Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.032553

ARTICLE

A Secure and Efficient Information Authentication Scheme for E-Healthcare System

Naveed Khan[1], Jianbiao Zhang[1,*], Ghulam Ali Mallah[2] and Shehzad Ashraf Chaudhry[3]

[1]Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China

[2]Department of Computer Science, Shah Abdul Latif University, Khairpur, 66111, Pakistan

[3]Department of Computer Engineering, Faculty of Engineering Architecture, Nisantasi University, Istanbul, 34398, Turkey

*Corresponding Author: Jianbiao Zhang. Email: zjb@bjut.edu.cn

Received: 22 May 2022 Accepted: 12 July 2022 Published: 08 October 2023

ABSTRACT

The mobile cellular network provides internet connectivity for heterogeneous Internet of Things (IoT) devices. The cellular network consists of several towers installed at appropriate locations within a smart city. These cellular towers can be utilized for various tasks, such as e-healthcare systems, smart city surveillance, traffic monitoring, infrastructure surveillance, or sidewalk checking. Security is a primary concern in data broadcasting, particularly authentication, because the strength of a cellular network's signal is much higher frequency than the associated one, and their frequencies can sometimes be aligned, posing a significant challenge. As a result, that requires attention, and without information authentication, such a barrier cannot be removed. So, we design a secure and efficient information authentication scheme for IoT-enabled devices to mitigate the flaws in the e-healthcare system. The proposed protocol security shall check formally using the Real-or-Random (ROR) model, simulated using ProVerif2.03, and informally using pragmatic discussion. In comparison, the performance phenomenon shall tackle by the already result available in the MIRACL cryptographic lab.

KEYWORDS

IoT-enable device; e-healthcare; authentication; edge computing

1 Introduction

The IoT-enabled devices can be found in various domains, such as the healthcare system, cities, factories, homes, the Internet of Drones (IoD), and many more [1,2]. By 2025, IoT devices usages will have increased, and about 75 billion devices will be connected to the internet [3]. As a result, the e-healthcare market will expand by 16 percent between 2020 to 2027, while the current volume is 143.6 billion USD [4]. In an e-healthcare system, medical signals are used to monitor patients' health activities. These signals are one-dimensional (1D) and two-dimensional (2D) signals, such as blood pressure, electrocardiograms, electromyograms, electroglottograph, body temperature, and electroencephalograms. Although, traditional hospital management monitors patient activities manually. Therefore, it is inefficient and can lead to medication errors. The medication error can

be fatal and lead to patient harm. Furthermore, according to World Health Organization (WHO), medication error costs humans around 42 billion USD annually [5].

In contrast, edge computing plays a crucial role in medical emergencies and communication delays. Therefore, edge computing benefits the e-healthcare system in terms of real-time data collection, processing, and analyzation. Moreover, the edge architecture provides reliability and low latency in distributive applications such as IoT-enable sensors in e-healthcare. Although, the initial goal of edge computing was to reduce bandwidth costs. However, with the advancement of wireless networks such as 5G and even researchers working on 6G networks, edge computing will be able to support real-time applications such as self-driving cars, robotics, video processing, and medical enable IoT devices, to name a few. Edge computing is a distributed computing topology in which data storage and computation are located close to the devices in order to reduce latency. Latency is critical in the e-healthcare system because high latency can harm a patient's life. In contrast, low latency can sometimes save their lives [6].

Furthermore, IoT-enabled devices facilitate communication between doctors and patients. Doctors place these IoT-enabled devices on patients' bodies to monitor their health activities. However, IoT-enabled devices improve doctor-patient interaction but generate massive amounts of data that must be carefully stored and processed at edge computing. Therefore, using IoT-enabled devices in the medical field is advantageous because it eliminates the need for medical personnel to manually manage patient data. Although, these IoT-enabled devices are vulnerable to security threats due to their resource and energy limitations. Because of this, it is impossible to eliminate these vulnerabilities without strong authentication. Therefore, several different e-healthcare authentications and key agreement schemes have been implemented. However, these schemes [7–9] suffer from eavesdropping and forgery attacks. Furthermore, we identified security flaws in the scheme [10] and found out that the scheme suffers from different attacks such as spoofing, masquerading, and impersonation.

1.1 Motivation and Contribution

For academics, e-healthcare is a sensitive research area. Furthermore, any flaws in the protocol could result in the patients' fatal accidents. As a result, we take advantage of the opportunity to propose a secure and efficient authentication scheme for e-healthcare that reduces complexity while improving security over existing schemes. Our protocol is efficient and lightweight for IoT-enabled devices because we only use the XOR and hash functions. Recently author [10] proposed an authentication scheme for the healthcare system. According to [10], the scheme achieves mutual authentication, untraceability, forward secrecy, and resistance to replay and desynchronization attacks. However, careful examination reveals that the scheme is vulnerable to spoofing, masquerading, and impersonation attacks. In the scheme [10], when the attacker copies $M_4 = \{X, A_n\}$ and transmits it again later, the adversary ($\mathcal{A}$) can easily spoof the reader's radio frequency identification (RFID) because for each session, the same message is transmitted over the public network channel. Furthermore, an attacker may also modify it to masquerade as a legitimate peer. Similarly, for $M_5 = \{Y, A_{RI}, X, A_n\}$, the attacker can easily impersonate the server for a wrong decision due to its static nature. Therefore, the scheme suffers from spoofing, impersonation, and masquerading attacks. The following is our primary contribution:

- We identified security vulnerabilities in [10] and rectified them using our proposed scheme, which is lightweight and efficient because it utilizes only XOR and a hash function.

- Despite achieving some security objectives, the protocol [10] came at a high cost in terms of communication and computation. Since communication and computation costs are rising, we proposed a low-cost solution to address this issue.
- The security of our proposed protocol is formally analyzed through the ROR model [11] and ProVerif2.03 [12]. Using ProVerif and ROR model, we demonstrated that our proposed scheme is secure against replay and man in the middle attacks while securely providing mutual authentication and session key security.
- In the informal security analysis section, our proposed scheme demonstrates that our protocol is secure against various attacks.
- Our proposed protocol outperforms existing state-of-the-art schemes regarding communication, computation costs, and security. Among many other applications, the scheme can realize a smart city environment.

1.2 Threat Model

We extended the famous threat model developed by Dolev and Yao (DY), also called the DY model [13]. We are adopting a solid adversary $\mathcal{A}$. According to the DY model, any danger to the system must be examined and analyzed before operationalizing it in real-world environments. We also consider the adversary model of Cannetti and Knawezk (CK) model [14] and utilized [15] for a more solid adversary. The CK model is the most used in authentication and key exchange protocols. In the DY model, the $\mathcal{A}$ delivers the message, while in the CK model, the $\mathcal{A}$ can also compromise the session key and secret key.

Furthermore, IoT-enabled devices or sensor nodes can be accessed by the $\mathcal{A}$ physically. Thus, the $\mathcal{A}$ will try to extract secret information from it. Further, the communication between IoT-enable devices or sensor nodes and edge computing can be intercepted by the $\mathcal{A}$. Sensor nodes are connected to the edge node using a wireless network; therefore, the $\mathcal{A}$ can access open channel data and modify, delete, or insert it. The $\mathcal{A}$ can monitor the data between the IoT-enable sensor node and the user. The $\mathcal{A}$ can pretend to be a legal user to the edge server and launch Man-In-The-Middle (MITM) to masquerade and impersonate attacks.

