International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Lightweight Multi-Factor Authentication Scheme for Three-Layer Architecture: User-Fog-Cloud Environment

K. Shanthi[1], R. Maruthi[2]

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: Fog computing is an expanded and dispersed environment where processes related to applications are maintained between the end-user device and the clustered system's edge for better and more. The fog computing paradigm carries over the cloud's security and privacy vulnerabilities due to its inherited features. One of the primary security issues is authentication. Secure authentication scheme is necessary to access difference services for permissible users. Password-based authentications and other single sign-on procedures for user identification are not secure methods. To navigate around the drawbacks of the single sign-on process, a number of multi-tier authentication methods are suggested.For a user-fog-cloud scenario, this paper suggests a secure lightweight multifactor authentication technique. This paper presents a method for multifactor mutual authentication between user-fog and fog-cloud using lightweight cryptography functions using bitwise operators. For user-fog authentication, multifactor authentication scheme is used, which includes knowledge (password), possession (personal identity with QR-code) and inherent (biometric) factors. For fog-cloud authentication, simple mutual authentication is used which includes lightweight cryptographic hash function with simple operations. The computation and communication costs are examined to assess the efficacy of the proposed work. The simulation results demonstrate that the proposed approach is highly efficient and safe. When compared to the state-of-the-art, the suggested method drastically reduces the computing cost.

Keywords: *Fog computing, cloud computing, lightweight, authentication, three layer architecture*

1. Introduction

Cloud computing is a potential information technology architecture for both businesses and consumers. With features like on-demand self-services, pervasive network connectivity, rapid elasticity, measurable service, and location-independent resource pooling, it provides a desired paradigm for data storage and interaction.[1] However, due to its poor implementation effectiveness, the cloud computing platform cannot provide many of the current intelligent application features, including minimum delay, location awareness, and support for intelligent applications' mobility. To meet the demands, cisco initially proposed the concept of fog computing [n] in 2012. It's a development of conventional cloud computing. Its primary objective is improving computational capacity, storage space, network services, and management control complexity between terminal devices and cloud servers. Figure 1 illustrates the three-layer design of User-Fog-Cloud

Edge Layer: Physical devices and the end user are relatively close to the edge layer,which includes cellular, sensor networks, smart cards, smart devices, and further elements connected to the Internet of Things (IoT). These gadgets are frequently widely dispersed and practical, gathering information from real objects or items and relaying private information to the fog level for archival or examination [3]. In this research work, the edge layer contains only end users.

Fog Layer: It is located at the edge of the network. It has a lot of fog nodes, such as switches, routers, access points, gateways, low-level channels, etc. To boost capacity and throughput, fog nodes may cooperate and interact with the cloud using an IP network to communicate with the cloud's data centre.

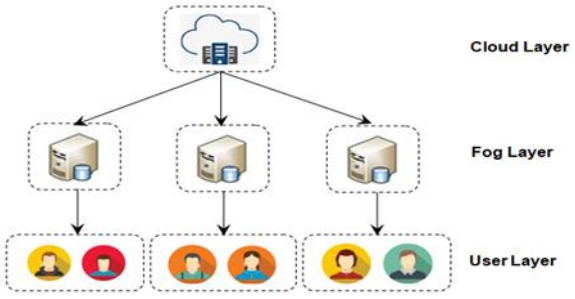

Figure 1 Three-layer architecture

Cloud Layer: The majority of the cloud computing platform's components are high-end servers and storage,is in charge of providing an extensive range of client applications, which includes smart navigation, manufacturing, smart house, smart workplaces etc. This layer can perform many calculations, analyses, and storage since it has a lot of computing, storage, and saving power [4].

Fog-cloud technology advancements have created new

[1] *Research Scholar, PRIST University, Thanjavur;*
[2] *Associate Professor, Hindustan Institute of Technology and Science, Chennai*

security risks, such as malicious insider attacks, data loss, and privacy violations. These networks are susceptible to a wide range of security threats. Before granting users access to resources, it must identify users. The primary method of identifying users is through authentication schemes, which can be done using various methods, including passwords, biometric verification, public key infrastructure, and symmetric key-based authentication schemes [5]

Initially, user authentication relied just on one (single) factor. As an illustration, using a secret word or personal identification number (PIN) to verify the rightful owner of the consumer ID might be considered. This kind of verification appears to be the weakest [6]. Due to their reliance on a single element of authentication, password-based and graphical authentication [7], systems are particularly susceptible to brute force and dictionary attacks [8]. For an upgrade over password-based authentication, biometric authentication [9] is suggested. However, because of the unchanging nature and control of biometric information in a centralized database or segments, biometric authentication also has drawbacks and dangers. Reusing stolen biometric details is one security risk that might result from the leak of biometric information [10].

