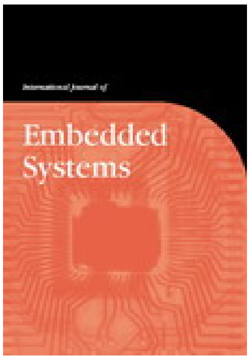
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Embedded Systems

ISSN online: 1741-1076 - ISSN print: 1741-1068
https://www.inderscience.com/ijes

A secure and lightweight hash-based mutual authentication scheme in fog-assisted healthcare network

Upendra Verma, Hemant Kumar Gianey

DOI: 10.1504/IJES.2024.10066866

Article History:

Received:	16 October 2023
Last revised:	04 July 2024
Accepted:	26 July 2024
Published online:	10 February 2025

A secure and lightweight hash-based mutual authentication scheme in fog-assisted healthcare network

Upendra Verma* and Hemant Kumar Gianey

Department of Computer Engineering,
Mukesh Patel School of Technology Management and Engineering,
SVKM'S NMIMS University,
Shirpur-425405, Maharashtra, India
Email: upendra4567@gmail.com
Email: hgianey@gmail.com
*Corresponding author

Abstract: Security and privacy are considered the two main challenges in fog-assisted healthcare networks. Several authentication approaches have been presented in recent years to address the security issues in fog-assisted healthcare networks. To cope with these challenges and improve the safety of fog-assisted healthcare networks, we propose a secure and efficient mutual authentication scheme. In this paper, we design a lightweight hash-based authentication scheme for fog-assisted healthcare networks to provide security against various attacks. The informal security analysis illustrates that the proposed scheme has the capability to resist various security threats. In addition, the proposed scheme has been evaluated with a real-or-random (ROR) model to prove its resilience against cryptographic attacks. The performance study demonstrates that the proposed scheme is more effective and lightweight compared to existing schemes. Moreover, a comprehensive comparison analysis has been undertaken, which shows the proposed scheme provides better security features than existing schemes.

Keywords: fog-assisted healthcare networks; real-or-random; ROR model; mutual authentication; hash function; cryptographic attacks.

Reference to this paper should be made as follows: Verma¸ U. and Gianey, H.K. (2024) 'A secure and lightweight hash-based mutual authentication scheme in fog-assisted healthcare network', *Int. J. Embedded Systems*, Vol. 17, Nos. 3/4, pp.200–212.

Biographical notes: Upendra Verma is currently working as an Assistant Professor in the Department of Computer Engineering at SVKM'S Narsee Monjee Institute of Management Studies (NMIMS University), Mumbai, Shirpur Campus, Maharashtra, India. He has over 16 years of experience in academics. He received his Bachelors of Engineering (BE) and Masters of Engineering (ME) in Computer Science and Engineering from the Rajiv Gandhi Technological University (State Government Technical University) from Madhya Pradesh, India. He has completed his PhD in Computer Science and Engineering from the GLA University, Mathura, India. His primary area of research includes cryptography, design of authentication protocol and fog computing. He has published more than 15 research articles in various peer reviewed journals and conferences and He is also reviewer for various renowned international journals and conferences.

Hemant Kumar Gianey is currently working as an Associate Professor in the Department of Computer Engineering at SVKM'S Narsee Monjee Institute of Management Studies (NMIMS University), Mumbai, Shirpur Campus, Maharashtra, India. He has over 20 years of experience in academics. He obtained his PhD from Rajasthan, MTech (CSE) from the Rajasthan Technical University, Rajasthan; BE from the Rajasthan University, Jaipur, Rajasthan, India and a Post-doctoral researcher from the National Chen Kung University of Taiwan. His area of research includes big data analytics, machine learning algorithms and image processing.

1 Introduction

The objective of the healthcare network is to offer a dependable and well-organised solution to improve societal health. The healthcare network is a product of the rapid digitalisation of industries over the past 20 years (Mehta and Pandit, 2018). According to Alshehri and Muhammad (2020), the smart healthcare market will expand by 16.2% between 2020 to 2027. The main duty of the healthcare network is to continuously monitor physical health indicators like heart rate, blood sugar, blood calcium, height, and weight. This information can be used to get a thorough understanding of the patients' health conditions (Kale et al., 2020; Milioris et al., 2022) and to periodically supply information to cloud servers. A further benefit of the e-Medical system is that ambulances, nurses, and doctors can remotely access this data on cloud servers over the Internet to learn about the patients' current state of health (Sathyaveti and Gomathy, 2023).

Due to its enormous storage capacity and processing power, cloud computing architecture is well-known as an effective method of processing data (Cai et al., 2021; Sharma et al., 2021). But current cloud models do not perform well for essential applications due to issues including reliance on network infrastructure, high bandwidth limitations, and unpredictable response times (Ni et al., 2017). Applications with specific needs, such as real-time, regionally distributed, and delay-sensitive applications, may not be suited for the cloud deployment approach (Jia et al., 2019). In order to solve these issues and offer relevant services at the network's edge, Cisco suggested fog computing. Fog computing applications benefit us by reducing the workload in data centres, speeding up reaction times, using less energy, and conserving network bandwidth (Chen et al., 2020). The shortcomings of current cloud-based models are claimed to be addressed by a novel paradigm called fog computing (Naik, 2021). Fog computing, in contrast to conventional cloud computing, handles computation, offers storage, and facilitates communication at the network edge. As a result, it can do computations that are delay-sensitive while consuming less energy and causing less traffic (Kumari et al., 2018).

In order to manage and interpret the huge amount of data generated by medical devices, patient monitoring systems, and sensors, fog computing is being used progressively in healthcare networks. Fog computing facilitates real-time decision-making by enabling healthcare organisations to analyse data closer to the source (i.e., at the edge of the network). Fog-assisted healthcare networks offer a diverse range of industrial applications that transform patient care delivery and improve clinical workflows in healthcare.

In healthcare networks, fog nodes, in contrast to centralised cloud computing systems, are typically installed in environments lacking sufficient physical security measures. In other words, fog nodes and end devices may be simpler to compromise. Due to this, user private information, including identity, location, health status, and medical records, may be compromised (Lata and Kumar, 2022; Mukherjee et al., 2018). Due to the complexity of the network architecture and the sensitivity of healthcare data, there are a number of security flaws in existing fog-assisted healthcare networks. Patient confidentiality and privacy can be violated by unauthorised access to healthcare data (Park, 2022). Unauthorised access to patient data may be caused by insufficient and weak authentication procedures. Therefore, each user or fog node in the network should be uniquely identified and authenticated in order to create trust and prevent impersonation. In this research, we devised an effective authentication method for a fog-assisted healthcare network.

1.1 Security requirements of fog-assisted healthcare network

Fog computing is one of the leading technologies for various healthcare applications (Santos et al., 2020). The fog-assisted healthcare network has been developed with great impact on society, and it has turned out to be a tremendously promising technology to bring human fitness closer to users. Today, the security of fog-assisted healthcare is a critical issue because the existing security and privacy-preserving schemes of cloud computing are not appropriate for fog computing due to their fundamental differences.

Due to the distributed structure of fog computing and the sensitive nature of patient data, security is still an essential concern in the current fog-assisted healthcare networks (Jalasri and Lakshmanan, 2024). Healthcare data is often handled and stored by fog networks at the edge, increasing the risk of security breaches. To preserve the security of a fog-assisted healthcare network, several security requirements are required. The security requirements are as follows:

- *Untraceability:* untraceability is an important security requirement, which assures that the attacker is not able to identify the network entities based on the transmitted messages (Amin and Biswas, 2015).
- *Perfect forward secrecy:* the perfect forward secrecy is one of the imperative security requirements in the fog-assisted healthcare network. This requirement ensures that all transmitted messages among the network entities are secure (Amanlou et al., 2021).
- *Mutual authentication:* authentication is a critical issue for the fog-assisted healthcare network. The attacker can pretend to be any legitimate user without proper authentication. The existing cloud computing-based authentication solutions are inappropriate in the fog computing environment due to fundamental differences (Zeng et al., 2022).
- *Session key agreement:* the authentication schemes are considered robust when they achieve efficient and successful session key agreements. To fulfil the purpose, the attacker should not predict the session key from the previous session (Mishra et al., 2023).
- *Anonymity:* anonymity is an important security requirement, as the patient or doctor cannot be identified by their identity. For example, the identities of the patients or doctors can be made anonymous when they store their health data on the fog; therefore, the fog servers could not acquire information about the identity (Al-Issa et al., 2019).

The fog-assisted healthcare network is also prone to various cryptographic attacks. So, the network should be resistant to several attacks, such as:

- *Session key leakage attack:* if the attackers are able to guess the session key, then they will be able to transmit and receive messages from the doctor to the patient, and vice versa, and waste the networking resources (Liu et al., 2018).
- *Offline password guessing attack:* offline password attacks are password attacks in which an attacker attempts to retrieve plaintext passwords from a password hash code (Praveen Kumar and Priyanka, 2023; Shao and Chen, 2020).
- *Man-in-the-middle attack (MITM):* during a MITM attack, the attacker modifies communication between two network entities (e.g., a patient and a doctor) that should be communicating directly. In most situations, neither network entity is aware that an attack has occurred (Zhang et al., 2021).
- *Insider attack:* an insider attack is a hostile attack on a network carried out by a user with authorised access. Because they have authorised system access and may be knowledgeable about network architecture, insiders with malicious intent have a significant advantage over external attackers (Rajamanickam et al., 2022).
- *Replay attack:* a replay attack is a network attack in which the attacker repeats or replays data transmissions between the patient and doctor. Replay attacks often involve capturing legal traffic and reusing it later without alteration (Baig and Eskeland, 2021).