1.3 System Model

Our system model consists of patients with IoT-enable sensor nodes, medical staff, edge server, and registration server, as shown in Fig. 1. First, the IoT-enable sensor nodes and users need to register themself with the registration server. After that, medical staff can monitor patients' activities in real-time using these IoT-enabled devices, whereas the edge server reduces latency. The registration server and edge server are the trusted authorities in our proposed scheme. The registration server is in charge of registering users and IoT-enabled devices. Finally, our system model detailed explanation is given in the proposed scheme.

1.4 Paper Organization

The rest of the article is structured as follows: Section 2 describes the literature review in detail. Additionally, Section 3 contains the proposed scenario. Then, in Section 4, we examine the proposed framework's security, Section 5 discusses informal security analysis, and Section 6 conducts a performance analysis. Finally, Section 7 concludes the paper.

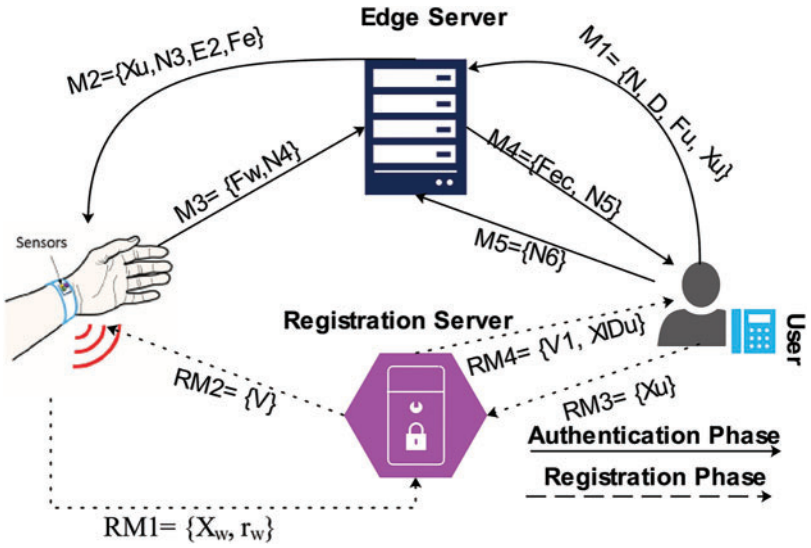

Figure 1: System model

2 Related Work

There are numerous advantages to having an e-healthcare system. Despite the benefits, there are multiple concerns, the most noteworthy of which is outsourcing data storage. As a result, it creates the possibility of unlawful physical access. However, encryption is the most effective method for preventing unauthorized access to outsourced data. Encrypting and storing data in the cloud can prevent malicious users or cloud service providers from accessing it [16]. These encryption techniques, however, could be improved. If an attacker obtains access to a secret key, the data must be protected from unauthorized access.

However, IoT-enabled devices have resource and energy limitations. As a result, these devices are susceptible to a wide range of security risks. In addition, traditional cryptographic protocols do not perform well on IoT-enabled devices due to resource and energy constraints. These devices are vulnerable to both passive and active security threats, and the attacks can be launched from inside or outside the network. These security breaches impede communication. As a result, Denial-of-Service (DoS) and Sybil attacks are potentially more dangerous because they deplete the device's resources and network bandwidth. Many researchers attempt to create security protocols that address authentication, confidentiality, and integrity. Authentication is one of the most visible aspects that ensures user identity and verifies it in order to protect data from malicious users. This section provides a brief overview and analysis of the existing schemes in e-healthcare systems.

The authors [7] proposed an authentication scheme for RFID-based IoT devices to prevent replay and data disclosure attacks. Their scheme also provides anonymity. However, their scheme has security flaws, such as the scheme cannot be resilient to impersonation, eavesdropping, and forgery attacks. Further, the authors [17] proposed an authentication scheme based on Chaotic-Map and Chebyshev. However, it provides better anonymity but suffers from offline password guessing, password disclosure, and impersonation attacks. Finally, in 2018, the authors [18] proposed a lightweight privacy preservation scheme using Physically Unclonable Functions (PUFs). However, their scheme also has security flaws such as perfect forward secrecy and heave storage and computation cost. Moreover, the schemes [8,9] cannot resist DoS, eavesdropping, and forgery attacks.

The authors [19] proposed an Elliptic Curve Cryptography (ECC) authentication protocol for the healthcare system. Nevertheless, their scheme suffers from password guessing and impersonation attacks. However, An authentication scheme based on Hash-based RFID was proposed [20]. Unfortunately, the scheme cannot resist forgery, privileged insiders, and Denial of Service (DoS) attacks. Furthermore, the scheme [21] cannot provide resistance against insider, MITM, session key security, and session-specific temporary information attacks. While the scheme [22] also cannot resist insider, offline password guessing, stolen smartcard, and session key security attacks. Furthermore, The scheme [23] cannot provide anonymity, insider, replay, and MITM attacks. The paper [24] proposed a high optimal path channel triggering scheme that offers data preservation and privacy with minimal network resources.

Elliptic Curve Cryptography (ECC) and integrated with a biometric authentication scheme were proposed by [25]. However, the scheme is vulnerable to machine learning [26] attacks and cannot provide perfect forward secrecy and perfect backward secrecy. The authors [27] proposed a certificateless authentication protocol, but their scheme cannot resist modification and impersonation attacks [28]. Another scheme was proposed in [29], which does not provide message integrity and physical security. An Intrusion Detection System (IDS) scheme was proposed in [30–32] to detect Botnet, DoS, distributed denial of service (DDoS), Wireless Body Area Networks (WBAN), and many more attacks, but these methods consume time and the accuracy rate is also low. The scheme [33] failed to resist insider attacks and could not provide session key security and untraceability.

On the other hand, the approach [34] did not provide traceability or mutual authentication, as the name suggests. As a result, researchers [23,35] presented a three-factor authentication technique based on ECC to ensure perfect forward secrecy. However, these systems do not guarantee absolute forward secrecy, user anonymity, or the ability to withstand replay attacks. Over the cost of computation, the protocol [36] provides a security feature that is advantageous. The authors proposed a lightweight authentication technique in [37], but the key generation time was highly elongated. As a result, it is in conflict with the characteristic of a lightweight scenario. Blockchain technology has recently garnered the interest of healthcare researchers. However, the blockchain has issues with accessing medical records [38].

Furthermore, a scheme [39] was proposed using symmetric en/decryption, hash function, and chaotic maps that provide authentication and key agreements for multi-server environments. However, according to [40], the scheme is prone to offline password guessing attacks and biometric and smart card leaks. Moreover, the scheme [41] is vulnerable to DoS attacks. Furthermore, it cannot provide perfect forward secrecy and provision of smartcard revocation. In contrast, the scheme cannot resist anonymity, user impersonation, mutual authentication, and server impersonation attacks. Therefore, we propose a secure and efficient authentication protocol for e-healthcare in edge computing to improve the security vulnerabilities of the existing scheme and especially the protocol proposed in [10].

3 Proposed Scheme

We proposed a secure and efficient information authentication protocol for an IoT-enable device in an e-healthcare system to improve the flaws in the protocol [10]. Our proposed approach is divided into four phases: setup, registration, login and authentication, and password changing. Detailed notation and their description are shown in Table 1.