Due to many security concerns, the single factor is unreliable in offering appropriate protection [11]. Therefore, two-factor authentication, which combines account name and secret code with the feature of individual ownership, like a digital wallet or a mobile [12], was presented as a wise step forward.

It was proposed to use more than two identifications in multi-aspect verification to boost security and make it simpler to protect computer systems and other vital services from unauthorized disclosure [13]. In multifactor authentication, the following factors are used: Knowledge Factor—a password or other piece of information the User is aware of; Possession Factors - The User's possession of anything, like as a digital wallet, mobile phone, or additional tokens; Biometric Factor - A biometric element, such as biometric information or a person's behaviour pattern.

This research paper aims to propose a user-fog-cloud environment-friendly, lightweight multifactor authentication solution.

To use the cryptographic function with bitwise operators for secure authentication

● To develop multifactor authentication using knowledge, possession and inherent factors.

The significant contribution of this paper is as follows:

● For user-fog authentication, a multifactor authentication scheme is used, which includes knowledge (password), possession (personal identity with QR code) and inherent (biometric) factors.

● For fog-cloud authentication, simple mutual authentication includes a lightweight cryptographic hash function with simple operations.

This paper's remaining section is organized as various authentication schemes using fog and cloud environments are explained in section 2. Next, section 3 illustrates the suggested approach with some preliminary concepts. Section 4 then analyzes the performance of the intended task, and Section 5 provides an explanation of the work's conclusion and next steps.

2. Literature Review

Simple anonymous authentication and secure communication system are revealed by Weng et al. [14]. This methodology mutually authenticates User, cloud and fog using a secure hash function and bitwise operation. Fog members can decide on a session (temporary) key when the authentication successfully encrypts the subsequent communication packets. This technique performs better in computing time and has additional security features.

Atiewi et al. [15] suggest identity verification and cryptographic techniques for IoT enabled by the cloud to safeguard massive data systems. It is also suggested to utilize multifactor authentication to access cloud-based data. The User provides their registered details to the reliable entity at the time of login. For accessing to the stored data, trusted authority offers three degrees of authentication: reading files from the cloud using first-level authentication, downloading files using second-level authentication, and downloading files from the hybrid cloud using third-level authentication.

A novel, safe, isolated verification method with three components—user id, secret word, and biometrics—is proposed by Liu et al. [16]. The implementation of crowdsourcing IoT uses a chaotic map zero-knowledge proof concept. It lessens the burden on computation and communication. A fog computing-based mutual authentication system that uses cryptography and one-way hash functions were proposed by Kalaria et al. [17]. It efficiently provides a defence against cyber-attacks. This method accomplished mutual authentication across fog devices, but immutability presented a challenge.

For cross-platform IoT systems, Khalid et al. [18] propose a novel authentication scheme. By extending the kerberos workflow, this method uses the AES-ECC (Elliptical Curve Cryptography) technique to handle encryption keys effectively and create secure mutual authentication between edge and fog nodes. However, this method does not allow changing the password and smart card. To

protect financial transactions using Virtual Private Networks (VPN), Prabakaran et al. [19] present a system based on ECC that employs robust authentication with user identity and biometrics.

A lightweight authentication method is suggested by Deebak et al. [20] and relies on the cryptographic system. This method makes advantage of simple processes to create secure network connectivity for data transmission. Moreover, it maintains compatibility criteria such as low-cost and low power to reduce communication and computation costs.

ECC-based end-user authentication for home automation is suggested by Kaur et al. [21]. However, this technique is vulnerable to security threats and inappropriate for home automation because it uses public key-based crypto algorithms. To deliver safe home services for authorized end users in IoT-based home automation, and to solve the security vulnerabilities raised in [21], Yu et al [22] suggests a powerful multi-factor authentication approach.

Ali et al. [23] suggest a heterogeneous authentication solution for the cloud which is edge-centric that employs biometrics encryption. The solution uses individualized portable electronics to protect biometric data, which improves resource usage and addresses the cloud environment constraint. The edges send the encrypted voice and facial to the cloud for processing. The cloud then uses the biometric data to decrypt and verify the information and determine the identity of the user.. Dhillon et al. [24] provide an effective, robust authentication system to obtain patient information for smart healthcare using cloud-IoT networks. It includes multifactor mutual authentication with secure key sharing. However, the protocol does not offer robust identity verification or user anonymity.

