OTP, CAL, OTP+CAL, and LOC vary for complexity percentage and show the value ranges from low to high (Refer to Fig. 11). For LOC, the complexity increases, whereas for CAL+OTP, it shows lesser value. The complexity decreases for CAL and OTP, and the LOC shows a higher range than other methods.
The proposed 2WIAM is analyzed using demonstrations by configuring a software-based OTP generating system and 50 mobile devices. The devices are connected through 2.4 GHz wireless links for file sharing. The sharing is authenticated post the verification of passwords. The identities of 12 mobile devices are swapped periodically for performing a cloning attack. The three-way hash is used to provide secure data sharing in which the SHA-224 is used. The location of the devices is periodically changed based on the movement of the devices. The performance is verified through instance observations for the metrics authentication failures, processing time, and information loss. The benchmarked methods PUF-AAS [21], M2M-DA [15], and RAP [17] are considered in a comparative analysis using the above metrics.

Authentication failure

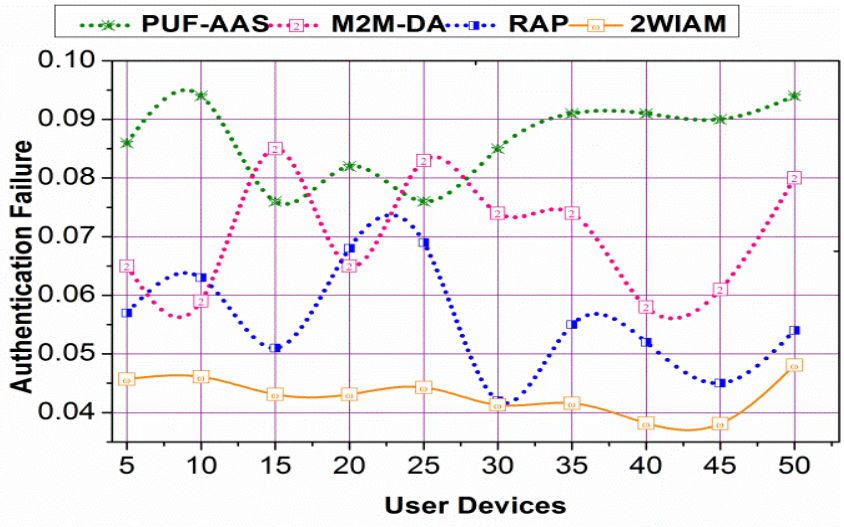

Fig.12—Authentication Failure Comparison

The authentication failure varies for user devices that deploy the 5G, and the verification is performed for the appeal from the user. Here, the analysis is monitored, and the acknowledgment is provided, and it is represented as $\left(v' - \frac{f_m}{\frac{eq}{\omega}}\right)$. The information appeals from mutual authentication and decides the device's usage; if it is not secure, the authentication is not provided. Here, the authentication failure decreases and addresses the leakage of information that deploys user privacy. The clone information is monitored in the initial stage, and security is given to the users, which deploys the replication and change. The 2-way identification is made for the varying users. It is associated with the mobile IP, and it is represented as $(x_0 - u_0) * \left(\frac{q'}{a'}\right)$. Periodic surveillance is carried out reliably and securely. Cloning for this PUF method is used. It addresses the information leakage and distributes the service by performing mutual authentication. Thus, the mapping is performed for the mobile IP to track the device's location, for this mutual authentication is done promptly. The evaluation is done by a 2-way identification method and determines the decision-making approach. The service provider is responsible for forwarding the service to the secure user; by performing this, the authentication failure is decreased (Refer to Fig. 12).

