Mutual Authentication Security Scheme in Fog Computing

Gohar Rahman[1], Chuah Chai Wen[2]
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
86400, Johor Malaysia

Abstract*—Fog paradigm is a new and emerging technology that extends the services of cloud computing near to edge network. This paradigm aims to provide rich resources near to edge devices and remove the deficiencies of cloud computing for example, latency. However, this paradigm is distributed in nature and does not guarantee the trustworthiness and good behavior of edge devices. Thus, authentication and key exchange are significant challenges in front of this new paradigm. The researchers have worked on different authentication and key exchange protocols. Recently Maged Hamada Ibrahim proposed an authentication scheme that permits fog user to authenticate mutually with fog server under the authority of a cloud service provider. Alongside, Amor et al proposed an anonymous mutual authentication scheme. In this scheme, the fog user and fog server authenticate each other without disclosing the user real identity, using public-key cryptosystem. But, we demonstrated that Maged Hamada Ibrahim does not preserve the user anonymity, hence, it was exposed to man in the middle attack. Amor et al. scheme is computationally complex as it is using public key cryptosystem that has low throughputs and requires large memory, which not suitable to employ for fog computing that connecting internet of things with small memory, and requires high throughputs. Therefore, to overcome the above-aforementioned security problems internet of things constraints, an improved mutual authentication security scheme based on advanced encryption standard and hashed message authentication code in fog computing has been proposed. Our scheme provides mutual authentication between internet of things devices and fog servers. We proved that the proposed improved scheme provides secure mutual authentication using the widely accepted Burrows Abdi Needham logic. In this study, the properties i.e. performance, security, and functionality are analyzed and compared with existing and related mutual authentication schemes. Our scheme provides better in security, functionalities, communication and computation cost as compared with the existing schemes.

Keywords*—*Fog computing; mutual authentication; man in the middle attack; key exchange; ban logic

I. INTRODUCTION

Fog computing is decentralized computing architecture where the data is processed between the internet of things (IoT) devices and cloud servers. This computing paradigm brings the services of cloud computing near to the edge devices. The edge devices i.e. switches, routers and gateways act as computing nodes along with the cloud data center [1]. Compared to cloud computing, the computations of fog computing provide better results (location awareness, geographical accessibility, low latency, mobility support, etc.). It is because the fog computing nodes are near to the IoT devices. A typical IoT cloud architecture works in three phases. IoT devices reside in the first phase where sensors collect the information and forward the collected information to the cloud servers. In the second phase, cloud servers analysed the received information. In the third phase, the cloud servers processed the information and send back to the IoT devices. In this case, cloud computing compromise on high latency, security, and privacy of data [2][3].

Like the cloud, fog computing gives processing and storage services to the IoT users. Fog computing depends on giving processed information and storage locally to the fog devices as opposed to sending them to the cloud [4]. The architecture of fog computing consists of three-layers as well. The first layer contains IoT devices such as sensors, actuators wearable devices, smartphone, smartwatches, etc. The second layer called the middle layer consist of fog nodes where the computation is performed in a real-time manner. The last layer includes the cloud server where the data is stored for future use [5]. Fog computing is believed to be an extension of cloud computing and the security problems in the cloud are inherited to fog computing. As fog computing is decentralized in nature, therefore, the same methods applying to cloud computing is not applicable in fog computing [6, 7]. In fog computing, when a user opens their resources, the attackers easily comes and attacked on the fog nodes [8]. One of the important malicious attack is man in the middle attack (MitM) [9, 10]. In this type of attack, the attacker is passed out through malicious inner user between two computers, secretly relays, and pretends himself to be the legitimate [11, 12].

MitM can be either categorized as eavesdropping and manipulation. Eavesdropping is a passive attack as the attacker is merely concerned in the information passed. While in manipulation attack, the attacker makes changes in data sent to it and pretend it as the original sender. Detection and preventions of MitM attacks are critical in fog computing [13, 14]. The architecture of fog is characteristically analogous to a MitM attack, as fog node is intermediate in the cloud and IoT devices, allowing the attacker to camouflage easily. Nodes of fog transform personal information intensely like the medical history of a patient, prescription and health status of a person. Whatever the case is, such kind of information might prove terrible in the erroneous hands [15]. Therefore, the security must need necessary while designing fog computing specially in the edge fog layers.

MiTM attack can be prevented with mutual authentication [16]. Where the literature reveals that none of the mutual authentication protocols cannot attain the complete security requirements in fog edge cloud environment. This work studies the protocol presented by Maged Hamada Ibrahim [17]. Maged Hamada Ibrahim scheme cannot resist MitM. Thus has motivated us to propose a modified mutual authentication protocol that achieves the weaknesses of Maged Hamada Ibrahim scheme. Our proposed mutual authentication scheme may resist known security attacks and offer better functionalities. For example (a) user anonymity, (b) mutual authentication and session key establishment, (c) less computation cost. The proposed scheme is using the hash message authentication code (Hmac) for integrity and authenticity between fog users and fog servers. For authentication between fog servers and registration authority, public key infrastructure (PKI) is used. Moreover, the advanced encryption standard (AES) is used for encryption and decryption. Lastly, key derivation function (KDF) is used for session key creation to establish secure communication between fog user and fog server.