An innovative inter mutual dual-factor validation protocol among an Internet of Things device and a server is suggested by Mostafa et al. [25], and it simply needs hash functions. Two-factor authentication provides strong protection against online assaults. Additionally, the authors provide a way to create secure session keys.To establish the appropriate level of security, it leverages two Physical Unclonable Functions (PUF) in the Internet of Things device.

An effective IoT authentication strategy is presented by Alshawish et al. [26], which enables mutual authentication between IoT devices, and servers which provide authentication and IoT manufacturer.It uses a hash function for authentication and a cryptographic function for data security.

A robust shared authentication method for cloud-assisted IoT is presented by Liu et al. [27]. The authentication is built using a hash signature. It offers storage monitoring with the help of a fully trusted organization, greatly enhancing the fairness and effectiveness of the search. A two-factor authentication approach for smart medical care is proposed by Agrahari et al. [28]. Prior to allowing users to log in and exchange mutual authentication with sensor hubs, a trusted authority registers users, servers, and sensor hub nodes as part of the scheme.

Nevertheless, the authors omitted steps for updating smart cards and passwords. For multi-gateway Wireless Sensor Networks (WSN), Dai et al. [29] suggested a three-factor ECC-based authentication mechanism. This system reduces password-guessing tries and increases the effectiveness of authentication.

Sahoo et al. [30] suggest a three-factor-based user authentication approach. It supports the phase of smart card cancellation and adaptive node sensor addition. This approach lowers the cost of storage and communications. Singh et al. [31] offer a mutual authentication system to track health data. This method makes advantage of cryptographic operations. It reduces network latency and costs, effectively controls medical resources, and complies with high-security standards ensuring data confidentiality.

Zou et al. [32] proposed a user authentication technique utilizing ECC for safe, smart home environments in IoT. This system offers forward secrecy and user anonymity. However, this strategy is susceptible to various attacks, such as forgery and leakage attacks. A simple and anonymity-preserving user authentication system was created by Masud et al. [33]. The suggested approach offers a secure user session and prevents unauthorized users from accessing the IoT sensor nodes. To lower the minimal CPU cost of the node, cryptography is used. The method is effective and superior because it requires low cost for computation and communication.

Junhui Zhao[39] put forward a multi-gateway lightweight authentication method as a solution to address problems such increased cost for communication, decreased performance on the network, and ineffective cross-domain connectivity inside the same gateway paradigm with greater network. First, the three-factor authentication technique that our scheme is built on uses the hash function, XOR operation, and Chebyshev chaotic mapping. This technique generates session keys, enables user key changes, and accomplishes safe authorization in between sensor both users and nodes. Second, they show via security analysis that the suggested systemensures session key forward security and is impervious to transient secret leakage, internal disguise, and sensor capture threats.Additionally, they provide a Random Oracle Model (ROM)-based verification of the semantic reliability of session credentials.Ultimately, the results demonstrate that our suggested approach is better in consistent with the needs of lightweight authorization for device security in

the Internet of Things and requires less computational resources and communication overhead than previous techniques.

3. Methods

This section explains the predicted secure, lightweight multifactor validation scheme for a user-fog-cloud environment. The proposed work contains three entities: User (U= U1, U2, U3, … Un), Fog Server (FS = FS1, FS2, FS3,…,FSm) and Cloud Server (CS). Figure 2 shows the proposed generalized architecture.

The proposed method includes multi-factor and mutual authentication to provide security. It comprises two phases: registration and authentication phases. In the registration phase, each server for fog and users must register their information to the cloud server. For secure communication between the user, fog, and cloud, deploy the secure channel. In the authentication, the User is verified by the fog server through the cloud server.

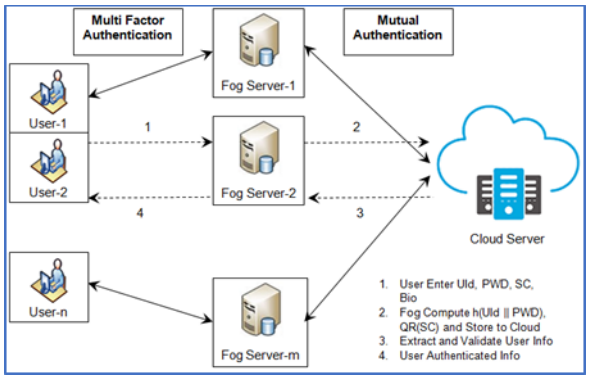

Figure 2 Proposed Generalized Architecture

Initially, simple hash computations are used to register the fog server. Then, the fog user enters the User id, password, and secret code and selects biometric features for registration. Then, the hash function is used for secure computation. Finally, the computed hash value is stored in a cloud server through a secure fog server.