1.2 Research contributions

- The proposed scheme offers mutual authentication and anonymity with the help of a one-way cryptographic hash function, which is suitable for fog-assisted healthcare networks.
- The informal security analysis demonstrates that our scheme is resilient against the various security threats.
- The performance analysis in terms of computation and communication costs is carried out, which shows our scheme is lightweight compared to existing schemes.
- Finally, we demonstrate the formal security verification of the proposed approach using the ROR model.

1.3 Organisation of paper

The paper is structured as follows: Section 1 introduces the necessities and security requirements of a fog-assisted healthcare network with research contributions. Section 2 provides a review of relevant literature. Section 3 describes the network and threat model. The proposed authentication scheme is presented in Section 4. Section 5 discusses the formal security analysis using the ROR model. Informal security analysis and performance analysis are evaluated in Sections 6 and 7, respectively. Section 8 presents the limitations and future scope of the proposed work. Finally, Section 9 concludes the research work.

2 Related work

There are numerous advantages to having a fog-assisted healthcare network. Fog-assisted healthcare network has some challenges apart from benefits. The biggest barrier to widespread implementation of fog computing in the healthcare sector is security. In the recent years, authentication is the pertinent security issue and many authentication schemes have been proposed for fog-assisted healthcare network.

Abi-Char et al. (2007) offered authentication method, which provides protection against MITM attack. Certificate-based authentication is impractical in fog-assisted healthcare environments due to the higher computational burden. A certificate-based authentication method was proposed by Jiang et al. (2013). This method utilises certificates to guarantee reciprocal authentication. Due to the need of certificates, the communication and computation cost is substantial. Porambage et al. (2014) proposed authentication scheme for fog computing enabled IoT application. The authentication mechanism provides mutual authentication protocol for all network entities involved in communication. No informal and formal security analysis is conducted on the protocol.

In order to communicate with future internet of things-based healthcare service systems, Hou and Yeh (2015) investigated sensor tag-based communication architecture. The single sign-on (SSO)-based authentication solution entrusts TTP with device authentication. The use of SSO for authentication is unacceptable for a fog-assisted healthcare environment with limited computing resources. Chaudhry et al. (2016) proposed ECC based two factor authentication protocols for telecare medical information system (TMIS). However, their protocol is susceptible to MITM and offline password guessing attacks.

Ibrahim (2016) has devised a secure technique for mutual authentication between edge-fog-cloud networks. To build a mutual authentication protocol, the technique requires hash computations and symmetric encryption/decryption. Qiu et al. (2017) proposed mutual authentication scheme for TMIS. Their scheme utilised ECC. Alizai et al. (2018) introduced an authentication technique based on the concepts of digital signature and device capability. However, no security analysis is undertaken to demonstrate the effectiveness of the proposed approach. The proposed scheme is not compared to existing related authentication schemes.

The user authentication and key management strategy for fog computing was designed by Wazid et al. (2019). The proposed solution utilised the hash function and XOR operation since they are suitable for networks with limited resources. Their scheme is vulnerable to a variety of cryptographic attacks. Sharma and Kalra (2019) propounded an authentication method for cloud-assisted healthcare network. Their proposed approach does not guarantee the anonymity property.

Loffi et al. (2019) developed a challenge-response authentication strategy for fog computing enabled IoT applications. Their scheme is resilient against the various cryptographic attacks. Abbas et al. (2019) introduced an authentication technique that offers fog security services. The presented authentication technique employs the RSA algorithm, which has a larger computation cost than cryptographic hash functions. Tuli et al. (2020) propounded a deep learning based smart healthcare system for fog computing environment. HealthFog was offered to autonomously treat heart patients utilising IoT sensors and a deep learning algorithm. The primary objective of HealthFog is to efficiently manage heart patient data generated by IoT devices using fog computing paradigm. A secure mutual authentication mechanism for healthcare services was offered in 2021 by Shamshad et al. (2022). They asserted that their approach is resistant to a variety of cryptographic attacks, including replay, offline password guessing and insider attacks.

Rangwani and Om (2021) propounded ECC-based secure protocol for the cloud computing environment. They have conducted security analysis to prove its resilience against the cryptographic threats. However, their scheme is vulnerable against the MITM and insider attacks. Mohit et al. (2021) presented a secure authentication scheme for e-healthcare using TMIS. They have conducted formal and informal security analysis, which shows robustness of the authentication scheme. Kalaria et al. (2021) introduced an authentication approach based on ECC and hash for fog computing environment. Their approach is robust against common cryptographic attacks such as fog server and user impersonation, replay and MITM attacks. In addition, their approach also supports user anonymity with service aware authentication.

In consideration of existing research on authentication schemes, we presented a hash-based authentication scheme for fog-assisted healthcare network. The proposed protocol is capable of achieving all security objectives.

3 Network and threat model

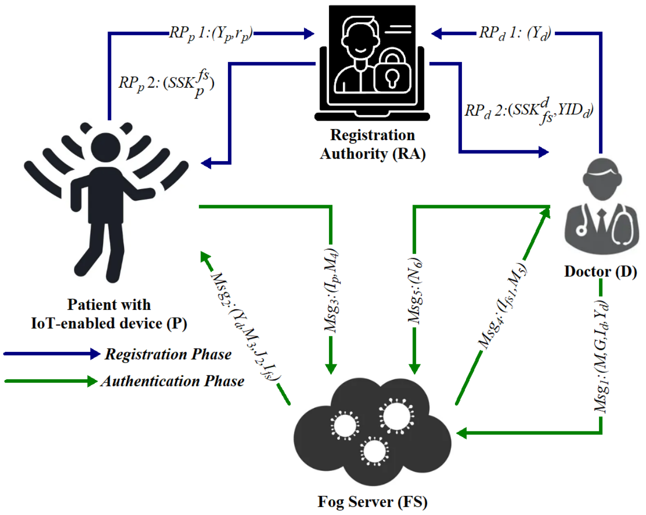
This section presents the network and threat model of our proposed authentication scheme.

3.1 Network model

The network is consisted of patient with IoT enabled device, doctor, fog server and registration authority as shown in Figure 1. These network entities are described as follows:

- *Registration authority:* in the proposed scheme, we assumed that the network has only a single registration authority and it is only trusted party to the patients and doctors. This authority is responsible to generate secret parameters for the patients and doctors and these parameters are shared among the patient and doctor over a secure communication channel.
- *Fog server:* the fog server is located between patient and doctor, which serve the mutual authentication between patient and doctor. Fog server helps patient and doctor to mutual authenticate themselves called three-way authentication procedure (Verma and Bhardwaj, 2022).
- *Patient:* the patient is enabled with multiple sensors or IoT devices that attached to or in the human body, which transmits various parameters such as heart rate, blood sugar level, body temperature, burnt calories, pulse rate, etc. to the doctor. These physical parameters should be shared with doctor after performing mutual authentication.
- *Doctor:* doctor receives the physical parameters from the patient via fog server. After successful authentication, doctor provides healthcare services to the patient.

Figure 1 Network model (see online version for colours)

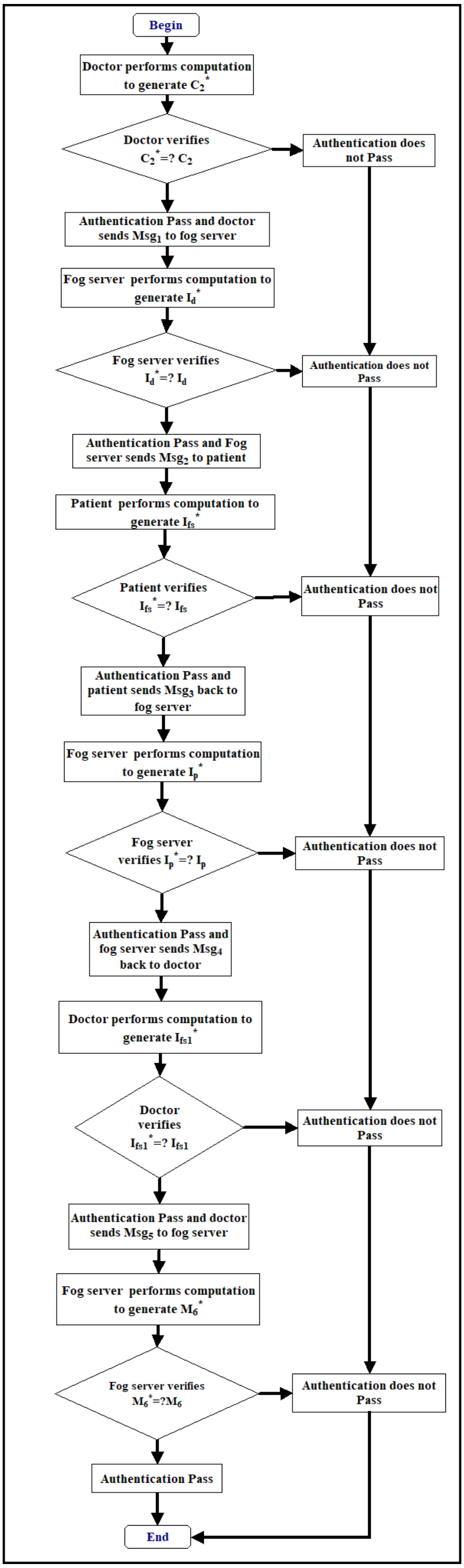

RP_p 1:(Y_p,r_p)
RP_p 2: (SSK_p^{fs})
RP_d 1: (Y_d)
RP_d 2:(SSK_{fs}^d,YID_d)
Registration Authority (RA)
Patient with IoT-enabled device (P)
Doctor (D)
Registration Phase
Authentication Phase
Msg_2:(Y_d,M_3,J_2,I_{fs})
Msg_3:(I_p,M_4)
Msg_5:(N_6)
Msg_4:(I_{fs1},M_5)
Msg_1:(M,G,I_d,Y_d)
Fog Server (FS)