Table 1: Notations and description

Notation	Description
ID_u	User identity
ID_e	Edge server identity
ID_w	IoT-enable sensor node identity
PW_u	User password
r_u, r_{u1}	User random numbers
r_w, r_{w1}	IoT-enable sensor node random numbers
r_e	The random number of an edge server
r_{rs}	The random number of the registration server
SK_{rs}	Registration server secret key
V	Edge server and IoT-enable sensor node shared secret key
V_1	User and edge server shared secret key
S_K	Session key
h(.)	One-way hash function
$\oplus$	XOR
$\|\|$	Concatenation

3.1 Setup Phase

The registration server generates the secret key SKrs in our proposed protocol. The edge server and IoT-enable sensor node both have their own unique identities, ID_e and ID_w, and a secret user key, PKu.

3.2 Registration Phase

Our proposed scheme registration phase comprises of two-part. In the first portion, we will register the IoT-enable sensor node with the registration server, while in the second phase, we will register the user with the registration server. The process is under:

3.2.1 IoT-Enable Sensor Node Registration Phase

i. In this step, the IoT-enable sensor node selects identity ID_u and generates a random number r_w to calculate $X_w = h(ID_u||r_w)$. The IoT-enable sensor node sends $RM1 = \{X_w, r_w\}$ toward the registration server.
ii. Upon receiving $RM1 = \{X_w, r_w\}$ from IoT-enable sensor node, the registration server generates random number r_{rs} to computes $V = h(X_w||r_{rs}||SK_{rs})$ and store $\{X_w, V, r_{rs}\}$ in edge server database. After that the registration server send $RM2 = \{V\}$ to IoT-enable sensor node over secure channel.
iii. The IoT-enable sensor node further calculates $S_1 = h(ID_w||SK_w) \oplus r_w$, $S_2 = h(r_w||SK_w) \oplus V$ and Store $\{X_w, S_1, S_2\}$ in memory and the procedure as shown in Table 2.

Table 2: IoT-enable sensor node registration

IoT-enable sensor node		Registration Server (RS)
Select identity ID_w		
Generate random number r_w		
Calculate:		
$X_w = h(ID_w\|\|r_w)$		
	$RM1 \underset{\rightarrow}{=} \{X_w, r_w\}$	
		Generate random number r_{rs}
		Computes:
		$V = h(X_w\|\|r_{rs}\|\|SK_{rs})$
		Store $\{X_w, V, r_{rs}\}$ in edge server database
	$RM2 \underset{\leftarrow}{=} \{V\}$	
Computes:		
$S_1 = h(ID_w\|\|SK_w) \oplus r_w$		
$S_2 = h(r_w\|\|SK_w) \oplus V$		
Store $\{X_w, S_1, S_2\}$ in memory		

3.2.2 User Registration Phase

In this section, the user registers with the registration server in our proposed protocol.

i. The user selects identity ID_u, generates a random number r_u and computes $X_u = h(ID_u||r_u)$, and sends $RM3 = \{X_u\}$ toward the registration server over a secure channel.
ii. After receiving $RM3 = \{X_w\}$ from user, the registration server calculates $V_1 = h(X_u||SK_{rs}||r_{rs})$, $XID_u = h(X_u||V_1)$ and store $\{X_u, XIDu, V_1\}$ in edge server database. After computation the registration server send $RM4 = \{V_1, XIDu\}$ to user over secure channel.
iii. The user chooses a password PW_u and computes $HPW_u = h(PW_u||r_u)$, $B_1 = h(ID_u||PW_u) \oplus r_u$, $B_2 = h(ID_u||PW_u||r_u||HPW_u)$, $B_3 = h(HPW_u||r_u) \oplus XID_u$, $B_4 = h(HPW_u||XID_u) \oplus V_1$ and Store $\{X_u, B_1, B_2, B_3, B_4\}$ and the procedure is illustrated in Table 2.

3.3 Login and Authentication Phase

i. The user input identity ID_u and password PW_u and computes, $r_u = h(ID_u||PW_u) \oplus B_1$, $HPW_u = h(PWu||r_u)$, $B_2^* = h(ID_u||PW_u||r_u||HPW_u)$. The user check $B_2^{*}? = B_2$ and if it corrects then proceed further otherwise terminate connection. The user generates random number r_{u1} and calculates $XID_u = h(HPW_u||r_u) \oplus B_3$, $V_1 = h(HPW_u||XID_u) \oplus B_4$, $N = h(X_u||XID_u||V_1) \oplus (X_u||r_{u1})$, $D = h(ID_u||r_u) \oplus h(V_1||r_{u1})$, $F_u = h(X_u||XID_u||r_{u1}||X_w||V_1)$. After calculations the user sends $M1 = \{N, D, F_e, X_u\}$ towards edge server.
ii. The edge server extracts XID_u and V_1 as per the X_u and calculates $(X_w^*||r_{u1}^*) = h(X_u||XID_u||V_1)$, $F_u^* = h(X_u||XID_u||r_{u1}^*||X_w^*||V_1)$ and Check $F_u^{*}? = F_u$, if edge authenticate user then proceed further otherwise terminate connection. The edge server selects random number r_e and further calculates $N_2 = h(r_e||r_{u1})$, $N_3 = h(X_w||V||r_w) \oplus N_2$, $h(ID_u||r_{u1}) = E_1 \oplus h(V_1||r_{u1})$, $E_2 = (h(ID_u||r_{u1})||h(ID_e||r_e)) \oplus h(V||r_w)$, and $F_e = h(X_u||N_2||V)$. After computation the edge server send $M2 = \{X_w, N_1, E_2, F_e\}$ to IoT-enable sensor node.

iii. The IoT-enable sensor node calculates $r_w = h(ID_w||PK_w)$, $V = h(r_w||PK_w) \oplus S_2$, $N_2^* = h(X_w||V||r_w) \oplus N_3$, $F_e^* = h(X_u||N_2^*||V)$. The IoT-enable sensor node authenticates edge server through $Fe^*? = F_e$, if correct then proceed further otherwise terminate connection. The IoT-enable sensor node generates random number r_{u1} and computes $(h(ID_u||r_{u1})||h(ID_e||r_e)) = E_2 \oplus h(V||r_w)$, $S_K = h(h(ID_u||r_{u1})||h(ID_e||r_e)||h(ID_w||r_e)$, $N_4 = h(X_w||V||r_w) \oplus h(ID_w||r_{w1})$, $F_w = h(X_u||X_w||N_2^*||h(ID_w||r_{w1})||V)$ and send M3 = $\{F_w, N_4\}$ to edge server back.

iv. The edge server calculates $h(ID_w||r_{w1}) = h(X_w||V||r_w) \oplus N_4$, $F_w^* = h(X_u||X_w||N_2||h(ID_w||r_{w1}||V)$ and check $F_w^*? = F_w$. If it corrects the proceed further otherwise terminate connection. The edge server further calculates $S_K = h(h(ID_u||r_{u1})||h(ID_e||r_e)||h(ID_w||r_{w1})$, $X_u^{new} = h(X_u||r_{u1})$, $XID_u^{new} = h(X_u^{new}||V)$, $N_5 = h(XID_u||r_{u1}) \oplus (h(ID_e||r_e)||h(ID_w||r_{w1})||X_u^{new}$, and $F_{ec} = h(X_u||r_{u1})||h(ID_e||r_e)||h(ID_w||r_{w1})||X_u^{new}||V)$. The edge server store $\{X_u^{new}, XID_u^{new}\}$ and send M4 = $\{F_{ec}, N_5\}$ towards user.

v. The user calculates $X_u^{new} = h(X_u||r_{u1})$, $(h(ID_e||r_e)||h(ID_w||r_{w1})||X_u^{new} = h(XID_u||r_{u1}) \oplus N_5$, and $F_{ec}^* = h(Xu||r_{u1})||h(ID_e||r_e)||h(ID_w||r_{w1})||X_u^{new}||V)$. The user Check $F_{ec}^*? = F_{ec}$ and if it is correct then proceed further otherwise terminate connection. The user further calculates $S_K = h(h(ID_u||r_u)||h(ID_e||r_e)||h(ID_w||r_{w1})$, $XID_u^{new} = h(X_u^{new}||V)$, $B_3^{new} = h(XID_u^{new}||HPW_u) \oplus XID_u^{new}$, and $B_4^{new} = h(XID_u^{new}||HPW_u) \oplus V_1$. The user update $\{B_3^{new}, B_4^{new}, X_u^{new}\}$ and compute $N_6 = h(S_K||X_u^{new})$. The user sends M5 = $\{N_6\}$ towards edge server.

vi. The edge server $N_6^* = h(S_K||X_u^{new})$ and check $N_6^*? = N_6$. After calculations, the edge server deletes $\{XID_u, X_u\}$ Table 3. Further details are given in Table 4.