Table 1 shows the notation and description.

Table 1 Notations and Description

Notation	Description
CS	Cloud Server
FS_i	i^{th} Fog Server
U_j	j^{th} User
$FSID_i$	Identity of i^{th} Fog Server
UID_j, PWD_j, SC_j	Identity, Password and Secret Code of j^{th} User
QR_j, $BioF_j$	QR code and Fingerprint of j^{th} User
h(-)	Cryptographic hash function
‖, ⊕	Concatenation and Bitwise XOR operator

3.1 Registration Stage

In this phase, each fog server and User must register their information to the cloud server.

3.1.1 Fog Server Registration

The cloud server registers the fog server via a secure communication channel. Figure 3 shows the process of fog server registration.

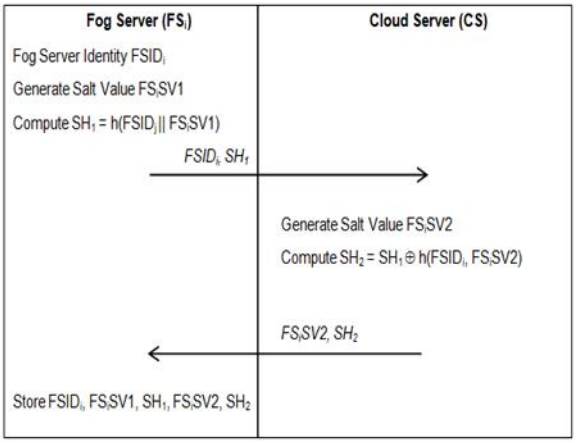

Figure 3 Fog Server Registration Process

The following steps are used for fog server registration:

Step1: FSi select FSIDi

Step2: FSi generate Random salt value FSiSV1

Step3: FSi compute SH1 = h(FSIDi ‖ FSiSV1)

Step4: Send M1={FSIDi, SH1} to CS

Step5: CS generate FSiSV2

Step6: CS compute SH2 = SH1 ⊕ h(FSIDi, FSiSV2)

Step7: CS Send FSiSV2, SH2 to FSi

Step8: FSi Store FSIDi, FSiSV1, SH1, FSiSV2, SH2

3.1.2 Fog User Registration

The User is registered to the cloud server through the secure communication channel. The User inputs their UID, PWD, SC, and BioF and generates a random salt value.

The following steps are used in the user registration process.

Step1: User Uj Input UIDj, PWDj, SCj, BioFj

Step 2: User Uj Compute UH1 = h(UIDj ‖ PWDj), UH2 = h(SCj), and UH3 = h (BioFj)

Step 3: User Uj send UIDj, UH1, UH2, and UH3 to Cloud Server

Step4: Cloud Server Generate UjSV1 and QR(UH2)

Step5: Cloud Server Compute UH4 = h(UIDj ‖ UjSV1), UH5 = h(UIDj ‖ UH1 ‖ UH3), UH6 = UH4 ⊕ h(QR) ⊕ UH1

Step6: Cloud Server send UjSV1, QR(UH2), UH4, UH5, UH6

Step7: User store UjSV1, QR(UH2), UH4, UH5, UH6

Figure 4 shows the process of user registration

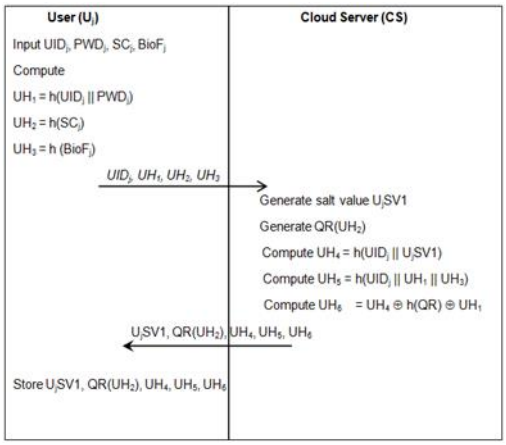

Figure 4 Fog User Registration Process

3.2 Authentication Phase

The authorized user is identified through authentication, and the legitimate user is allowed to read/write information retained in the cloud. The CS validates the user through the fog server.

The following steps are used in the user authentication process.