3.2 Threat model

The threat model explains about the capabilities and strength of an attacker. In our threat model, the capabilities of attacker are stated as follow:

- The attacker can compromise the various parameters exchanged between patient and doctor and vice-versa.
- The attacker may obtain the session key (SK) of previous sessions.
- The attacker may eavesdrop the sensitive information, while the communication between patient and doctor have not been fully secured and encrypted.
- If the FS is compromised, the attacker can get all sensitive information between patient and doctor.
- All communication between the patient and the doctor is under the attacker's exclusive control.

Figure 2 Block diagram of proposed scheme (see online version for colours)


Begin
Doctor performs computation to generate C_2^*
Doctor verifies C_2^*=? C_2
Authentication does not Pass
Authentication Pass and doctor sends Msg_1 to fog server
Fog server performs computation to generate I_d^*
Fog server verifies I_d^*=? I_d
Authentication does not Pass
Authentication Pass and Fog server sends Msg_2 to patient
Patient performs computation to generate I_{fs}^*
Patient verifies I_{fs}^*=? I_{fs}
Authentication does not Pass
Authentication Pass and patient sends Msg_3 back to fog server
Fog server performs computation to generate I_p^*
Fog server verifies I_p^*=? I_p
Authentication does not Pass
Authentication Pass and fog server sends Msg_4 back to doctor
Doctor performs computation to generate I_{fs1}^*
Doctor verifies I_{fs1}^*=? I_{fs1}
Authentication does not Pass
Authentication Pass and doctor sends Msg_5 to fog server
Fog server performs computation to generate M_6^*
Fog server verifies M_6^*=?M_6
Authentication does not Pass
Authentication Pass
End

4 Proposed authentication scheme

This section describes our proposed authentication approach in deeper level. One-way cryptographic hash function consumes less computing resources (i.e., processing, energy, etc.) compared to symmetric and asymmetric key cryptography (Singh and Chauhan, 2017). Therefore, we offer a lightweight hash-based mutual authentication scheme for securing fog-assisted healthcare network. The block diagram of proposed scheme is depicted in Figure 2.

The block diagram is essentially the flowchart of authentication procedure that outlines the steps involved in verifying the network entities attempting to access the networks. The brief description of block diagram is illustrated below:

1 The authentication procedure begins.

2 The doctor computes C_2^* and performs verification (C_2^* =? C_2). If yes, then proceed to next step, otherwise terminate the procedure. [C_2^* is computed in step AP1 and C_2 is computed in step RP_d^3].

3. The fog server computes I_d^* and performs verification (I_d^* =? I_d). If yes, then proceed to next step, otherwise terminate the procedure. [I_d^* is computed in step AP2 and I_d is computed in step AP1].

4 The doctor computes I_{fs1}^* and performs verification (I_{fs1}^* =? I_{fs1}). If yes, then proceed to next step, otherwise terminate the procedure. [I_{fs1}^* is computed in the step AP5 and I_{fs1} is computed in the step AP4].

5 The fog server computes M_6^* and perform verification (M_6^* =? M_6). If yes, then proceed to next step, otherwise terminate the procedure. [M_6^* is computed in the step AP6 and M_6 is computed in the step AP5].

Table 1 Notations used in this paper

Notations	*Meaning*
P	Patient
D	Doctor
FS	Fog server
RA	Registration authority
ID_p	Patient's identity
ID_{fs}	Fog server's identity
ID_d	Doctor's identity
r_p, r_{p1}	Random number derived by P
r_{ra}	Random number derived by RA
r_{fs}	Random number derived by FS
r_d, r_{d1}	Random number derived by D
PW_d	Password generated by D
SSK_{fs}^p	FS and P share a secure session key
SSK_{fs}^d	D and FS share a secure session key
h(·)	One-way hash function
||	Concatenation operation
⊕	XOR operation

Figure 3 Summary of proposed authentication scheme (see online version for colours)