Processing time

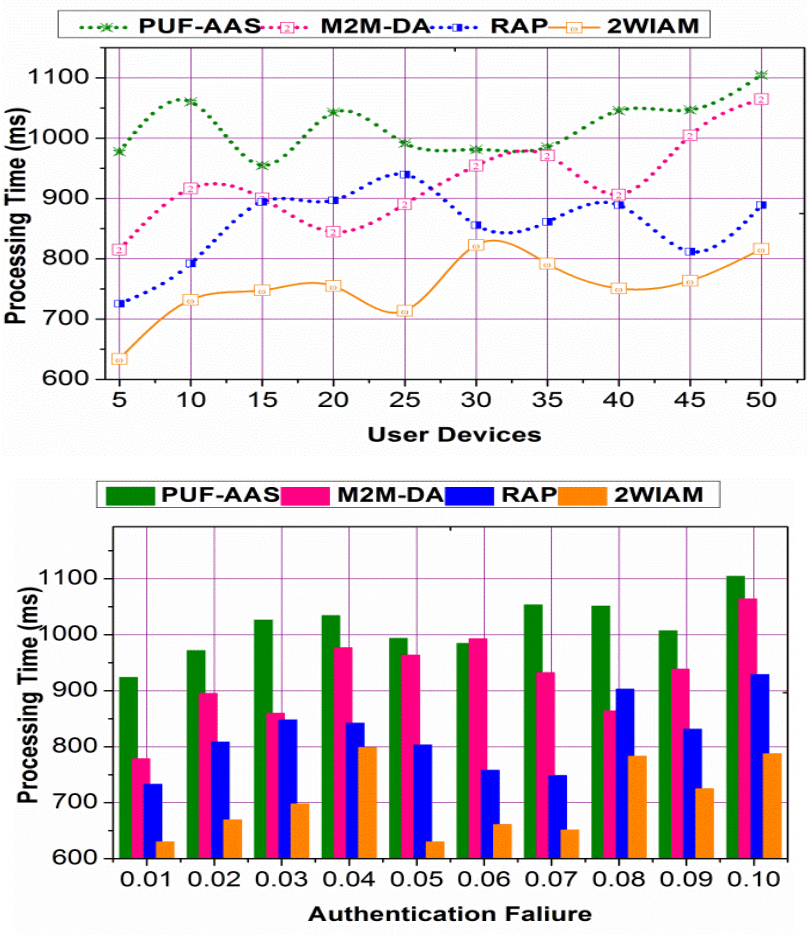

Fig. 13—Processing Time Comparisons

The processing time for the proposed work decreases for varying user devices and authentication failure (Refer to Fig. 13). Here, the mobile IP does not change for the varying devices for the appeal from the user. For the processed appeal, the service is provided, computed as $q'(s') - v'(r_d)$. If the user appeals for the service, the authentication verification is done for the varying devices in 5G. For this, the preliminary step is to analyze the manual and location-based to deploy the authentication. Here, the processing time decreases, and the clone's analysis for the varying user appeal and the mapping is performed for the mobile IP. The acknowledgment is given to the user, and the OTP is produced for the verification process. Thus, the monitoring is carried out to decrease information leakage and provides privacy for the user. When determining whether to proceed with this course of action, mutual authentication is utilized to assess risk. The processing time is calculated for the number of devices deployed by equating $\left[(r_d - v') + \left(\frac{g_0}{x_0+q'}\right)\right]$. Here the mapping is performed, and the acknowledgment is done for the varying user by the 2WIAM method. The location is tracked for the varying user, addresses the appeal, and provides the response on time, thus the processing time decreases.