Step1: User Uj Input UID'j, PWD'j, SC'j, BioF'j

Step2: User Compute UH'1 = h(UID'j ‖ PWD'j)

Step3: If UH'1 ≅ UH1 then send h(SC'j) and h(BioF'j) to Fog

Step4: Fog Server Get SH1, FSiSV2

Step5: Fog Server Send h(SC'j), h(BioF'j), SH1, FSiSV2 to Cloud

Step6: Compute SH'2 = SH1 ⊕ h(FSIDi, FSiSV2)

Step 7: If SH'2 ≅ SH2 Fog Server FSj is authenticated.

Step 8: Cloud Send QR(UH2) and UH5 to Fog Server.

Step9: Fog Server Extract SCr = QR(UH2)

Step10: Fog Server Verify T1 = h(SC'j) ≅ SCr

Step11: Fog Server sends T1 and UH5 to User

Step12: User Compute UH'5 =h(UIDj ‖ UH1‖UH3)

Step13: User Verify T2 = UH5≅ UH'5

Step 14: If T1 and T2 are true, then User Ui is Successfully Authenticated.

Figure 5 shows the verification process of the User.

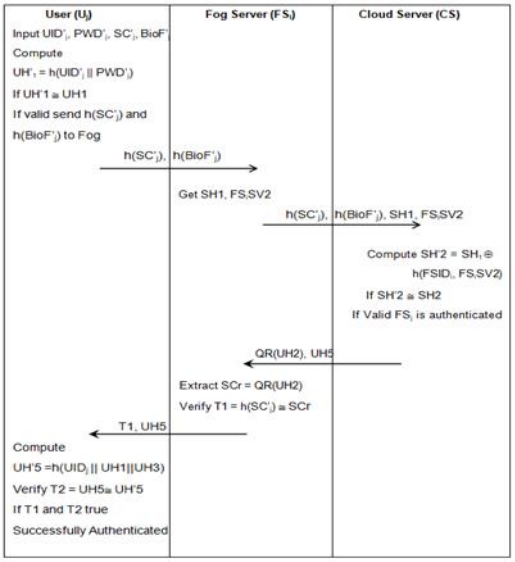

Figure 5 Verification Process of User

4. Results

The findings of the experiments are used to assess how well the suggested work performs. The computing cost measures are used to assess the efficacy of the proposed work. The cost of computation is defined as the duration spent in the process, i.e. running time.

Five different authentication methods, including Weng [14], Nikravan [34], Wu [35], Chen [36], and Yu [37], are compared with the proposed approach. Table 2 shows the completion time of the diverse cryptographic process.

Tbp represents the time needed to execute a single bilinear pairing operation, and Tecm indicates the time needed to execute a single elliptic curve point multiplication operation. The stands for the amount of time needed to execute a single hash function operation, Tfe indicates the amount of time needed to execute a single fuzzy extraction operation, Tased represents the amount of time needed to execute a single asymmetric encryption or decryption operation, The concatenation and XOR processes don't require much communication time in comparison to the other operations. Thus these can be disregarded.

Table 2 Cryptographic process completing time

Operator	Description	Completion Time (ms)
T_{bp}	Bilinear Pairing	17.4
T_{ecm}	Point multiplication on an elliptic curve	13.5

T_h	hash function	0.42
T_{fe}	Fuzzy extract [36]	2.28
T_{ased}	Asymmetric Encryption or Decryption [36]	5.25

Table 3 shows the computational cost for different entities. The total time of the proposed work is 7Th + 2Th + 5Th ≈ 5.88 ms. The user entity has a high computational cost compared to the other two entities.

Table 3 Computational cost for different entities

Entity	Computation Cost	Total Time
User	$7T_h \approx 2.94$	$14T_h = 5.88$
Fog Server	$2T_h \approx 0.84$	
Cloud Server	$5T_h \approx 2.1$	

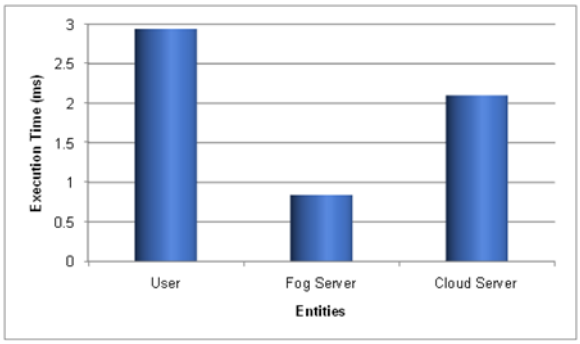

Figure 6 compares execution time for user, fog and cloud server entities.

Table 4 and Figure 7 compares computational cost for different methods.