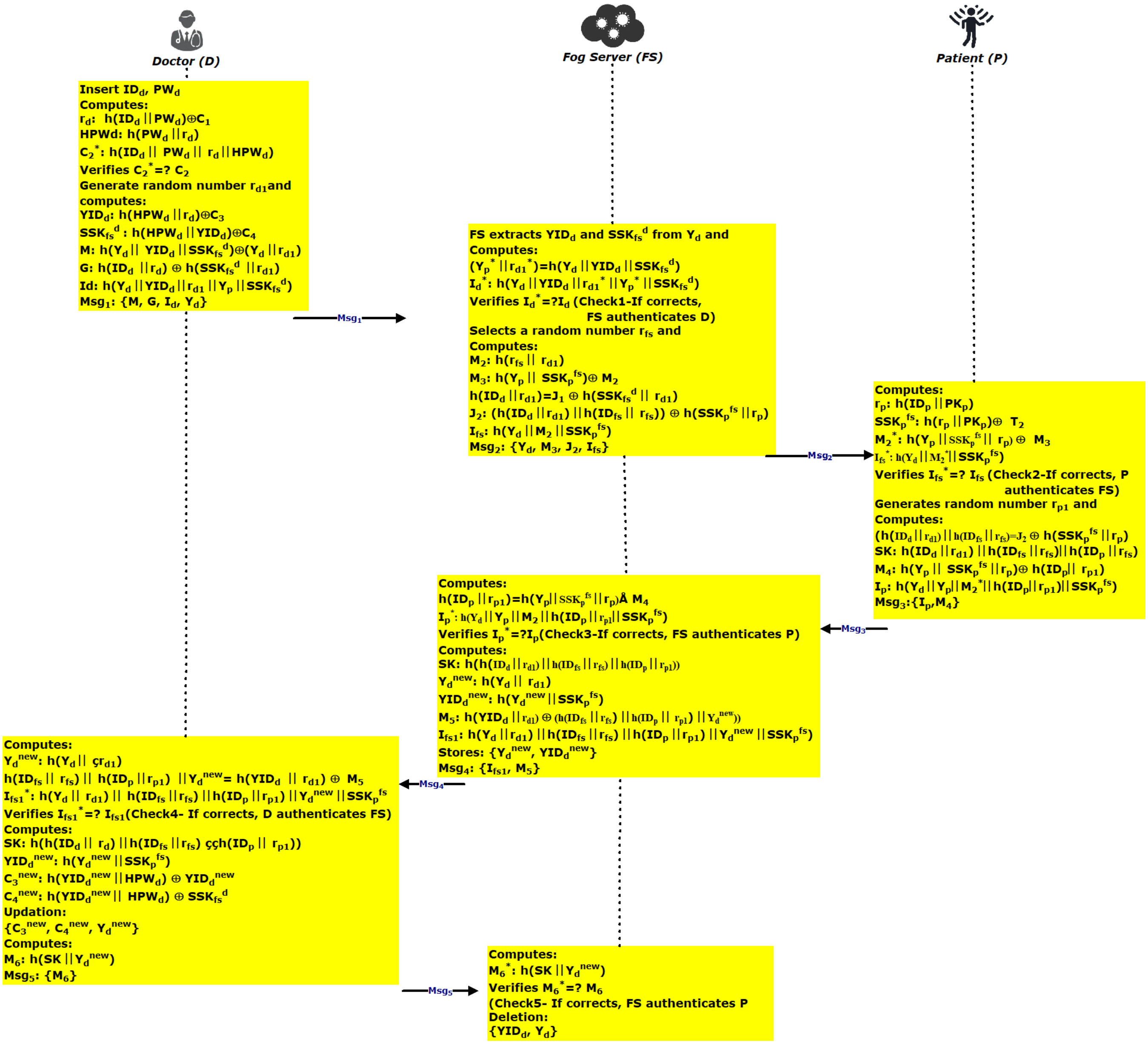

Doctor (D)
Fog Server (FS)
Patient (P)
Insert ID_d, PW_d
Computes:
r_d: $h(ID_d || PW_d) \oplus C_1$
HPWd: $h(PW_d || r_d)$
C_2^*: $h(ID_d || PW_d || r_d || HPW_d)$
Verifies $C_2^* =? C_2$
Generate random number $r_{d1}$and computes:
YID_d: $h(HPW_d || r_d) \oplus C_3$
SSK_{fs}^d : $h(HPW_d || YID_d) \oplus C_4$
M: $h(Y_d || YID_d || SSK_{fs}^d) \oplus (Y_d || r_{d1})$
G: $h(ID_d || r_d) \oplus h(SSK_{fs}^d || r_{d1})$
Id: $h(Y_d || YID_d || r_{d1} || Y_p || SSK_{fs}^d)$
Msg_1: {M, G, I_d, Y_d}
Msg_1
FS extracts YID_d and SSK_{fs}^d from Y_d and
Computes:
$(Y_p^* || r_{d1}^*) = h(Y_d || YID_d || SSK_{fs}^d)$
I_d^*: $h(Y_d || YID_d || r_{d1}^* || Y_p^* || SSK_{fs}^d)$
Verifies $I_d^* =? I_d$ (Check1-If corrects, FS authenticates D)
Selects a random number r_{fs} and
Computes:
M_2: $h(r_{fs} || r_{d1})$
M_3: $h(Y_p || SSK_p^{fs}) \oplus M_2$
$h(ID_d || r_{d1}) = J_1 \oplus h(SSK_{fs}^d || r_{d1})$
J_2: $(h(ID_d || r_{d1}) || h(ID_{fs} || r_{fs})) \oplus h(SSK_p^{fs} || r_p)$
I_{fs}: $h(Y_d || M_2 || SSK_p^{fs})$
Msg_2: {Y_d, M_3, J_2, I_{fs}}
Msg_2
Computes:
r_p: $h(ID_p || PK_p)$
SSK_p^{fs}: $h(r_p || PK_p) \oplus T_2$
M_2^*: $h(Y_p || SSK_p^{fs} || r_p) \oplus M_3$
I_{fs}^*: $h(Y_d || M_2^* || SSK_p^{fs})$
Verifies $I_{fs}^* =? I_{fs}$ (Check2-If corrects, P authenticates FS)
Generates random number r_{p1} and
Computes:
$(h(ID_d || r_{d1}) || h(ID_{fs} || r_{fs}) = J_2 \oplus h(SSK_p^{fs} || r_p)$
SK: $h(ID_d || r_{d1}) || h(ID_{fs} || r_{fs}) || h(ID_p || r_{fs})$
M_4: $h(Y_p || SSK_p^{fs} || r_p) \oplus h(ID_p || r_{p1})$
I_p: $h(Y_d || Y_p || M_2^* || h(ID_p || r_{p1}) || SSK_p^{fs})$
Msg_3:{I_p,M_4}
Msg_3
Computes:
$h(ID_p || r_{p1}) = h(Y_p || SSK_p^{fs} || r_p)$Å M_4
I_p^*: $h(Y_d || Y_p || M_2 || h(ID_p || r_{p1} || SSK_p^{fs})$
Verifies $I_p^* =? I_p$(Check3-If corrects, FS authenticates P)
Computes:
SK: $h(h(ID_d || r_{d1}) || h(ID_{fs} || r_{fs}) || h(ID_p || r_{p1}))$
Y_d^{new}: $h(Y_d || r_{d1})$
YID_d^{new}: $h(Y_d^{new} || SSK_p^{fs})$
M_5: $h(YID_d || r_{d1}) \oplus (h(ID_{fs} || r_{fs}) || h(ID_p || r_{p1}) || Y_d^{new}))$
I_{fs1}: $h(Y_d || r_{d1}) || h(ID_{fs} || r_{fs}) || h(ID_p || r_{p1}) || Y_d^{new} || SSK_p^{fs})$
Stores: {Y_d^{new}, YID_d^{new}}
Msg_4: {I_{fs1}, M_5}
Msg_4
Computes:
Y_d^{new}: $h(Y_d ||$ ç$r_{d1})$
$h(ID_{fs} || r_{fs}) || h(ID_p || r_{p1}) || Y_d^{new} = h(YID_d || r_{d1}) \oplus M_5$
I_{fs1}^*: $h(Y_d || r_{d1}) || h(ID_{fs} || r_{fs}) || h(ID_p || r_{p1}) || Y_d^{new} || SSK_p^{fs}$
Verifies $I_{fs1}^* =? I_{fs1}$(Check4- If corrects, D authenticates FS)
Computes:
SK: $h(h(ID_d || r_d) || h(ID_{fs} || r_{fs})$ çç$h(ID_p || r_{p1}))$
YID_d^{new}: $h(Y_d^{new} || SSK_p^{fs})$
C_3^{new}: $h(YID_d^{new} || HPW_d) \oplus YID_d^{new}$
C_4^{new}: $h(YID_d^{new} || HPW_d) \oplus SSK_{fs}^d$
Updation:
{C_3^{new}, C_4^{new}, Y_d^{new}}
Computes:
M_6: $h(SK || Y_d^{new})$
Msg_5: {M_6}
Msg_5
Computes:
M_6^*: $h(SK || Y_d^{new})$
Verifies $M_6^* =? M_6$
(Check5- If corrects, FS authenticates P
Deletion:
{YID_d, Y_d}

Table 1 depicts the symbolic notations utilised by our proposed approach. The proposed approach is comprised of four phases: initialisation, registration, authentication, and password update. Figure 3 illustrates a summary of the proposed scheme.

4.1 Initialisation phase

In the proposed authentication scheme, the RA generates the secret key SK_{ra}. The patient (*P*), fog server (*FS*) and doctor (*D*) have their own unique identities ID_p, ID_{fs} and ID_d.

4.2 Registration phase

The registration authority is responsible to register patient and doctor over a secure communication channel. For registration, patient and doctor submit secret parameters to the registration authority. The registration phase includes two phases. In the first phase, patient would register with the registration authority (*RA*), while in second phase; doctor would register with the registration authority. The registration process is described as follows:

4.2.1 Registration phase for patient (RP_p)

In this phase, the patient registers with the RA. The steps of registration phase for patient are as follows:

- *RP_p1.* The patient selects the identity ID_p and generates a random number r_p to calculate Y_p: $h(ID_p || r_p)$. Now, the patient sends $\{Y_p, r_p\}$ to the registration authority over a secure channel.
- *RP_p2.* Upon receiving $\{Y_p, r_p\}$ from the patient, the registration authority generates a random number r_{ra} to

compute SSK_p^{fs}: $h(Y_p \| r_{ra} \| SK_{ra})$ and store $\{Y_p, SSK_p^{fs}, r_{ra}\}$ in the fog server database. After that, registration authority sends SSK_p^{fs} to the patient over secure channel.

- *RP$_p$3.* The patient further calculates T_1: $h(ID_p \| SK_p) \oplus r_p$, T_2: $h(r_p \| SK_p) \oplus SSK_p^{fs}$ and store $\{Y_p, T_1, T_2\}$ in its memory.

4.2.2 Registration phase for doctor (RP$_d$)

In this phase, the doctor registers with the registration authority. The steps of registration phase for doctor are as follows:

- *RP$_d$1.* The doctor selects its identity ID_d, creates a random number r_d and computes Y_d: $h(ID_d \| r_d)$. After that, doctor sends Y_d to registration authority over a secure channel.
- *RP$_d$2.* Upon receiving $\{Y_d\}$ from the doctor, the registration authority computes SSK_{fs}^d: $h(Y_d \| SK_{ra} \| r_{ra})$, YID_d: $h(Y_d \| SSK_{fs}^d)$ and store $\{Y_d, YID_d, SSK_{fs}^d\}$ in the fog server database. After that, registration authority sends $\{SSK_{fs}^d, YID_d\}$ to the doctor over a secure channel.
- *RP$_d$3.* The doctor selects a password PW_d and computes HPW_d: $h(PW_d \| r_d)$, C_1: $h(ID_d \| PW_d) \oplus r_d$, C_2: $h(ID_d \| PW_d \| r_d \| HPW_d)$, C_3: $h(HPW_d \| r_d) \oplus YID_d$, C_4: $h(HPW_d \| YID_d) \oplus SSK_{fs}^d$ and store $\{Y_d, C_1, C_2, C_3, C_4\}$ in its memory.