Information loss

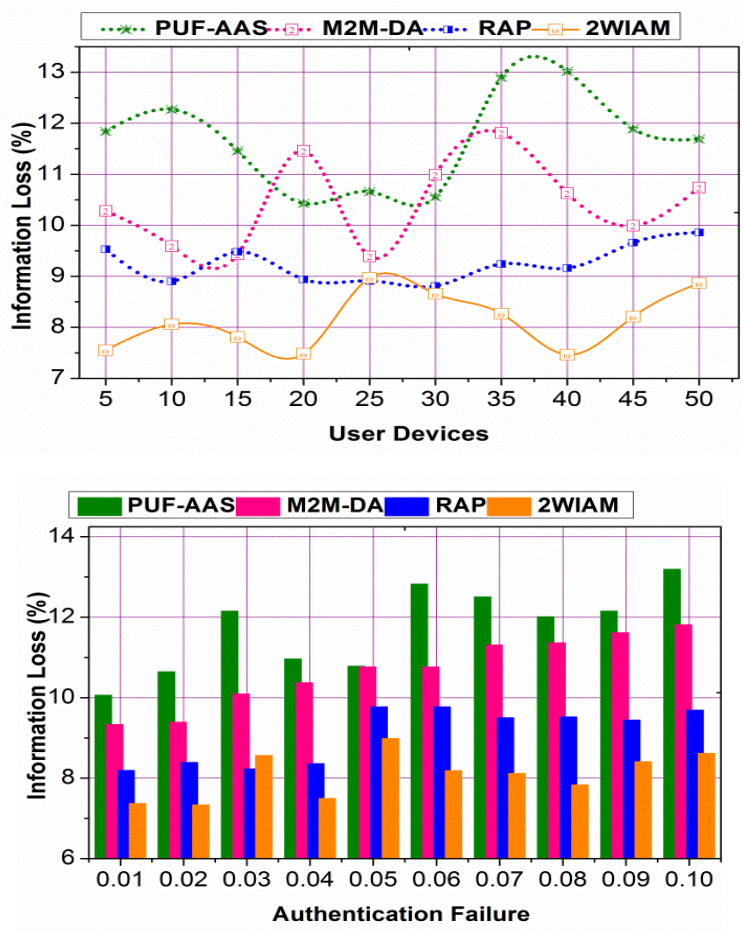

Fig. 14—Information Loss Comparisons

In Fig. 14, the information loss decreases for varying users' devices and authentication failure, and it is denoted as $\left[\prod_{k_g}^{q'} \left(\delta * \frac{j_s+\sigma}{u_n}\right)\right]$. The verification is done for the appeal from the user that deploys the manual and location-based authentication. The authentication check is done for the appeal, and the service provider provides the security. The information loss is addressed, and it deploys the decision-making approach by mapping the mobile IP. Mutual authentication is done to address the clone for the information and decreases the leakage. Here, the 2-way verification is done, and it evaluates the usage permission, and the mapping is performed for the replication and changes in services. The user is provided with safety by distinguishing the genuine from the fake by using both manual and location-based verification. Thus, leakage and information loss are addressed in 2-way identification processes that deploy PUF. It is responsible for monitoring the number of devices and appeals from the user, and the acknowledgment is done periodically on time. Here, both the replication and change of information are analyzed and produced by mapping the mobile IP. Thus, information loss and leakage are decreased in the proposed work. For concluding the comparative analysis, the above results are summarized in Tables 1 (User Devices) and 2 (Authentication Failure)

Table 1—Summary of Comparison for User Devices

Metrics	PUF-AAS	M2M-DA	RAP	2WIAM
Authentication Failure	0.094	0.08	0.054	0.0481
Processing Time (ms)	1104.85	1064.85	888.95	816.504
Information Loss (%)	11.69	10.74	9.86	8.866

Compared to the existing methods, the proposed method reduces authentication failure, processing time, and information loss by 8.37%, 19.92%, and 5.7%.

Table 2—Summary of Comparison for Authentication Failure

Metrics	PUF-AAS	M2M-DA	RAP	2WIAM
Processing Time (ms)	1104.45	1063.92	928.97	787.232
Information Loss (%)	13.19	11.81	9.69	8.614

The proposed method achieves 23.75% less processing time and 8.8% less information loss for the different authentication failure factors.