Table 4 Computational cost comparison

Author	Computations	Total time (ms)
Nikravan et al., [34]	$4T_{bp}+10T_{ecm}+25T_h$	215.1
Wu et al. [35]	$3T_{bp}+10T_{ecm}+21T_h$	196.02
Chen et al. [36]	$T_{fe} + 31T_h + T_{ased}$	20.55
Yu et al. [37]	$T_{fe} + 25T_h$	12.78
Weng et al., [14]	$22T_h$	9.24
Proposed	$14T_h$	5.88

The Nikravan et al. [34] protocol, which combines bilinear pairing, hash function, and elliptic curve point multiplication, is the most time-consuming. However, the suggested protocol takes the least amount of time.

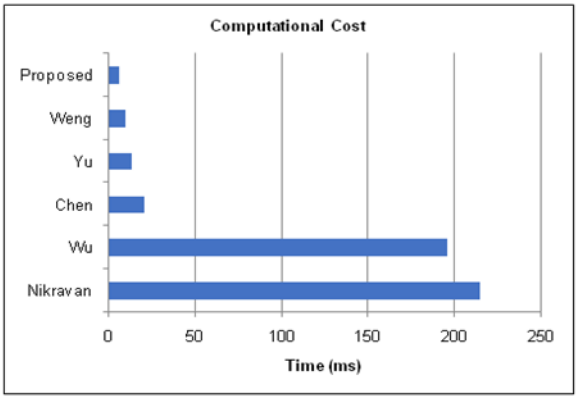

Figure 7 Computational cost comparison

From that results, the Nikravan et al. [34] method has a high computational cost. On the other hand, the proposed work takes less computation time for the authentication process compared to other methods. Nikravan et al., [34] < Wu et al., [35] < Chen et al., [36] < Yu et al, [37] < Weng et al., [14] < proposed.

The cost of communications is determined by the size of the authentication messages exchanged between entities during authentication. The asymmetric encryption and decryption have a massive 1024-bit overhead. The elliptic curve point multiplication process requires 320 bits of length, the hash values and random numbers are roughly 160, and the identification, password, and biometrics are 128. Table 5 shows the communication cost for a different protocol.

Table 5 Communication Cost Comparison

Author	Communication Cost (bit)
Nikravan et al., [34]	3840
Wu et al., [35]	7744
Chen et al., [36]	2496
Yu et al. [37]	2560
Proposed	1184

Figure 8 shows the comparison of communication costs. The proposed approach only needs 1184 bits for communication

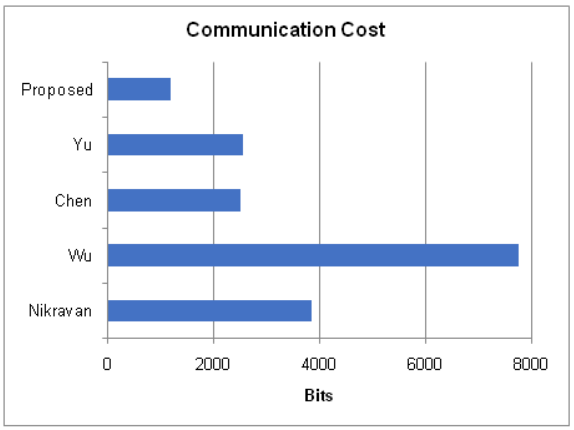

Figure 8 Communication Cost

5. Discussion

This scheme uses two operations hash function and XOR operation. The cost of the XOR operation is minimal compared to the hash operation. Therefore, the paper omits XOR operation in the performance analysis. The symbol Th represents the time for the hash function. The time taken to complete the hash function is 0.42 ms.

This work thwarts different types of attacks. When a user's identity is compromised, it can have serious repercussions in various security applications. User anonymity is a characteristic of authentication procedures where it is desirable that communicating users' identities remain hidden. When communicating over public channels, the original communicating User cannot be identified by any adversary for security reasons.

Eavesdropping is a security hazard in which intruders or hackers secretly overhear conversations between two participants. Communication that has been intercepted can be utilized to identify weaknesses and gather crucial data. The User always transmits new encrypted information via the public channel, making it impossible for an adversary to initiate an eavesdropping assault.

Due to the unlawful fog server's lack of registration with the cloud server and inability to connect with a legitimate user, the attacker cannot obtain information about a legitimate user through the illegal fog server.

An impersonation attack occurs when a hacker tries to communicate with the fog server and cloud server while posing as a legitimate user. The cloud server will confirm the User's identity in the suggested system, preventing impersonation attacks.