4.3 Authentication phase (AP)

This phase allows to achieve mutual authentication between P and D through FS. The description of this phase is as follows:

- *AP1.* In this phase, firstly doctor computes rd with the help of its identity ID_d and password PW_d as r_d: $h(ID_d \| PW_d) \oplus C_1$, HPW_d: $h(PW_d \| r_d)$ and C_2^*: $h(ID_d \| PW_d \| r_d \| HPW_d)$. Now the doctor verifies $C_2^* =? C_2$. If yes (it corrects) then proceed to the next step, otherwise terminate the authentication process. The doctor generates random number r_{d1} and compute YID_d: $h(HPW_d \| r_d) \oplus C_3$, SSK_{fs}^d: $h(HPW_d \| YID_d) \oplus C_4$, *M*: $h(Y_d \| YID_d \| SSK_{fs}^d) \oplus (Y_d \| r_{d1})$, *G*: $h(ID_d \| r_d) \oplus h(SSK_{fs}^d \| r_{d1})$, I_d: $h(Y_d \| YID_d \| r_{d1} \| Y_p \| SSK_{fs}^d)$. After that, the doctor transmits $Msg_1 = \{M, G, I_d, Y_d\}$ to the fog server.
- *AP2.* Upon receiving Msg_1 from the doctor, fog server extracts YID_d and SSK_{fs}^d as per the Y_d [see step(2) – registration phase of doctor]. Now fog sever computes $(Y_p^* \| r_{d1}^*) = h(Y_d \| YID_d \| SSK_{fs}^d)$, I_d^*: $h(Y_d \| YID_d \| r_{d1}^* \| Y_p^* \| SSK_{fs}^d)$ and verifies $I_d^* =?$ Id (*Check1*). If it corrects then fog server successfully authenticates doctor and continues the authentication process, otherwise fog server stops the authentication process. Now fog sever selects random number rfs and computes M_2: $h(r_{fs} \| r_{d1})$, M_3: $h(Y_p \| SSK_p^{fs} \| r_p) \oplus M_2$, $h(ID_d \| r_{d1}) = J_1 \oplus h(SSK_{fs}^d \| r_{d1})$, J_2: $(h(ID_d \| r_{d1}) \| h(ID_{fs} \| r_{fs})) \oplus h(SSK_p^{fs} \| r_p)$ and I_{fs}: $h(Y_d \| M_2 \| SSK_p^{fs})$. After that, fog server sends $Msg_2 = \{Y_d, M_3, J_2, I_{fs}\}$ to the patient.
- *AP3.* Upon receiving Msg_2 by the fog server, the patient computes r_p: $h(ID_p \| PK_p)$, $SSK_p^{fs} = h(r_p \| PK_p) \oplus T_2$, M_2^*: $h(Y_p \| SSK_p^{fs} \| r_p) \oplus M_3$, I_{fs}^*: $h(Y_d \| M_2^* \| SSK_p^{fs})$. Now check $I_{fs}^* =? I_{fs}$ (*Check2*). If it corrects then patient authenticates fog server, otherwise stops the authentication process. Now patient creates a number r_{p1} and calculates $(h(ID_d \| r_{d1}) \| h(ID_{fs} \| r_{fs})) = J_2 \oplus h(SSK_p^{fs} \| r_p)$, SK: $h(ID_d \| r_{d1}) \| h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{fs})$, M_4: $h(Y_p \| SSK_p^{fs} \| r_p) \oplus h(ID_p \| r_{p1})$, I_p: $h(Y_d \| Y_p \| M_2^* \| h(ID_p \| r_{p1}) \| SSK_p^{fs})$. After that patient sends Msg_3: $\{I_p, M_4\}$ back to the fog server.
- *AP4.* FS receives Msg_3 and computes $h(ID_p \| r_{p1}) = h(Y_p \| SSK_p^{fs} \| r_p) \oplus M_4$, I_p^*: $h(Y_d \| Y_p \| M_2 \| h(ID_p \| r_{p1} \| SSK_p^{fs})$. Now fog sever verifies $I_p^* =?$ Ip (*Check3*). If it corrects then fog server authenticates patient, otherwise stops the authentication process. Now fog server computes SK: $h(h(ID_d \| r_{d1}) \| h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{p1}))$, Y_d^{new}: $h(Y_d \| r_{d1})$, YID_d^{new}: $h(Y_d^{new} \| SSK_p^{fs})$, M_5: $h(YID_d \| r_{d1}) \oplus (h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{p1}) \| Y_d^{new}))$, I_{fs1}: $h(Y_d \| r_{d1}) \| h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{p1}) \| Y_d^{new} \| SSK_p^{fs})$. The fog server stores $\{Y_d^{new}, YID_d^{new}\}$ in the fog server's memory. Now FS sends Msg_4: $\{I_{fs1}, M_5\}$ back to the doctor.
- *AP5.* Upon receiving Msg_4, the doctor computes Y_d^{new}: $h(Y_d \| r_{d1})$, $h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{p1}) \| Y_d^{new} = h(YID_d \| r_{d1}) \oplus M_5$, I_{fs1}^*: $h(Y_d \| r_{d1}) \| h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{p1}) \| Y_d^{new} \| SSK_p^{fs}$. Now doctor verifies $I_{fs1}^* =? I_{fs1}$ (*Check4*), if it corrects then doctor authenticates fog server, otherwise stops the authentication process. The doctor computes SK: $h(h(ID_d \| r_d) \| h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_{p1}))$, $YID_d^{new} = h(Y_d^{new} \| SSK_p^{fs})$, $C_3^{new} = h(YID_d^{new} \| HPW_d) \oplus YID_d^{new}$, C_4^{new}: $h(YID_d^{new} \| HPW_d) \oplus SSL_{fs}^d$. Now the doctor updates $\{C_3^{new}, C_4^{new}, Y_d^{new}\}$ and computes M_6: $h(SK \| Y_d^{new})$. The doctor sends Msg_5: $\{M_6\}$ to the FS.
- *AP6.* The FS receives the Msg_5 and computes M_6^*: $h(SK \| Y_d^{new})$. The fog server verifies $M_6^* =? M_6$ (*Check5*). If it corrects then fog server authenticates the doctor, otherwise stops the authentication process. After completion the authentication process, the fog server deletes $\{YID_d, Y_d\}$ from its database.

4.4 Password update phase (PUP)

The password should be updated frequently. Thus, this phase is executed intermittently to update the password. The explanation of this phase is as follows:

- *PUP1:* The doctor enters their identity ID_d and password PW_d.

- *PUP2:* after that, doctor computes $HPW_d = h(PW_d \| r_d)$, $C_1 = h(IDd \| PW_d) \oplus r_d$, $C_2 = h(ID_d \| PW_d \| r_d \| HPW_d)$, $C_3 = h(HPW_d \| r_d) \oplus YID_d$, $C_4 = h(HPW_d \| YID_d) \oplus SSK_f^{sd}$, $r_d = h(ID_d \| PW_d) \oplus C_1$, $C_2^* = h(ID_d \| PW_d \| r_d \| HPW_d)$. Now verifies $C_2^* =? C_2$, if it corrects then continues the process, otherwise terminate the connection.
- *PUP3:* the doctor enters a new password PW_d^{new}.
- *PUP4:* after that, doctor updates the values as $HPW_d^* = h(PW_d^{new} \| r_d)$, $C_1^* = h(ID_d \| PW_d^{new}) \oplus r_d$, $C_2^{**} = h(ID_d \| PW_d^{new} \| r_d \| HPW_d^*)$, $C_3^* = h(HPW_d^* \| r_d) \oplus YID_d$, $C_4^* = h(HPW_d^* \| YID_d) \oplus SSK_{fs}^d$, $r_d^* = h(ID_d \| PW_d^{new}) \oplus C_1^*$, $C_2^{***} = h(ID_d \| PW_d^{new} \| r_d \| HPW_d^*)$ and update $\{ HPW_d^*, C_1^*, C_2^{**}, C_3^*, C_4^*, C_2^{***}\}$.

5 Formal security verification using ROR model

ROR model (Srinivas et al., 2019) is used to demonstrate the security of session key SK in the proposed scheme. In the proposed scheme, there are three entities E: Patient E_p, Doctor E_d and fog server E_{fs}. The attacker has the ability to modify, construct, eavesdrop and intercept the parameters, which are transmitted across the insecure communication channel.

The ROR model has defined various queries such as send, receive, CorruptedMD, test, reveal and executive queries. By the execution of such queries, attacker may attack the network in active or passive mode. As per the proposed scheme, the queries have following instructions, which are listed below:

- *Send (E, M):* the attacker sends message M to E as per the rule.
- *Receive (E, M):* the E responds to the received message M to attacker as per the rule.
- *CorruptedMD(E_d):* the attacker may obtain secret and confidential information stored on doctor side.
- *Test(E):* the attacker tossed a coin and results of toss was only known to the attacker. The attacker uses the result to decide on a Test query and if the session key SK is fresh then it return 0 or 1, otherwise the result is null.
- *Reveal(E):* the attacker reveals the session key SK between Ed and Ep. If the attacker is not able to reveal SK, then it indicates that the SK is secure.
- *Executive (E_d, E_{fs}, E_p):* the attacker may capture transmitted information over the insecure channel among doctor, fog server and patient.

Proposition 1: The attacker can access the security of session key of the proposed scheme. The execution time of attacker is defined as A_E:

$$A_E \le \left(h_Q / |h|\right) + \left\{a \cdot Q_{Snd}{}^S\right\} \tag{1}$$

where

h_Q the total number of hash queries

Q_{Snd} the total number of send queries

|h] hash function range

a a parameter.