Table 3: User registration

User (u)		Registration Server (RS)
Select identity ID_u		
Generate random number r_u		
Computes:		
$X_u = h(ID_u||r_u)$		
	$RM3 = \{X_u\} \rightarrow$	
		Computes:
		$V_1 = h(X_u||SK_{rs}||r_{rs})$
		$XID_u = h(X_u||V_1)$
		Store $\{X_u, XID_u, V_1\}$ in edge server database
	$RM4 = \{V_1, XID_u\} \leftarrow$	
Choose password		
PW_u		
Computes:		
$HPW_u = h(PW_u||r_u)$		
$B_1 = h(ID_u||PW_u) \oplus r_u$		
$B_2 = h(ID_u||PW_u||r_u||HPW_u)$		
$B_3 = h(HPW_u||r_u) \oplus XID_u$		
$B_4 = h(HPW_u||XID_u) \oplus V_1$		
Store $\{X_u, B_1, B_2, B_3, B_4\}$		

Table 4: Login and authentication phase

User	Edge server	IoT-enable sensor node
Input ID_u, PW_u Calculate: $r_u = h(ID_u\|\|PW_u) \oplus B_1$ $HPW_u = h(PW_u\|\|r_u)$ $B_2^* = h(ID_u\|\|PW_u\|\|r_u\|\|HPW_u)$ Check $B_2^*? = B_2$ Generate random number r_{u1} Computes: $XID_u = h(HPW_u\|\|r_u) \oplus B_3$ $V_1 = h(HPW_u\|\|XID_u) \oplus B_4$ $N = h(X_u\|\|XID_u\|\|V_1) \oplus (X_u\|\|r_{u1})$ $D = h(ID_u\|\|r_u) \oplus h(V_1\|\|r_{u1})$ $F_u = h(X_u\|\|XID_u\|\|r_{u1}\|\|X_w\|\|V_1)$ $M1 = \{N, D, F_u, X_u\} \rightarrow$	Corresponding to X_u, the XID_u and V_1 are retrieved $(X_w^*\|\|r_{u1}^*) = h(X_u\|\|XID_u\|\|V_1)$ $F_u^* = h(X_u\|\|XID_u\|\|r_{u1}^*\|\|X_w^*\|\|V_1)$ Check $F_u^*? = F_u$ Generate random number r_e Calculates: $N_2 = h(r_e\|\|r_{u1})$ $N_3 = h(X_w\|\|V\|\|r_w) \oplus N_2$ $h(ID_u\|\|r_{u1}) = E_1 \oplus h(V_1\|\|r_{u1})$ $E_2 = (h(ID_u\|\|r_{u1}) \|\|h(ID_e\|\|r_e)) \oplus h(V\|\|r_w)$ $F_e = h(X_u\|\|N_2\|\|V)$ $M2 = \{X_u, N_3, E_2, Fe\} \rightarrow$	Calculates: $r_w = h(ID_w\|\|PK_w)$ $V = h(r_w\|\|PK_w) \oplus S_2$ $N_2^* = h(X_w\|\|V\|\|r_w) \oplus N_3$ $F_e^* = h(X_u\|\|N_2^*\|\|V)$ Check $F_e^*? = F_e$ Generate random number r_{w1} Calculates: $(h(ID_u\|\|r_{u1}) \|\|h(ID_e\|\|r_e)) = E_2 \oplus h(V\|\|r_w)$ $S_K = h(h(ID_u\|\|r_{u1}) \|\|h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_e)$ $N_4 = h(X_w\|\|V\|\|r_w) \oplus h(ID_w\|\|r_{w1})$ $F_w = h(X_u\|\|X_w\|\|N_2^*\|\|h(ID_w\|\|r_{w1}) \|\|V)$ $M3 = \{F_w, N_4\} \leftarrow$

(Continued)

Table 4 (continued)

User	Edge server	IoT-enable sensor node
	$h(ID_w\|\|r_{w1}) = h(X_w\|\|V\|\|r_w) \oplus N_4$ $F_w^* = h(X_u\|\|X_w\|\|N_2\|\|h(ID_w\|\|r_{w1}\|\|V)$ Check $F_w^*? = F_w$ Computes: $S_K = h(h(ID_u\|\|r_{u1}) \|\|h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_{w1})$ $X_u^{new} = h(X_u\|\|r_{u1})$ $XID_u^{new} = h(X_u^{new}\|\|V)$ $N_5 = h(XID_u\|\|r_{u1}) \oplus (h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_{w1}) \|\|X_u^{new}$ $F_{ec} = h(X_u\|\|r_{u1}) \|\|h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_{w1}) \|\|X_u^{new}\|\|V)$ Store $\{X_u^{new}, XID_u^{new}\}$ in edge server	
	$M4 = \{F_{ec}, N_5\}$ ←	
Calculates: $X_u^{new} = h(X_u\|\|r_{u1})$ $(h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_{w1}) \|\|X_u^{new} = h(XID_u\|\|r_{u1}) \oplus N_5$ $F_{ec}^* = h(X_u\|\|r_{u1}) \|\|h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_{w1}) \|\|X_u^{new}\|\|V)$ Check $F_{ec}^*? = F_{ec}$ Calculates: $S_K = h(h(ID_u\|\|r_u) \|\|h(ID_e\|\|r_e) \|\|h(ID_w\|\|r_{w1})$ $XID_u^{new} = h(X_u^{new}\|\|V)$ $B_3^{new} = h(XID_u^{new}\|\|HPW_u) \oplus XID_u^{new}$ $B_4^{new} = h(XID_u^{new}\|\|HPW_u) \oplus V_1$ Updates $\{B_3^{new}, B_4^{new}, X_u^{new}\}$ Computes: $N_6 = h(S_K\|\|X_u^{new})$		
$M5 = \{N_6\}$ →		
	$N_6^* = h(S_K\|\|X_u^{new})$ Check $N_6^*? = N_6$ Delete $\{XID_u, X_u\}$	

3.4 Password Change Phase

i. The user enters their identity ID_u and password PW_u.
ii. After input ID_u and PW_u, the device computes $HPW_u = h(PW_u||r_u)$, $B_1 = h(ID_u||PW_u) \oplus r_u$, $B_2 = h(ID_u||PW_u||r_u||HPW_u)$, $B_3 = h(HPW_u||r_u) \oplus XID_u$, $B_4 = h(HPW_u||XID_u) \oplus V_1$, $r_u = h(ID_u||PW_u) \oplus B_1$, and $B_2^* = h(ID_u||PW_u||r_u||HPW_u)$. Then check $B_2^*? = B_2$ and proceed further if correct otherwise terminate connection.
iii. The user inputs a new password PW_u^{new}.
iv. After input new password then update the values of $HPW_u^* = h(PW_u^{new}||r_u)$, $B_1^* = h(ID_u||PW_u^{new}) \oplus r_u$, $B_2^{**} = h(ID_u||PW_u^{new}||r_u||HPW_u^*)$, $B_3^* = h(HPW_u^*||r_u) \oplus XID_u$, $B_4^* = h(HPW_u^*||XID_u) \oplus V_1$, $r_u^* = h(ID_u||PW_u^{new}) \oplus B_1^*$, $B_2^{***} = h(ID_u||PW_u^{new}||r_u||HPW_u^*)$ and update $\{HPW_u^*, B_1^*, B_2^{**}, B_3^*, B_4^* B_2^{***}\}$.