6. Conclusion and future work

Due to its critical uses in businesses, the private sector, home appliances, etc., cloud-Fog applications have recently gained popularity among researchers. This work suggests a safe, lightweight multifactor authentication system for the user-fog-cloud environment. Multi-factor authentication is a secure and convenient user authentication method that can identify which users are authorized to utilize cloud services and which are not. Furthermore, the suggested method offers greater efficiency, safety and less computational cost than earlier methods. Therefore, it may be appropriate for a real-world cloud-fog computing environment because it is safer and lighter than the preceding systems. In the future, the authentication method will be extended with the blockchain with ECC-based multi-factor authentication and secure data communication.

Acknowledgement

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Kumar V, Jangirala S, Ahmad M. An efficient mutual authentication framework for healthcare system in cloud computing. Journal of medical systems. 2018;42(8):1-25.

[2] Mukherjee M, Shu L, Wang D. Survey of fog computing: fundamental, network applications, and research challenges. IEEE Communications Surveys & Tutorials. 2018;20(3):1826-1857.

[3] Neware R, Shrawankar U. Fog computing architecture, applications and security issues. International Journal of Fog Computing. 2020;3(1):75-105.

[4] Sarkar S, Misra, S. Theoretical modelling of fog computing: a green computing paradigm to support IoT applications. Iet Networks. 2016;5(2):23-29.

[5] Ali HS, Sridevi R. Credential-based authentication mechanism for IoT devices in fog-cloud computing. ICT Analysis and Applications, Springer. 2022;307-318

[6] Sudha MN, Rajendiran M, Specht M, Reddy KS, Sugumaran S. A low-area design of two-factor authentication using DIES and SBI for IoT security. The Journal of Supercomputing. 2022;78(3):4503-4525.

[7] Juneja K. An XML transformed method to improve effectiveness of graphical password authentication. Journal of King Saud University-Computer and Information Sciences. 2020;32(1):11-23.

[8] Wang X, Yan Z, Zhang R, Zhang P. Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications. 2021;188.

[9] Ghahramani M, Javidan R, Shojafar M. A secure biometric-based authentication protocol for global mobility networks in smart cities. The Journal of supercomputing. 2020;76:8729-8755.

[10] Lee YK, Jeong J. Securing biometric authentication system using blockchain. ICT Express. 2021; 7:322–326.

[11] Khaskheli GM, Sherbaz M, Shaikh UR. A comparative usability study of single-factor and two-factor authentication. Tropical Scientific Journal. 2022;1(1):17-27.

[12] Sadri MJ, Asaar MR. An anonymous two-factor authentication protocol for IoT-based applications. Computer Networks. 2021;199.

[13] Alsahlani AY F, Popa A. LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. Journal of Network and Computer Applications, 2021;192

[14] Weng CY, Li CT, Chen CL, Lee CC, Deng YY. A lightweight anonymous authentication and secure communication scheme for fog computing services. IEEE Access. 2021;9:145522-145537.

[15] Atiewi S, Al-Rahayfeh A, Almiani M, Yussof S, Alfandi O, Abugabah A, Jararweh Y. Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. IEEE Access. 2020;8:113498-113511.

[16] Liu W, Wang X, Peng W. Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things. IEEE Access. 2020;8:8754-8767.

[17] Kalaria R, Kayes ASM, Rahayu W, Pardede E. A secure mutual authentication approach to fog computing environment. Computers & Security. 2021;111.

[18] Khalid H, Hashim SJ, Ahmad SMS, Hashim F, Chaudhary MA. SELAMAT: a new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems. Sensors. 2021; 21(4).

[19] Prabakaran D, Ramachandran S. Multi-factor authentication for secured financial transactions in cloud environment. CMC-Computers. Materials & Continua. 2022;70(1):1781-1798.

[20] Deebak BD, Fadi AT. Lightweight authentication for IoT/cloud-based forensics in intelligent data computing. Future generation computer systems. 2021;116:406-425.

[21] Kaur D, Kumar D. Cryptanalysis and improvement of a two-factor user authentication scheme for smart home. Journal of Information Security and Applications. 2021;58.

[22] Yu S, Jho N, Park Y. Lightweight three-factor-based privacy-preserving authentication scheme for IoT-enabled smart homes. IEEE Access. 2021;9:126186-126197.

[23] Ali Z, Hossain MS, Muhammad G, Ullah I, Abachi H, Alamri A. Edge-centric multimodal authentication system using encrypted biometric templates. Future Generation Computer Systems. 2018;85:76-87.