5. CONCLUSION

User device authentication is a prominent task in preserving the privacy of the user and information. With the growth of 5th generation communication systems and networks, security stands in high demand for combating real-world attacks. A 2-way identity authentication method for reliable security in user device authentication is proposed in this article. This method exploits physical unclonable function and three-way hash for providing device authentication and information security. Device authentication is provided using manual and location-based verifications for identifying replications or clones in the network. The specific decision-making process accounts for mutual authentication using the service provider and device credentials to ensure robust security measures. The decision remains unbiased until the authentication is reliable and information loss is contained. The proposed method's performance is verified using demonstrations, and it is found that it reduces authentication failure, information loss, and processing time. This is unanimous for different devices and authentication failures.

Funding: This research received no external funding.
Conflict of interest: The authors declare no conflicts of interest.

REFERENCES

[1] Jones AD, Jagannathan KA, Rhoades A, Srivastava AK, Grotjahn R, Ullrich PA. Decision-relevant metrics for regional hydroclimate phenomena. AGUFM. 2018 Dec;2018: GC14C-01.
[2] Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 5G networks: New areas and new challenges. *Digital Communications and Networks*, *6*(3), 281-291.
[3] Bouk SH, Ahmed SH, Eun Y, Park KJ. Multimodal Named Data Discovery with Interest Broadcast Suppression for Vehicular CPS. IEEE Transactions on Mobile Computing. 2020 Feb 3.
[4] Anbarasan M, Muthu B, Sivaparthipan CB, Sundarasekar R, Kadry S, Krishnamoorthy S, Dasel AA. Detection of flood disaster system based on IoT, big data and convolutional deep neural network. Computer Communications. 2020 Jan 15;150:150-7.
[5] Shankar A, Jaisankar N. A novel energy efficient clustering mechanism in wireless sensor network. Procedia Computer Science. 2016 Jan 1;89:134-41.
[6] Yu, W., & Wen, Y. (2019). Leveraging Balanced Logic Gates as Strong PUFs for Securing IoT Against Malicious Attacks. *Journal of Electronic Testing*, *35*(6), 853-865.
[7] Pramanik A, Luhach AK, Batra I, Singh U. A systematic survey on congestion mechanisms of CoAP based Internet of Things. InInternational Conference on Advanced Informatics for Computing Research 2017 Mar 17 (pp. 306-317). Springer, Singapore.
[8] Akbarzadeh, A., Bayat, M., Zahednejad, B., Payandeh, A., & Aref, M. R. (2019). A lightweight hierarchical authentication scheme for internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *10*(7), 2607-2619.
[9] Abdulsahib GM, Khalaf OI. An improved algorithm to fire detection in forest by using wireless sensor networks. International Journal of Civil Engineering & Technology (IJCIET)-Scopus Indexed. 2018 Nov;9(11):369-77.
[10] Hao, P., & Wang, X. (2019). Integrating PHY Security Into NDN-IoT Networks By Exploiting MEC: Authentication Efficiency, Robustness, and Accuracy Enhancement. *IEEE Transactions on Signal and Information Processing over Networks*, *5*(4), 792-806.
[11] Molano JI, Lovelle JM, Montenegro CE, Granados JJ, Crespo RG. Metamodel for integration of internet of things, social networks, the cloud and industry 4.0. Journal of ambient intelligence and humanized computing. 2018 Jun 1;9(3):709-23.