4 Security Analysis

This section analyzed and critiqued the proposed scheme's security using two distinct methodologies. Firstly, we utilized Real-or-Random (ROR) model to determine the security of our session key SK. Furthermore, we used the ProVerif simulation toolkit to demonstrate that the session secret is secure. Finally, further details are given below.

4.1 Formal Security Analysis Using Real-or-Random (ROR) Model

We used the ROR model [11] to demonstrate our proposed scheme's session key security SK. In our proposed scheme login and authentication phase, we have three participants P^t, user P^t_u, edge server P^t_e, and IoT-enable sensor node P^t_w. The $\mathcal{A}$ has the ability to intercept, manipulate, and eavesdrop on data delivered across an unsecured connection. The $\mathcal{A}$ may attack actively or passively by executing various queries outlined in the ROR model, including CorruptedMD, Executive, Send, Reveal, and Test queries. The exact instructions for these queries are included below:

- CorruptedMD (P^t_u): The $\mathcal{A}$ can obtain secret information stored on the user side.
- Executive (P^t_u, P^t_e, P^t_w): The $\mathcal{A}$ can capture transmitted data over an insecure channel among users, edge servers, and IoT-enable sensor nodes.
- Send (P^t, m): The $\mathcal{A}$ sends message m to P^t, and P^t replies to $\mathcal{A}$ according to the rule.
- Reveal (P^t): The $\mathcal{A}$ reveals the session key S_K between P^t_u and P^t_w. If the $\mathcal{A}$ unable to reveal S_K, then it means that the session key is secure.
- Test (P^t): The $\mathcal{A}$ tossed a coin, and the result was only known to $\mathcal{A}$. The $\mathcal{A}$ uses the result to decide on the Test query and if S_K is fresh, then return *1* or *0*. Otherwise, return null.

Theorem 1: The $\mathcal{A}$ can access the session key security of our proposed scheme. The proof of Theorem 1 is similarly presented in [42]. The polynomial-time of $\mathcal{A}$ as $Adv\ \mathcal{A}$.

$$Adv_A \leq \frac{q2h}{|Hash|} + \{c.\ q2send\}$$

$q2h$ denoted the number of hash queries, q_{send} is the number of send queries, and $|Hash|$ is the range of hash function $h(.)$ while c is a parameter from Zipf's law [43].

Proof: We prove the session key security in four-game "Game$_i$" where $i \in [0, 3]$. The $\mathcal{A}$ use S_A, i to win the $Game_i$ by guessing the random bit fc correctly. $Pr[S_A, Game_i]$ shows the advantage of $\mathcal{A}$ to win $Game_i$. The games are described below:

i. $Game_0$: In this game, we allow the $\mathcal{A}$ to launch an actual attack on our proposed scheme. The $\mathcal{A}$ select random bit fc at the start of the Game$_0$.

$$Adv_A = |2\ Pr[S_A,\ GAME_0] - 1| \tag{1}$$

ii. $Game_1$: The $\mathcal{A}$ execute the Executive (P^t_u, P^t_e, P^t_w) queries and eavesdrops transmitted message $\{N, D, F_u, X_u\}$, $\{X_u, N_3, E_2, F_e\}$, $\{F_w, N_4\}$ and $\{F_{ec}, N_5\}$. The $\mathcal{A}$ run Reveal and Test queries to check whether the derived session key is real or not. Our proposed scheme session key is constructed as $S_K = h(h(ID_u||r_{u1})\ ||h(ID_e||r_e)||h(ID_w||r_w))$. The $\mathcal{A}$ needs random numbers and identities of a user, edge server, and IoT-enable sensor node. Therefore, the probability for $\mathcal{A}$ is non to win the Game$_0$ and Game$_1$. As a result of the paradox [44], we get the following result:

$$Pr[S_A,\ GAME_1] = Pr[S_A,\ GAME_0] \tag{2}$$

iii. *Game₂:* The $\mathcal{A}$ send and perform Hash to obtain the S_K. The $\mathcal{A}$ modify exchanged messages. However, our proposed scheme of exchange messages is constructed using a random number and secret keys and protected by $h(.)$, a one-way hash function. Therefore, we get the following result:

$$|Pr[S_A, GAME_2] - Pr[S_A, GAME_1]| \leq \frac{q2h}{2\ |Hash|} \tag{3}$$

iv. *Game₃:* In the last $Game_3$, the $\mathcal{A}$ tries to use the CorruptedMD query in order to obtain S_K. Using the CorruptedMD query, the $\mathcal{A}$ can get $\{B_1, B_2, B_3, B_4\}$ stored on the user side. These values are expressed as $B_1 = h(ID_u||PW_u) \oplus r_u$, $B_2 = h(ID_u||PW_u||r_u||HPW_u)$, $B_3 = h(HPW_u||r_u) \oplus XID_u$ and $B_4 = h(HPW_u||\ XID_u) \oplus V_1$. The $\mathcal{A}$ cannot extract ID_u, PW_u, r_u, and V_1 values. Therefore, we obtain

$$|Pr[S_A,\ GAME_3] - Pr[S_A,\ GAME_2]| \leq c.q^s_{send} \tag{4}$$

By running these games, the $\mathcal{A}$ must guess the bit in order to win the game. Thus, we obtain

$$Pr[S_A, GAME_3] = 1/2 \tag{5}$$

From Eqs. (1) and (2), we get

$$1/2\ Adv_A = |Pr[S_A, GAME_0 - 1/2]| = |\ Pr[\ SA,\ GAME_1\ - 1/2]| \tag{6}$$

By using Eqs. (5) and (6).

$$1/2\ Adv_A = |Pr[S_A, Game_1] - Pr[S_A, Game_3]| \tag{7}$$

With Eqs. (4), (5), and (7) and using triangular inequality, we obtain

$$\begin{aligned} 1/2\ Adv_A &= |Pr[S_A, GAME_1] - Pr[S_A, GAME_3]| \\ &\leq |Pr[S_A, GAME_1] - Pr[S_A, GAME_2]| \\ &+ |Pr[S_A, GAME_2] - Pr[S_A, GAME_3]| \\ &\leq \frac{q2h}{2\ |Hash|} + c.q^s_{send} \end{aligned} \tag{8}$$

By multiplying both sides of Eq. (8) by 2, we get

$$Adv_A \leq \frac{q2h}{|Hash|} + 2\{c.\ qssend\} \tag{9}$$

As we obtain in Eq. (9), we proved Theorem 1.