[24] Dhillon PK, Kalra S. Multi-factor user authentication scheme for IoT-based healthcare services. Journal of Reliable Intelligent Environments. 2018;4:141-160.

[25] Mostafa A, Lee SJ, Peker YK. Physical unclonable function and hashing are all you need to mutually authenticate IoT devices. Sensors. 2020;20(16).

[26] Alshawish I, Al-Haj A. An efficient mutual authentication scheme for IoT systems. The Journal of Supercomputing. 2022;1-32.

[27] Liu D, Li Z, Wang C, Ren Y. Enabling secure mutual authentication and storage checking in cloud-assisted IoT. Mathematical Biosciences and Engineering. 2022;19(11):11034-11046.

[28] Agrahari AK, Varma S, Venkatesan S. Two factor authentication protocol for IoT based healthcare monitoring system. Journal of Ambient Intelligence and Humanized Computing. 2022;1-18.

[29] Dai C, Xu Z. A secure three-factor authentication scheme for multi-gateway wireless sensor networks based on elliptic curve cryptography. Ad Hoc Networks. 2022;127.

[30] Sahoo SS, Mohanty S, Majhi B. An efficient three-factor user authentication scheme for industrial wireless sensor network with fog computing. International Journal of Communication Systems. 2022;35(3).

[31] Singh S, Chaurasiya VK. Mutual authentication framework using fog computing in healthcare. Multimedia Tools and Applications. 2022;81(22):31977-32003.

[32] Zou S, Cao Q, Wang C, Huang Z, Xu G. A robust two-factor user authentication scheme-based ECC for smart home in IoT. IEEE Systems Journal. 2021;16(3):4938-4949.

[33] Masud M, Gaba GS, Choudhary K, Hossain MS, Alhamid MF, Muhammad G. Lightweight and anonymity-preserving user authentication scheme for

IoT-based healthcare. IEEE Internet of Things Journal. 2021;9(4):2649-2656.

[34] Nikravan M, Reza A. A multi-factor user authentication and key agreement protocol based on bilinear pairing for the Internet of Things. Wireless Personal Communication. 2020;111(1):463–494.

[35] Wu TY, Wang T, Lee YQ, Zheng W, Kumari S, Kumar S. Improved authenticated key agreement scheme for fog-driven IoT healthcare system. Security and Communication Network. 2021;1–16.

[36] Chen CM, Chen Z, Kumari S, Lin MC. LAP-IoHT: A lightweight authentication protocol for the internet of health things. Sensors. 2022;22(14).

[37] Yu S, Park Y. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. IEEE Internet of Things Journal. 2022;9(20):20214-20228.

[38] Ayman Mohamed Mostafa 1,* , Mohamed Ezz 2 , Murtada K. Elbashir 1 , Meshrif Alruily 2 , Eslam Hamouda 2 , Mohamed Alsarhani 2 and Wael Said 3, Strengthening Cloud Security: An Innovative Multi-Factor Appl. Sci. 2023, 13(19), 10871; https://doi.org/10.3390/app131910871

[39] Junhui Zhao a b, Fanwei Huang a, Huanhuan Hu a, Longxia Liao a, Dongming Wang c, Lisheng Fan d User security authentication protocol in multi gateway scenarios of the Internet of Things Ad Hoc Networks Volume 156, 1 April 2024, 103427 https://doi.org/10.1016/j.adhoc.2024.103427 February 2024

AUTHORS:

K.Shanthi received Master in Computer Application with first Class in 2010, Masters in Philosophy in 2017 and currently pursuing PhD in PRIST University. She is working as Assistant Professor in Department of Computer Science in Shri Krishnaswamy College, Chennai. She has published many papers at national /international Journals and Conferences in the areas of Cloud Security. She published three books and own a patent in IOT.

R.Maruthi completed her MCA, M.Phil anPh.D from Mother Teresa Women's University, currently working as an associate Professor & HoD , in the Department of Computer Applications , Hindustan Institute of Technology and Science, Chennai, having 21 years of experience in teaching and research in various reputed institutes like Velammal Engineering College, SSN college of Engineering etc., published 40+ papers in International conferences and Journal

Appendix I

S.No.	Abbreviation	Description
1	CS	Cloud Server
2	ECC	Elliptical Curve Cryptography
3	FS	Fog Server
4	IoT	Internet of Things
5	PIN	Personal Identification Number
6	PUF	Physical Unclonable Functions
7	PWD	Password
8	SC	Secret Code
9	UID	User Identity
10	VPN	Virtual Private Networks
11	WSN	Wireless Sensor Network
12	XOR	bitwise exclusive OR operation