Proof: The security of SK is proved using game denoted as G_k, where $k \in [0, 1, 2, 3]$. The attacker uses SA, k to win the G_k. P_r [S_A, k] indicates the advantage of attacker to win Gk. The G_k: {0 to 3} is described below:

1 G_0: in this game, attacker can launch an actual attack on the proposed scheme. The attacker selects random bit at start of the G_0.

$$A_E = \left|2 \cdot P_r\left[S_A, G_0\right] - 1\right| \tag{2}$$

2 G_1: in this game, we allow attacker to execute the Executive (E_d, E_{fs}, E_p) queries and eavesdrops transmitted parameters between the entities {M, G, I_d, Y_d}, {Y_d, M_3, J_2, I_{fs}}, {I_w, M_4} and {I_{fs1}, M_5}. The attacker run Reveal and test queries to verify, whether the derived SK is real or not. In the proposed scheme, the SK is constructed as $SK = h(h(ID_d \| r_{d1}) \| h(ID_{fs} \| r_{fs}) \| h(ID_p \| r_p))$. The attacker needs identity of doctor, patient and fog server and random numbers to win the G_0. Hence, the probability for the attacker is non to win the G_1.

$$\text{Therefore, } P_r\left[S_A, G_1\right] = P_r\left[S_A, G_0\right] \tag{3}$$

3 G_2: the attacker can perform hash to obtain SK. The attacker can modify the transmitted messages. However, in the proposed scheme, messages are constructed using SK's and random numbers and also protected by $h(\cdot)$. Thus, we get the result as follows as:

$$\left|P_r\left[S_A, G_2\right] - P_r\left[S_A, G_1\right]\right| \le h_Q / 2\,|\,h\,|) \tag{4}$$

4 G_3: in this game, the attacker tries to use CorruptedMD query to obtain session key SK. Attacker may use the query to obtain {C_1, C_2, C_3, C_4}. The attacker cannot construct C_1, C_2, C_3 and C_4 without extracting ID_d, PW_d, r_d and SSK_{fs}^d. Hence, we obtain,

$$\left|P_r\left[S_A, G_3\right] - P_r\left[S_A, G_2\right]\right| \le a \cdot Q_{Snd}{}^S \tag{5}$$

The attacker must guess the random bit to win the game with the help of running games G_k. Hence, we obtain $P_r[S_A, G_3] = ½$

From equation (1) and (2), we obtain

$$\begin{aligned} ½A_E &= \left|P_r\left[S_A, G_0 - ½\right]\right| \\ &= \left|P_r\left[S_A, G_1 - ½\right]\right| \end{aligned} \tag{6}$$

From equation (5) and (6), we obtain

$$½A_E = \left|P_r\left[S_A, G_1\right] - P_r\left[S_A, G_3\right]\right| \tag{7}$$

From equation (4), (5) and (7), we get

$$\begin{aligned} ½A_E &= \left|P_r[S_A, G_1] - P_r[S_A, G_3]\right| \\ &\le \left|P_r[S_A, G_1] - P_r[S_A, G_2]\right| + \left|P_r[S_A, G_2] - P_r[S_A, G_3]\right| \quad (8) \\ &\le \left(h_Q / 2|h|\right) + \left\{a \cdot Q_{Snd}{}^{S}\right\} \end{aligned}$$

The value 2 multiplies with both side of equation (8) to obtain

$$A_E \le \left(h_Q / |h|\right) + 2\left\{a \cdot QS_{nd}{}^{S}\right\} \quad (9)$$

Therefore, the proposition 1 is proved by equation (9), which is stated in equation (1).

6 Informal security analysis

This section explains how the proposed authentication defends against a variety of cryptographic attacks.

6.1 Untraceability

In the proposed authentication scheme, doctor and fog server update $Y_d^{new} = h(Y_d \| r_{d1})$ for every session. Hence, the proposed scheme provides untraceability.

6.2 Replay attack

Let us suppose the attacker tries to modify the authentication request and pretend to be a doctor or fog server. However, attacker cannot change $\{M, J_1, I_d, I_{fs}, M_6, I_p\}$ without knowledge of ID_d, PW_d, r_d, ID_{fs}, ID_p. Therefore, the proposed scheme is resilience against replay attack.

6.3 Session key leakage attack

Let us suppose attacker might get $\{C_1, C_2, C_3, C_4, Y_d\}$ and $\{T_1, T_2, Y_d\}$ of the doctor and patient to compute the SK. However, attacker needs actual identities and random number such as ID_d, ID_{fs}, ID_p, r_d, r_{d1}, r_{fs}, r_p, r_{p1} to calculate parameters C_1, C_2, C_3, C_4, Y_d, T_1 and T_2. The attacker cannot obtain the actual identities from the transmitted message because the actual identities are encrypted using $h(\cdot)$. Thus, the proposed authentication scheme defends against the session key leakage attack.

6.4 Offline password guessing attack

In the proposed authentication scheme, attacker cannot get $C_1 = h(ID_d \| PW_d) \oplus r_{d1}$, $C_2 = h(ID_d \| PW_d \| r_d \| HPW_d)$, $C_3 = h(HPW_d \| r_d) \oplus YID_d$, $C_4 = h(HPW_d \| YID_d) \oplus SSK_{fs}{}^{d}$, $Y_d = h(ID_d \| r_d)$. The parameters C_1, C_2, C_3, C_4 and Y_d are constructed using ID_d, PW_d and r_d. Hence, attacker cannot construct C_1, C_2, C_3, C_4 and Y_d.

6.5 MITM attack

Let's suppose attacker gets previous authentication request between doctor and fog server. Further, attacker tries to send it again to the FS. However, fog server verifies the freshness of the random number and rejects the authentication request of attacker. Therefore, the proposed scheme defends against MITM attack.

6.6 Perfect forward secrecy

The attacker might obtain secret key of the registration authority SKra and tries to create a session key SK. In our scheme, SK is constructed using random numbers $\{r_d, r_{d1}, r_{fs}, r_p, r_{p1}\}$ for every session. So, attacker needs random number to perform forward secrecy, which is computationally infeasible.

6.7 Anonymity

The attacker cannot obtain the actual identities ID_d, ID_{fs} and ID_p from the $Y_d = h(ID_d \| r_d)$ and $Y_p = h(ID_p \| r_p)$. Because, ID_d and ID_p are protected using one-way hash function, which is irreversible and computationally infeasible to obtain actual identities.

6.8 Provides mutual authentication

In the authentication phase, doctor, patient and fog server must verify the message validity. To ensure the authentication, the network entities (D, P, FS) verifies Check1, Check2, Check3, Check4 and Check5. If these parameters are correct and equivalent with each other, then entities authenticate each other successfully, otherwise stops the authentication process. The proposed method enables mutual authentication among the network entities.

6.9 Insider attack

The attacker might obtain $Y_d = h(ID_d \| r_d)$ in the registration phase. The attacker try to construct $\{C_1, C_2, C_3, C_4, Y_d\}$, which are stored on the doctor side. However, attacker cannot get the actual parameters ID_d, PW_d and r_d as they are neither stored nor transmitted across the network entities.

7 Performance analysis

This section presents evaluation and comparison of the proposed scheme with other related schemes, considering into account of various security attributes and communication and computation overhead. To demonstrate the efficacy and efficiency of proposed scheme, the results of evaluation are shown in Table 3 and Table 4. Table 3 compares the communication and computation overhead of the proposed approach with related approaches (Chaudhry et al., 2016; Qiu et al., 2017; Rangwani and Om, 2021) and Table 4 lists some security attacks and security attributes in order to compare the proposed scheme with other schemes.

Figure 4 Comparative analysis of communication overhead among authentication schemes (see online version for colours)

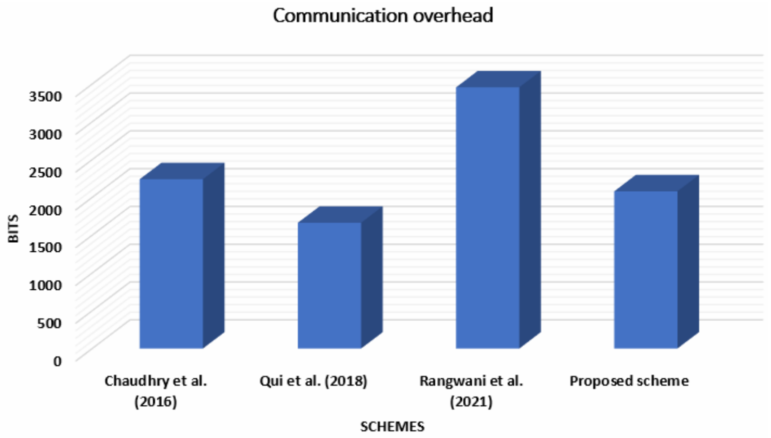
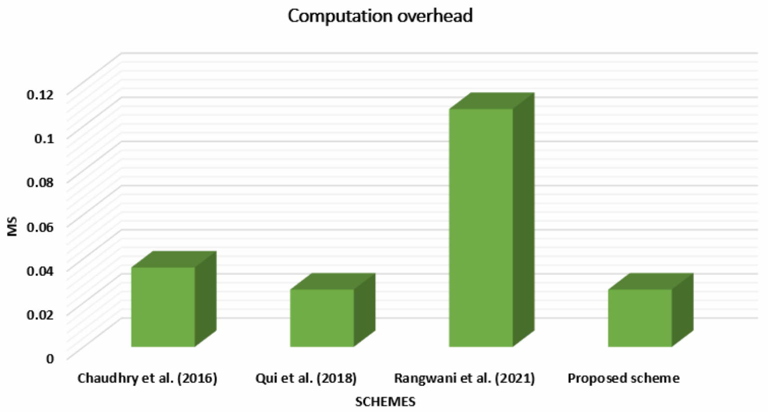


Figure 5 Comparative analysis of computation overhead among authentication schemes (see online version for colours)



7.1 Communication overhead

The reduced network congestion and faster message transmission can be achieved by designing authentication schemes with as low communication overhead as possible. To calculate the communication overhead of proposed approach, we consider the values of ECC point multiplication, symmetric key, random number, identities, hash function and timestamp are 320, 256, 128, 160, 160 and 32 bits respectively.