4.2 Formal Security Analysis Using ProVerif

ProVerif2.03 verification software toolkit [12] is used to determine if the session secret is secure if it is computed confidentially, if it is exchanged securely among peers, and if an attacker may acquire it during a starting session. It is a popular simulation verification toolkit. Fig. 2 depicts ProVerif's results.

```
(*=====================================RESULT==========================*)
Completing equations...
---------------------------------------
Completing equations...
-- Query not attacker(SK[])
---------------------------------------
Completing...
Starting query not attacker(SK[])
---------------------------------------
Completing...
Starting query not attacker(SK[])
--------------------------------------------------------------------------------
RESULT not attacker(SK[]) is true.
-- Query inj-event(end_Ui(id)) ==> inj-event(start_U(IDu))
Completing...
Starting query inj-event(end_U(IDu)) ==> inj-event(start_U(IDu))
goal reachable: begin(start_U(IDu[]), @sid_876 = endsid_3030, @occ27 = @occ_cst) -
> end(endsid_3030,end_U(IDu[]))
--------------------------------------------------------------------------------
RESULT inj-event(end_U(IDu)) ==> inj-event(start_U(IDu)) is true.
-- Query inj-event(end_W(IDw)) ==> inj-event(start_W(IDw))
Completing...
Starting query inj-event(end_W(IDw)) ==> inj-event(start_W(IDw))
--------------------------------------------------------------------------------
RESULT inj-event(end_W(IDw)) ==> inj-event(start_W(IDw)) is true.
-- Query inj-event(end_RS(IDe)) ==> inj-event(start_RS(IDe))
Completing...
Starting query inj-event(end_RS(IDe)) ==> inj-event(start_RS(IDe))
RESULT inj-event(end_RS(IDe)) ==> inj-event(start_RS(IDe)) is true.
--------------------------------------------------------------------------------
```

Figure 2: ProVerif result

5 Informal Security Analysis

This section shows how our proposed scheme defends against various threats and incorporates security features such as mutual authentication and perfect forward secrecy to protect users' data.

5.1 Offline Password Guessing Attack

In our proposed scheme the $\mathcal{A}$ cannot get $B_1 = h(ID_u||PW_u) \oplus ru$, $B_2 = h(IDu||PWu||ru||HPWu)$, $B_3 = h(HPWu||ru) \oplus XIDu$, $B_4 = h(HPWu||XIDu) \oplus V_1$, $X_u = h(ID_u||r_u)$. The values of B_1, B_2, B_3, B_4, and X_u were constructed using ID_u, PW_u, and random number r_u. Therefore, the $\mathcal{A}$ cannot construct B_1, B_2, B_3, B_4, and X_u. Thus, our proposed scheme resists offline password guessing attacks.

5.2 Mutual Authentication

The user, edge server, and IoT-enable sensor node check the message's validity in the login and authentication phase. The user, edge server, and IoT-enable node checks $F_u? = F_u$, $F_e? = F_e$, $F_w? = F_w$, $F_{ec}? = F_{ec}$, and $N_6 ? = N_6$. If these values are correct, then the entities authenticate each other. Therefore, our proposed scheme provides mutual authentication property.

5.3 Insider Attack

In registration phase, the $\mathcal{A}$ might obtain $X_u = h(ID_u||r_u)$. The $\mathcal{A}$ try to construct $\{B_1, B_2, B_3, B_4, X_u\}$ store on the user side. However, the $\mathcal{A}$ cannot obtain actual ID_u, PW_u, and r_u. Therefore, the $\mathcal{A}$ cannot construct S_K. Thus, our proposed scheme resists insider attacks.

5.4 Desynchronization

The $\mathcal{A}$ trying to modify and block the transmitted messages to the user, edge server, and IoT-enable sensor node cannot authenticate each other. However, the $\mathcal{A}$ cannot do it because, according to our protocol, the $\mathcal{A}$ cannot obtain ID_u, PW_u, r_u, and S_k. Thus, user and edge servers always have synchronized values. Therefore, in our proposed scheme, a desynchronization attack is not possible.

5.5 Anonymity

The $\mathcal{A}$ cannot obtain the actual identities of ID_u, PW_u, ID_e, ID_w, to construct $X_u = h(ID_u||ru)$, $X_w = h(ID_w||r_w)$. Therefore, our proposed scheme provides anonymity.

5.6 Untraceability

In our proposed protocol for every session, the edge server and user update $X_u^{new} = h(X_u||r_{u1})$. Therefore, our protocol provides untraceability.

5.7 Perfect Forward Secrecy

The $\mathcal{A}$ obtains secret key SK_{rs} and tries to create a session key S_K. Although, the $\mathcal{A}$ needs a random number $\{r_u, r_{u1}, r_e, r_w, r_{w1}\}$ because the S_K is composed of a random number for every session. Therefore, our proposed protocol; provides perfect forward secrecy.

5.8 Known Session Attack

The $\mathcal{A}$ attempts to obtain random numbers and construct the session key in accordance with the CK-adversary model. However, the $\mathcal{A}$ needs the identities of a user, edge server, and IoT-enable sensor node. Because in our proposed scheme, the session key was constructed using the identities of the user, edge server, and IoT-enable sensor node. Thus, our proposed scheme resists known session attacks.

5.9 MITM Attack

Let us suppose the $\mathcal{A}$ gets a previous authentication request between the user and edge server. Further, the $\mathcal{A}$ tries to send it again to the edge server. However, the edge server checks the freshness of the random number and rejects the request of $\mathcal{A}$. Thus, our scheme resists the MITM attack.

5.10 Session Key Leakage Attack

The $\mathcal{A}$ might get $\{B_1, B_2, B_3, B_4, X_u\}$ and $\{S_1, S_1, X_u\}$ of the user and IoT-enable sensor node to calculate the S_K. However, the $\mathcal{A}$ need actual identities $(ID_u, ID_w, ID_e\}$ and random numbers $\{r_u, r_{u1}, r_e, r_w, r_{w1}\}$. The identities and random numbers cannot obtain from transmitted messages because these values are encrypted. Thus, our proposed scheme resists session key leakage attacks.

5.11 Replay Attack

Let us suppose the $\mathcal{A}$ tries to modify the authentication request and pretend to be a user or edge server. However, the $\mathcal{A}$ cannot change $\{N, E_1, F_u\}$ and $\{F_{ec}, N_6\}$ without the knowledge of ID_u, PW_u, r_u, ID_e ID_w. Therefore, the proposed scheme resists replay attacks.

5.12 User Impersonation Attack

Let us suppose the $\mathcal{A}$ extract secret values $\{X_u, B_1, B_2, B_3, B_4\}$. The $\mathcal{A}$ tries to impersonate the user using these values. However, the $\mathcal{A}$ cannot send authentication messages towards the edge server

because the $\mathcal{A}$ needs ID_u, PW_u, r_u, and HPW_u to construct $\{N, D, F_u, X_u\}$. Therefore, our proposed scheme resists user impersonation attacks.

5.13 IoT-Enable Sensor Node Impersonation Attack

The $\mathcal{A}$ found a lost IoT-enable sensor node to impersonate the IoT-enable sensor node. However, the $\mathcal{A}$ cannot construct $\{F_u, r_u\}$ because the $\mathcal{A}$ needs ID_w, r_w, and r_{w1} to construct $\{F_w, N_4\}$. Therefore, our proposed scheme resists IoT-enable sensor node impersonation attacks.