[12] Saravanan V, Parthiban KT, Kumar P, Anbu PV, Ganesh PP. Evaluation of fuel wood properties of Melia dubia at different age gradation. Research Journal of Agriculture and Forestry Sciences. 2013;1(6):8-11.
[13] Karageorgos, I., Isgenc, M. M., Pagliarini, S., & Pileggi, L. (2019). Chip-to-Chip Authentication Method Based on SRAM PUF and Public Key Cryptography. *Journal of Hardware and Systems Security*, *3*(4), 382-396.
[14] Balan, A., Balan, T., Cirstea, M., & Sandu, F. (2020). A PUF-based cryptographic security solution for IoT systems on chip. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 1-22.
[15] Easwaramoorthy S, Moorthy U, Kumar CA, Bhushan SB, Sadagopan V. Content Based Image Retrieval with Enhanced Privacy in Cloud Using Apache Spark. InInternational Conference on Data Science Analytics and Applications 2017 Jan 4 (pp. 114-128). Springer, Singapore.
[16] Ezhilmaran D, Adhiyaman M. Soft computing method for minutiae-based fingerprint authentication. International Journal of Industrial and Systems Engineering. 2018;30(2):237-52.
[17] Prathik A, Anuradha J, Uma K. A Novel Algorithm for Soil Image Segmentation using Color and Region Based System. optimization.;12:13.
[18] Broumi, S., Nagarajan, D., Lathamaheswari, M., Talea, M., Bakali, A., & Smarandache, F. (2020). Intelligent algorithm for trapezoidal interval valued neutrosophic network analysis. CAAI Transactions on Intelligence Technology, 5(2), 88-93. doi:10.1049/trit.2019.0086
[19] T.-W. Yang, Y.-H. Ho, and C.-F. Chou, "Achieving M2M-device authentication through heterogeneous information bound with USIM card," *Future Generation Computer Systems*, vol. 110, pp. 629–637, 2020.
[20] D. Korać and D. Simić, "Fishbone model and universal authentication framework for evaluation of multifactor authentication in mobile environment," *Computers & Security*, vol. 85, pp. 313–332, 2019.
[21] Y. Jiang, Y. Zhu, J. Wang, and Y. Xiang, "Efficient authentication protocol with anonymity and key protection for mobile Internet users," *Journal of Parallel and Distributed Computing*, vol. 137, pp. 179–191, 2020.
[22] P. Laka and W. Mazurczyk, "User perspective and security of a new mobile authentication method," *Telecommunication Systems*, vol. 69, no. 3, pp. 365–379, 2018.
[23] T.-Y. Chang, C.-J. Tsai, J.-Y. Yeh, C.-C. Peng, and P.-H. Chen, "New soft biometrics for limited resource in keystroke dynamics authentication," *Multimedia Tools and Applications*, vol. 79, no. 31-32, pp. 23295–23324, 2020.
[24] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-Factor Authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018.
[25] J. Long, W. Liang, K.-C. Li, D. Zhang, M. Tang, and H. Luo, "PUF-Based Anonymous Authentication Scheme for Hardware Devices and IPs in Edge Computing Environment," *IEEE Access*, vol. 7, pp. 124785–124796, 2019.
[26] A. V. Galkov, I. V. Mashechkin, and I. S. Popov, "Behavioral Model of Text Input in the Authentication of Mobile Device Users," *Moscow University Computational Mathematics and Cybernetics*, vol. 44, no. 3, pp. 109–119, 2020.
[27] T. Dee, R. Scheel, N. Montelibano, and A. Tyagi, "User-Silicon Entangled Mobile Identity Authentication," *Journal of Hardware and Systems Security*, vol. 4, no. 3, pp. 208–229, 2020.
[28] Z. Gao, Z. Cheng, W. Diao, J. Zhang, and H. Lu, "Identity authentication based on trajectory characteristics of mobile devices," *Journal of Systems Architecture*, p. 101857, 2020.
[29] B. L. Parne, S. Gupta, and N. S. Chaudhari, "ESAP: Efficient and secure authentication protocol for roaming user in mobile communication networks," *Sādhanā*, vol. 43, no. 6, 2018.
[30] B. Abazi, B. Qehaja, and E. Hajrizi, "Application of biometric models of authentication in mobile equipment," *IFAC-PapersOnLine*, vol. 52, no. 25, pp. 543–546, 2019.
[31] P. Xie, J. Feng, Z. Cao, and J. Wang, "GeneWave: Fast Authentication and Key Agreement on Commodity Mobile Devices," *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1688–1700, 2018.
[32] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.