In this subsection, the proposed approach is compared with related approaches (Chaudhry et al., 2016; Qiu et al., 2017; Rangwani and Om, 2021) in terms of communication overhead. Figure 4 shows the comparative graph of communication overhead among the authentication schemes. In the proposed scheme, five messages are exchanged between the network entities, as listed below:

- $Msg_1 = \{M, G, I_d, Y_d\} = 640$ bits.
- $Msg_2 = \{Y_d, M_3, J_2, I_{fs}\} = 640$ bits.
- $Msg_3 = \{I_p, M_4\} = 320$ bits.
- $Msg_4 = \{I_{fs1}, M_5\} = 320$ bits.
- $Msg_5 = \{M_6\} = 160$ bits.

The total communication overhead of proposed approach is $\sum_{L=1}^{5} Msg_L = 2{,}080$ bits.

The comparative analysis of communication overhead between proposed approach and existing related schemes (Chaudhry et al., 2016; Qiu et al., 2017; Rangwani and Om, 2021) are illustrated in Table 3 and Figure 4. The results in Table 3 imply that our scheme has better communication overhead as compared to related schemes (Chaudhry et al., 2016; Rangwani and Om, 2021). Furthermore, the schemes (Chaudhry et al., 2016; Rangwani and Om, 2021) have several security challenges. The scheme (Chaudhry et al., 2016) suffers from offline password guessing attack and MITM attack. In addition, the scheme (Rangwani and Om, 2021) does not provide mutual authentication and untraceability. Although, the communication overhead of proposed scheme is little bit more than related scheme (Qiu et al., 2017). Nevertheless, the scheme (Qiu et al., 2017) does not provide mutual authentication. In addition, the scheme (Qiu et al., 2017) is vulnerable to offline password guessing attack. Therefore, it is concluded that our scheme has proper communication overhead while providing best security attributes among all related schemes.

7.2 Computation overhead ($65T_h$)

A high computational overhead should not be necessary for the efficient authentication scheme. The hash function is employed in the proposed scheme as compare to other expensing operations such as asymmetric encryption/decryption. The cryptographic operations such as time required for symmetric key encryption and decryption (T_{sked}), cryptographic hash function (T_h), ECC point addition (T_{padd}), modular inversion (T_{min}) and ECC point multiplication (T_{pmul}) are utilised to find the computation overhead (Mo and Chen, 2019). The cryptographic operation T_{pmul} is most computationally intensive operation. However, the proposed scheme is based on a single cryptographic operation, i.e., one-way hash function. Table 2 illustrates the various cryptographic operations with their execution time. Figure 5 shows the comparative graph of computation overhead among the authentication schemes.

Table 2 Cryptographic operations with execution time

Cryptographic operations	*Execution time (in ms)*
T_{sked}	0.109
T_h	0.0004
T_{padd}	0.0028
T_{pmul}	0.0035

Table 3 shows the proposed scheme requires computationally overhead of 65 hash function in total. Therefore, the total computational overhead of proposed scheme is $65T_h \approx 0.026$ ms. The scheme (Chaudhry et al., 2016) requires $9T_h + 7T_{pmul} + 1T_{padd} + 1T_{min} \approx 0.036$ ms in total. The scheme (Rangwani and Om, 2021) requires $17T_h + 6T_{pmul} + 10T_{padd} \approx 0.1078$ ms in total. Hence, it is found that the computational overhead of proposed scheme is lesser than the related schemes (Chaudhry et al., 2016; Rangwani and Om, 2021). However, the computational overhead of proposed scheme is similar than the scheme (Qiu et al., 2017). This is due to the fact that, the proposed scheme achieves mutual authentication through session key agreement between network entities, which is not feasible in the scheme (Qiu et al., 2017). Moreover, the proposed scheme is secure against the offline password guessing attack, which can not be prevented by scheme (Qiu et al., 2017).

Table 3 Performance comparison

Schemes	*Communication overhead (bits)*	*Computation overhead (ms)*
Chaudhry et al. (2016)	2,240	$9T_h + 7T_{pmul} + 1T_{padd} + 1T_{min} \approx 0.036$
Qiu et al. (2017)	1,664	$13T_h + 4T_{pmul} \approx 0.026$
Rangwani et al. (2021)	3,456	$17T_h + 6T_{pmul} + 10T_{padd} \approx 0.1078$
Ours	2,080	$65T^h \approx 0.026$

7.3 Comparison of security attributes

In this subsection, we compare our proposed authentication scheme with (Chaudhry et al., 2016, Qiu et al. (2017) and Rangwani and Om (2021) in terms of various security features. Table 4 shows that the proposed approach provides untraceability, anonymity, mutual authentication and resistance against MITM, replay, insider and offline password guessing attacks.

Table 4 Security attributes (SA) comparison

Schemes	*Chaudhry et al. (2016)*	*Qiu et al. (2017)*	*Rangwani and Om (2021)*	*Proposed scheme*
SA1	•	•	×	✓
SA2	✓	✓	✓	✓
SA3	✓	•	✓	✓
SA4	×	×	✓	✓
SA5	×	✓	×	✓
SA6	✓	✓	✓	✓
SA7	✓	✓	✓	✓
SA8	✓	×	✓	✓
SA9	✓	✓	×	✓

Notes: SA1: untraceability; SA2: replay attack; SA3: session key leakage attack; SA4: offline password guessing attack, SA5: MITM attack, SA6: perfect forward secrecy, SA7: anonymity, SA8: provides mutual authentication, SA9: Insider attack, ✓: provides security attributes and robust against the attacks, ×: does not provide security attributes and insecure against the attacks, •: not considered security attributes.

As seen in Table 4, the schemes (Chaudhry et al., 2016; Qiu et al., 2017) are vulnerable to offline password guessing attack and the schemes (Chaudhry et al., 2016; Rangwani and Om, 2021) are susceptible to MITM attack. We have found that the scheme (Rangwani and Om, 2021) is also suffer from the insider attack. Furthermore, the scheme (Qiu et al., 2017) does not provide mutual authentication. Therefore, the proposed scheme outperforms than existing related schemes.

8 Limitation and future scope

Security has received a lot of attention recently, and developing robust authentication protocols for the healthcare system is exceedingly difficult. We have presented anonymous authentication method for fog-assisted healthcare networks. We draw the following limitations about the authentication scheme based on our study: complex management of public key infrastructure and processing constraints. The major limitation in the proposed approach that we neglected to address the issue of computation energy. Future research must provide a solution to the energy computation. Recognise 'malicious behaviour' is usually preferable to direct research in the area of security in fog-enabled healthcare networks with minimal communication overhead. The proposed scheme is resilience against the several cryptographic attacks. However, it is impossible to propose a security solution for all cryptographic attacks. It might be useful to investigate new attacks on fog-assisted healthcare networks in the future. The study identifies new components that might be incorporated into authentication protocols to further improve the security of fog-assisted healthcare networks. We are looking into ways to promote our mutual authentication method in an environment with multiple servers. Moreover, we will work on the proposed scheme's practical application in a real computing environment. A test-bed network will be developed to verify communication cost and executing time. We are considering methods to expand intradomain authentication schemes; so that they take into account computing paradigms like dew computing and edge computing for future work.

9 Conclusions

A lightweight and efficient hash-based authentication approach is presented in fog-assisted healthcare networks. The hash function is extremely useful for resource constrained fog-enabled networks. In this scheme, patient and doctor are mutually authenticating themselves using fog server. The proposed approach is resilient against different threats, according to the informal security analysis. The formal security verification is conducted using ROR model, which gives additional detailed analysis for the cryptographic attacks. Finally, the performance of proposed scheme is also evaluated in terms of communication and computation overhead, which shows the proposed approach works well for fog-assisted healthcare networks.

References

Abbas, N., Asim, M., Tariq, N., Baker, T. and Abbas, S. (2019) 'A mechanism for securing IoT-enabled applications at the fog layer', *Journal of Sensor and Actuator Networks*, Vol. 8, No. 1, p.16.

Abi-Char, P.E., Mhamed, A. and El-Hassan, B. (2007) 'A secure authenticated key agreement protocol based on elliptic curve cryptography', *International Symposium on Information Assurance and Security*, IEEE, pp.89–94.

Al-Issa, Y., Ottom, M.A. and Tamrawi, A. (2019) 'eHealth cloud security challenges: a survey', *Journal of Healthcare Engineering*, Vol. 2019, No. 4, p.7516035.

Alizai, Z.A., Tareen, N.F. and Jadoon, I. (2018) 'Improved IoT device authentication scheme using device capability and digital signatures', *International Conference on Applied and Engineering Mathematics (ICAEM)*, IEEE, pp.1–5.

Alshehri, F. and Muhammad, G. (2020) 'A comprehensive survey of the internet of things (IoT) and AI-based smart healthcare', *IEEE Access*, Vol. 9, No. 2020, pp.3660–3678.

Amanlou, S., Hasan, M.K. and Bakar, K.A.A. (2021) 'Lightweight and secure authentication scheme for IoT network based on publish-subscribe fog computing model', *Computer Networks*, Vol. 199, No. 2021, p.108465.