5.14 Stolen IoT-Enable Sensor Node Attack

Let suppose the $\mathcal{A}$ get stolen IoT-enable sensor node and obtain secret $\{S_1, S_2, X_w\}$ stored in the memory of IoT-enable sensor node. However, the $\mathcal{A}$ cannot get ID_w, r_w, and r_{w1}. Thus, our proposed scheme resists stolen IoT-enable sensor node attacks.

6 Performance and Security Analysis

This section compared our proposed scheme to similar protocols in terms of security characteristics, communication, and computation cost comparisons, among other things.

6.1 Security Features

In this section, we compare our protocol with [10,21–23,33,45–47] in terms of security features. Table 5 shows that our scheme achieved all security features and provided mutual authentication, anonymity, and untraceability.

Table 5: Security feature comparison

Schemes	[21]	[22]	[23]	[33]	[10]	[45]	[46]	[47]	[48]	Our
Security features										
Offline password guessing attack	✓	⊙	✓	✓	✓	⊙	-	⊙	✓	✓
Mutual authentication	✓	✓	✓	✓	✓	✓	✓	⊙	✓	✓
Insider attack	⊙	⊙	⊙	⊙	✓	✓	✓	✓	✓	✓
Desynchronization	-	-	✓	⊙	✓	✓	✓	⊙	-	✓
Anonymity	✓	✓	⊙	✓	✓	✓	✓	-	✓	✓
Untraceability	✓	✓	✓	⊙	✓	✓	✓	✓	✓	✓
Perfect forward secrecy	✓	✓	✓	✓	✓	⊙	✓	⊙	✓	✓
Known session attack	⊙	⊙	✓	⊙	✓	-	⊙	-	✓	✓
MITM attack	⊙	✓	✓	⊙	⊙	-	-	⊙	✓	✓
Session key leakage attack	⊙	✓	✓	✓	✓	-	-	-	-	✓
Replay attack	✓	✓	⊙	✓	✓	✓	✓	✓	✓	✓
User impersonation attack	✓	✓	✓	⊙	⊙	✓	✓	✓	✓	✓
IoT-enable device impersonation attack	✓	✓	✓	-	✓	✓	✓	✓	✓	✓
Edge server impersonation attack	-	-	-	-	-	-	-	-	✓	✓
Stolen IoT-enable device attack	✓	⊙	✓	✓	✓	✓	✓	✓	✓	✓

Note: ✓: secure, ⊙: insecure, -: not considered.

6.2 Communication Cost

In this section, we first calculate our proposed scheme communication cost and then compare it with recent related protocols [10,21–23,33,45–48] in Table 6. The value of a hash function is (160 bits), the ECC point of multiplication is (320 bits), the symmetric key is (256 bits) timestamp is (32 bits), while the random number is (128 bits), and identities are (160 bits) [49]. Our proposed scheme exchange messages are $\{N, D, F_u, X_u\}$ is {640 bits}, $\{X_u, N_3, E_2, F_e\}$ is {640 bits}, $\{F_w, N_4\}$ is {320 bits}, $\{F_{ec}, N_5\}$ is {320 bits} and $\{N_6\}$ is {160}. As a result, our suggested scheme's overall communication cost is equivalent to 2080 bits. The scheme [45] has a lower communication cost, but the computation cost is high, and the scheme is vulnerable to offline password guessing attacks and unable to provide perfect forward secrecy.

Table 6: Communication cost comparison

[21]	[22]	[23]	[33]	[10]	[45]	[46]	[47]	[48]	Our
5088	7648	6080	4608	3648	1344	11008	2112	2688	2080

6.3 Computation Cost

We compared our proposed scheme computation cost with other related schemes [10,21–23,33,45–48]. First, we calculated our proposed scheme computation cost. According to [50], the ECC point of multiplication T_M is (7.3529 ms), hash function T_h is (0.0004 ms), symmetric key T_S is (0.1303 ms), and fuzzy extractor T_R is (7.3529 ms). Therefore, our scheme total computation cost is $66T_h$ is equal to 0.264 ms. Detail comparison of our proposed scheme computation and communication cost is shown in Fig. 3. The scheme [22] has a lower computation cost. However, the communication cost of the scheme [22] is very high. In contrast, Table 5 shows that the scheme is vulnerable to offline password guessing attacks, insider attacks, and known session attacks.

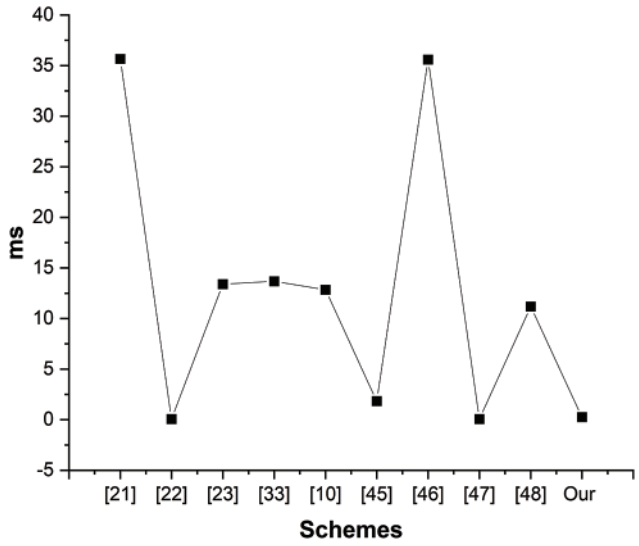

Figure 3: Computation cost comparison

6.4 Storage Cost

In this portion of our research article, we consider the work [49]. The hash function is 160, multiplication point is 320, identity is 160, symmetric key 256, timestamp is 32, and random numbers are 128 bits. Keep view this in mind, our proposed scheme storage cost calculation is $X_w = 160$, $S_1 = 160 + 128$, $S_2 = 160 + 160$, $X_u = 160$, $B_1 = 160 + 128$, $B_2 = 160$, $B_3 = 160 + 160$, $B_4 = 160 + 160$. Hence total storage cost is 2016 bits. Table 7 shows the comparison with other state-of-the-art schemes.

Table 7: Storage cost

[21]	[22]	[23]	[33]	[10]	[45]	[46]	[48]	Our
4480	1856	2880	1280	6464	1696	6240	2880	2016

7 Conclusion

In this research article, we proposed a secure and efficient authentication scheme. Our proposed scheme guarantees secure and efficient communication among the IoT-enable device, user, and edge server. E-healthcare is a prominent research area for researchers because any flaw in the protocol can lead to fatal damage to the patient. Therefore, we cryptanalysis the scheme of Zhu and find out that their scheme suffers from spoofing, impersonation, and masquerading attacks. To overcome the flaws of Zhu's scheme, we proposed a secure and efficient information authentication scheme for IoT-enabled devices in an e-healthcare system.

We choose edge computing to reduce latency for e-healthcare systems because latency is an essential factor. We performed the ROR model and ProVerif to demonstrate that our protocol provided session key security and resisted MITM. In the end, our proposed protocol achieved security features and lower computation costs than recent existing schemes. Therefore, we concluded that our scheme provides lower computation costs and better security.

Acknowledgement: The authors are thankful to the Natural Science Foundation of Beijing Municipality and Beijing University of Technology for funding this work under Grant M21039.

Funding Statement: This work was supported by the Natural Science Foundation of Beijing Municipality under Grant M21039.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Naveed Khan, Shehzad Ashraf Chaudhry and Jianbiao Zhang; security analysis: Naveed Khan; performance analysis: Naveed Khan, Ghulam Ali Mallah, and Shehzad Ashraf Chaudhry; draft manuscript preparation: Naveed Khan, and Shehzad Ashraf Chaudhry. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The first author will provide the supporting data for this work upon reasonable request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2019.