Amin, R. and Biswas, G.P. (2015) 'An improved RSA based user authentication and session key agreement protocol usable in TMIS', *Journal of Medical Systems*, Vol. 39, No. 8, p.79.

Baig, A.F. and Eskeland, S. (2021) 'Security, privacy, and usability in continuous authentication: a survey', *Sensors*, Vol. 21, No. 17, p.5967.

Cai, Z., Wu, Z., Zhang, J. and Wang, W. (2021) 'Design and implementation of a cloud encryption transmission scheme supporting integrity verification', *International Journal of Embedded Systems*, Vol. 14, No. 3, pp.218–228.

Chaudhry, S.A., Naqvi, H., Shon, T., Sher M., and Sabzinejad M. (2015) 'Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems', *Journal of Medical System*, Vol. 36, No. 66, pp.1–11.

Chen, S., Chen, N., Tang, J. and Wang, X. (2020) 'Cognitive fog for health: a distributed solution for smart city', *International Journal of Computational Science and Engineering*, Vol. 22, No. 1, pp.30–38.

Hou, J.L. and Yeh, K.H. (2015) 'Novel authentication schemes for IoT based healthcare systems', *International Journal of Distributed Sensor Networks*, Vol. 11, No. 11, p.183659.

Ibrahim, M.H. (2016) 'OCTOPUS: an edge-fog mutual authentication scheme', *Int. J. Netw. Secur.*, Vol. 18, No. 6, pp.1089–1101.

Jalasri, M. and Lakshmanan, L. (2024) 'An improved data aggregation for fog computing devices in internet of things', *International Journal of Networking and Virtual Organisations*, Vol. 30, No. 2, pp.114–133.

Jia, X., He, D., Kumar, N. and Choo, K.K.R. (2019) 'Authenticated key agreement scheme for fog-driven IoT healthcare system', *Wireless Networks*, Vol. 25, No. 8, pp.4737–4750.

Jiang, R., Lai, C., Luo, J., Wang, X. and Wang, H. (2013) 'EAP-based group authentication and key agreement protocol for machine-type communications', *International Journal of Distributed Sensor Networks*, Vol. 9, No. 11, p.304601.

Kalaria, R., Kayes, A.S.M., Rahayu, W. and Pardede, E. (2021) 'A Secure Mutual authentication approach to fog computing environment', *Computers & Security*, Vol. 111, No. 2021, p.102483.

Kale, S., Tamakuwala, H., Vijayakumar, V., Yang, L. and Rawal Kshatriya, B.S. (2020) 'Big data in healthcare: Challenges and promise', *International Conference on Big Data and Cloud Computing Challenges. Smart Innovation, Systems and Technologies*, Springer, Vol. 164, pp.3–17.

Kumari, A., Tanwar, S., Tyagi, S. and Kumar, N. (2018) 'Fog computing for Healthcare 4.0 environment: opportunities and challenges', *Computers & Electrical Engineering*, Vol. 72, No. 2018, pp.1–13.

Lata, M. and Kumar, V. (2022) 'Security and privacy issues in fog computing environment', *International Journal of Electronic Security and Digital Forensics*, Vol. 14, No. 3, pp.289–307.

Liu, C.L., Tsai, W.J., Chang, T.Y. and Liu, T.M. (2018) 'Ephemeral-secret-leakage secure ID-based three-party authenticated key agreement protocol for mobile distributed computing environments', *Symmetry*, Vol. 10, No. 4, p.84.

Loffi, L., Westphall, C.M., Grüdtner, L.D. and Westphall, C.B. (2019) 'Mutual authentication for IoT in the context of fog computing', *International Conference on Communication Systems & Networks (COMSNETS)*, IEEE, pp.367–374.

Mehta, N. and Pandit, A. (2018) 'Concurrence of big data analytics and healthcare: a systematic review', *International Journal of Medical Informatics*, Vol. 114, No. 2018, pp.57–65.

Milioris, K., Konstantopoulos, C., Papageorgiou, K. and Skordoulis, M. (2022) 'The use of healthcare information systems: a research study about health professionals' needs', *International Journal of Healthcare Technology and Management*, Vol. 19, No. 1, pp.77–89.

Mishra, D., Rana, S., Goyal, C. and Singh, G. (2023) 'FOESG: anonymous session key agreement protocol for fog assisted smart grid communication', *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 42, No. 3, pp.137–147.

Mo, J. and Chen, H. (2019) 'A lightweight secure user authentication and key agreement protocol for wireless sensor networks', *Security and Communication Networks*, Vol. 2019, No. 1, pp.1–17.

Mohit, P., Amin, R. and Biswas, G.P. (2021) 'An e-healthcare authentication protocol employing cloud computing', *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 36, No. 3, pp.155–168.

Mukherjee, M., Shu, L. and Wang, D. (2018) 'Survey of fog computing: fundamental, network applications, and research challenges', *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 3, pp.1826–1857.

Naik, K.J. (2021) 'A cloud-fog computing system for classification and scheduling the information-centric IoT applications', *International Journal of Communication Networks and Distributed Systems*, Vol. 27, No. 4, pp.388–423.

Ni, J., Zhang, K., Lin, X. and Shen, X. (2017) 'Securing fog computing for internet of things applications: challenges and solutions', *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 1, pp.601–628.

Park, H.A. (2022) 'Security and privacy model of an electronic medical record system', *International Journal of Healthcare Technology and Management*, Vol. 19, Nos. 3–4, pp.303–323.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. and Ylianttila, M. (2014) 'PAuthKey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications', *International Journal of Distributed Sensor Networks*, Vol. 10, No. 7, p.357430.

Praveen Kumar, E. and Priyanka, S. (2023) 'A password less authentication protocol for multi-server environment using physical unclonable function', *Journal of Supercomputing*, Vol. 79, No. 18, pp.21474–21506.

Qiu, S., Xu, G., Ahmad, H. and Wang, L. (2017) 'A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems', *IEEE Access*, Vol. 6, No. 2017, pp.7452–7463.

Rajamanickam, S., Ramasubramanian, N. and Vollala, S. (2022) 'Insider attack prevention using multifactor authentication protocols – a survey', in *Applied Information Processing Systems: Proceedings of ICCET*, Springer Singapore, pp.331–339.

Rangwani, D. and Om, H. (2021) '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.

Santos, G.L., Gomes, D., Kelner, J., Sadok, D., Silva, F.A., Endo, P.T. and Lynn, T. (2020) 'The internet of things for healthcare: Optimising e-health system availability in the fog and cloud', *International Journal of Computational Science and Engineering*, Vol. 21, No. 4, pp.615–628.

Sathyaveti, H. and Gomathy, C. (2023) 'Edge computing-based internet of medical things for healthcare using deep learning', *International Journal of Embedded Systems*, Vol. 16, No. 2, pp.117–125.

Shamshad, S., Ayub, M.F., Mahmood, K., Kumari, S., Chaudhry, S.A. and Chen, C.M. (2022) 'An enhanced scheme for mutual authentication for healthcare services', *Digital Communications and Networks*, Vol. 8, No. 2, pp.150–161.

Shao, T. and Chen, X. (2020) 'Hash-based and privacy-aware movie recommendations in a big data environment', *International Journal of Embedded Systems*, Vol. 13, No. 1, pp. 1-8.

Sharma, G. and Kalra, S. (2019) 'A lightweight user authentication scheme for cloud-IoT based healthcare services', *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, Vol. 43, No. 1, pp.619–636.

Sharma, V., Chauhan, A., Saxena, H., Mishra, S. and Bansal, S. (2021) 'Secure file storage on cloud using hybrid cryptography', *International Conference on Information Systems and Computer Networks (ISCON)*, IEEE, pp.1–6.

Singh, P. and Chauhan, R.K. (2017) 'A survey on comparisons of cryptographic algorithms using certain parameters in WSN', *International Journal of Electrical & Computer Engineering*, Vol. 7, No. 4, pp.2088–8708.

Srinivas, J., Das, A.K., Kumar, N. and Rodrigues, J.J. (2019) 'TCALAS: temporal credential-based anonymous lightweight authentication scheme for internet of drones environment', *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 7, pp.6903–6916.

Tuli, S., Basumatary, N., Gill, S.S., Kahani, M., Arya, R.C., Wander, G.S. and Buyya, R. (2020) 'HealthFog: an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments', *Future Generation Computer Systems*, Vol. 104, No. 2020, pp.187–200.

Verma, U. and Bhardwaj, D. (2022) 'A secure lightweight anonymous elliptic curve cryptography-based authentication and key agreement scheme for fog assisted-internet of things enabled networks', *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 23, p.e7172.

Wazid, M., Das, A.K., Kumar, N. and Vasilakos, A.V. (2019) 'Design of secure key management and user authentication scheme for fog computing services', *Future Generation Computer Systems*, Vol. 91, No. 2019, pp.475–492.

Zeng, Z., Chang, L. and Liu, Y. (2022) 'A fault tolerance data aggregation scheme for fog computing', *International Journal of Information and Computer Security*, Vol. 17, Nos. 3–4, pp.351–364.

Zhang, X.G., Yang, G.H. and Wasly, S. (2021) 'Man-in-the-middle attack against cyber-physical systems under random access protocol', *Information Sciences*, Vol. 576, No. 2021, pp.708–724.