[2] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma *et al.,* "A survey of Healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 53–71, 2019.

[3] I. Cvitić, D. Peraković, M. Periša and B. Gupta, "Ensemble machine learning approach for classification of IoT devices in smart home," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 11, pp. 3179–3202, 2021.

[4] F. Alshehri and G. Muhammad, "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2021.

[5] World Health Organization, "Medication without harm," 2017. [Online]. Available: https://www.bpsassessment.com/wp-content/themes/bpspsa/assets/Downloads/2.%20The%20third%20Global%20Patient%20Safety%20Challeng.pdf

[6] A. Al-Qerem, M. Alauthman, A. Almomani and B. B. Gupta, "IoT transaction processing through cooperative concurrency control on fog–cloud computing environment," *Soft Computing*, vol. 24, no. 8, pp. 5695–5711, 2020.

[7] C. T. Li, C. C. Lee, C. Y. Weng and C. M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 198–208, 2018.

[8] F. Al-Turjman and S. Alturjman, "Context-sensitive access in Industrial Internet of Things (IIoT) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, 2018.

[9] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti *et al.,* "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, 2017.

[10] F. Zhu, "SecMAP: A secure RFID mutual authentication protocol for healthcare systems," *IEEE Access*, vol. 8, pp. 192192–192205, 2020.

[11] W. Liu, X. Wang and W. Peng, "Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing Internet of Things," *IEEE Access*, vol. 8, pp. 8754–8767, 2019.

[12] B. Blanchet, B. Smyth, V. Cheval and M. Sylvestre, "ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial," 2018. [Online]. Available: https://www.crs811.com/uploads/2019/01/manual.pdf

[13] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[14] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Innsbruck, Austria, pp. 453–474, 2001.

[15] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv *et al.,* "A clogging resistant secure authentication scheme for fog computing services," *Computer Networks*, vol. 185, pp. 107731, 2021.

[16] N. Khan, J. Zhang and S. U. Jan, "A robust and privacy-preserving anonymous user authentication scheme for public cloud server," *Security and Communication Networks*, vol. 2022, pp. 1–14, 2022.

[17] C. T. Li, C. L. Chen, C. C. Lee, C. Y. Weng and C. M. Chen, "A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps," *Soft Computing*, vol. 22, no. 8, pp. 2495–2506, 2018.

[18] P. Gope, J. Lee and T. Q. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[19] A. Ostad-Sharif, D. Abbasinezhad-Mood and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *Journal of Medical Systems*, vol. 43, no. 1, pp. 1–22, 2019.

[20] B. D. Deebak, F. Al-Turjman and L. Mostarda, "A hash-based RFID authentication mechanism for context-aware management in IoT-based multimedia systems," *Sensors*, vol. 19, no. 18, pp. 3821, 2019.
[21] V. Sureshkumar, R. Amin, V. Vijaykumar and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation," *Future Generation Computer Systems*, vol. 100, pp. 938–951, 2019.
[22] P. Chandrakar, "A secure remote user authentication protocol for healthcare monitoring using wireless medical sensor networks," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 10, no. 1, pp. 96–116, 2019.
[23] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan *et al.,* "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2019.
[24] M. Adil, M. Attique, M. M. Khan, J. Ali, A. Farouk *et al.,* "HOPCTP: A robust channel categorization data preservation scheme for industrial healthcare Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7151–7161, 2022.
[25] X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang *et al.,* "Secure identity authentication of community medical Internet of Things," *IEEE Access*, vol. 7, pp. 115966–115977, 2019.
[26] H. Sun and R. Grishman, "Lexicalized dependency paths based supervised learning for relation extraction," *Computer Systems Science and Engineering*, vol. 43, no. 3, pp. 861–870, 2022.
[27] S. Ji, Z. Gui, T. Zhou, H. Yan and J. Shen, "An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services," *IEEE Access*, vol. 6, pp. 69603–69611, 2018.
[28] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1–8, 2019.
[29] B. D. Deebak, F. Al-Turjman, M. Aloqaily and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT," *IEEE Access*, vol. 7, pp. 135632–135649, 2019.
[30] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan *et al.,* "Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020.
[31] A. Bengag, O. Moussaoui and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," in *Third Int. Conf. on Intelligent Computing in Data Sciences (ICDS)*, Marrakech-Morocco, pp. 1–5, 2019.
[32] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao *et al.,* "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms," *Security and Communication Networks*, vol. 2019, pp. 1–11, 2019.
[33] D. Rangwani and H. Om, "A secure user authentication protocol based on ECC for cloud computing environment," *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3865–3888, 2021.
[34] S. A. Chaudhry, I. L. Kim, S. Rho, M. S. Farash and T. Shon, "An improved anonymous authentication scheme for distributed mobile cloud computing services," *Cluster Computing*, vol. 22, no. 1, pp. 1595–1609, 2019.
[35] J. J. Hathaliya, S. Tanwar and R. Evans, "Securing electronic healthcare records: A mobile-based biometric authentication approach," *Journal of Information Security and Applications*, vol. 53, pp. 102528, 2020.
[36] M. Nikooghadam and H. Amintoosi, "Secure communication in CloudIoT through design of a lightweight authentication and session key agreement scheme," *International Journal of Communication Systems*, vol. 36, pp. e4332, 2020.
[37] H. A. El Zouka and M. M. Hosni, "Secure IoT communications for smart healthcare monitoring system," *Internet of Things*, vol. 13, pp. 100036, 2021.
[38] A. Ali, H. A. Rahim, J. Ali, M. F. Pasha, M. Masud *et al.,* "A novel secure blockchain framework for accessing electronic health records using multiple certificate authority," *Applied Sciences*, vol. 11, no. 21, pp. 9999, 2021.

[39] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar *et al.,* "Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 824–839, 2016.
[40] S. Qiu, D. Wang, G. Xu and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1338–1351, 2020.
[41] S. A. Chaudhry, H. Naqvi and M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for TMIS," *Multimedia Tools and Applications*, vol. 77, no. 5, pp. 5503–5524, 2018.
[42] M. Rana, A. Shafiq, I. Altaf, M. Alazab, K. Mahmood *et al.,* "A secure and lightweight authentication scheme for next generation IoT infrastructure," *Computer Communications*, vol. 165, pp. 85–96, 2021.
[43] D. Wang, H. Cheng, P. Wang, X. Huang and G. Jian, "Zipf's law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.
[44] V. Boyko, P. MacKenzie and S. Patel, "Provably secure password-authenticated key exchange using diffie-hellman," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, pp. 156–171, 2000.
[45] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, pp. 23514–23526, 2019.
[46] Z. Zhou, P. Wang and Z. Li, "A quadratic residue-based RFID authentication protocol with enhanced security for TMIS," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 9, pp. 3603–3615, 2019.
[47] S. F. Aghili, H. Mala, P. Kaliyar and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for medical IoT," *Future Generation Computer Systems*, vol. 101, pp. 621–634, 2019.
[48] S. A. Chaudhry, "Correcting "PALK: Password-based anonymous lightweight key agreement framework for smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 125, pp. 106529, 2021.
[49] M. Shuai, N. Yu, H. Wang and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers & Security*, vol. 86, pp. 132–146, 2019.
[50] J. Mo and H. Chen, "A lightweight secure user authentication and key agreement protocol for wireless sensor networks," *Security and Communication Networks*, vol. 2019, pp. 1–17, 2019.