The rest of the paper is divided into sections. Related work is discussed in Section 2. A brief overview of the Maged Hamada Ibrahim scheme is presented in Section 3. The proposed mutual authentication scheme is discussed in Section 4. Security services of the proposed scheme are discussed in Section 5. The mutual authentication security proof based on Ban logic is presented in Section 6. The security functionalities and computation comparison of the proposed mutual authentication are discussed in Section 7 and Section 8. In the end, Section 9 counts the conclusion.

II. Related Work

Amor et al. [18] proposed an anonymous mutual authentication scheme where the fog user and the fog server authenticate each other without disclosing the user real identity using public-key cryptosystem. According to Albakri et al. [19], the computation cost of a public-key cryptosystem is high. The internet of things has limited memory, processing, and battery power. Therefore, this scheme is impractical in fog computing.

A framework was proposed by Dsouza et al. [20] based on policy-based security in fog computing. The proposed framework was intended to support the secret exchange of information, collaboration and reuse of data in a fog computing. The framework uses attribute-based authentication where first the fog user will be detected and then accesses the resources or services based on the fog user attribute. The framework comprises of numerous modules. The fundamental goal of these modules is to define rules and store them for user services and to send information to various fog nodes. The authors stated that these modules are important for real-time computation, and one of the modules is referred to as a policy enforcement module that is mapped to either fog nodes, cloud data servers or IoT devices. However as stated by the authors, this is a preliminary framework which does not take into account all the nuances of the federal fog ecosystem.

Jimoh and Abdul Hamid [21] proposed a conceptual framework in fog computing, based on swarm intelligence optimization technique also known as dragonfly algorithm. The main aim of the proposed framework is to detect the man in the middle attack (MitM) in fog computing. The authors used ifog simulator to detect the presence of MitM in the fog-computing environment. The authors considered two scenarios to determine the threshold consumption of CPU in MitM. In the first scenario, the memory consumption is tested without the presence of MitM between fog and cloud. While the second scenario is tested when there is a MitM attack takes place. The author claimed that the memory consumptions is less in normal communication as compared to the scenario where the MitM attack take place. However, this study is only based on preliminary results and outcomes. There is no solution to prevent the MitM attack in fog cloud IoT environment.

Alwaris et al. [22] proposed an efficient key exchange protocol based on ciphertext policy attribute encryption scheme (CP-ABE) for securing groups of fog nodes and cloud. To achieve better results in term of confidentiality, authentication, verifiability and access control they integrate CP-ABE with the digital signature. But Nikkah et al. [23] claimed that the aforesaid algorithm might be deliberated for obtaining the security of fog nodes and cloud because they are usually resourced consuming and are not appropriate for deployment in the IoT layer of the fog computing architecture.

Lee et al. [24] explored various unique security and privacy problems such as man in the middle attack (MitM), malicious detection technique, intrusion detection, data protection, and data management problems. However, the authors ignored the proper solutions that tackle these problems.

Lu et al. [25] proposed a lightweight privacy- preserving data aggregation scheme (LPDA) in fog computing. This scheme use three-techniques, namely, one-way hash chain, homomorphic Paillier encryption, and Chinese Remainder Theorem. The main goal of the scheme is to prevent data injection attack in the network edge. Besides, the scheme provides better results in terms of communication overhead and computation cost as compared to the basic paillier encryption scheme. However, the limitation of this scheme is that the traceability is not considered.

Stomojo et al. [26] highlighted different features of fog computing in smart grid, smart homes, and traffic control system. They examined the stealthy feature of man in the middle attack (MitM) on CPU and other memory consumptions fog computing devices. The authors explained that MitM is easy to be detected but difficult to be addressed. This study not gives any proper solution to prevent the MitM.

III. Review on Maged Hamda Ibrahim Scheme [17]

This section briefly review “Octopus: An Edge-Fog Mutual Authentication Scheme” for fog computing environment proposed by Maged Hamada Ibrahim. The scheme has three main phases namely, system initialization phase, registration phase and authentication phase. We present the brief overview of these phases to understand the security weaknesses of Maged Hamada Ibrahim scheme.

A. System Initialization Phase

In this phase of the scheme, the system is initialized. Registration authority RA contains their own public key and private key (〖PK〗 _RA 〖,SK〗 _RA). Similarly, fog server also contain private key and public key PK_{FS}, SK_{FS}. Registration authority knows the public key PK_{RA} of fog server. The registration Authority RA picks a unique identity ID_{FS} for fog server, sends the ID_{FS} signed with RA signature key SK_{RA}.

B. Registration Phase

In this phase of the scheme the fog user with identity, ID_{FU} approaching to registered with the *RA*. While every fog network having identity ID_F and containing a set of fog servers having identity ID_{FS}. The registration process (as shown in Fig. 1) is discussed below.

Step1: Fog user FU shows his identity ID_{FU} to the *RA*.

Step2: Upon receiving the request, *RA* pick random master secret key name K_{FU}, and send it to fog user FU.

Step 3: Fog user *FU* receive, the message from registration authority RA and store the master secret key K_{FU} and ID_{FU} on his smart device/card.

Step 4: RA calculates the secret key of FS and FU where K^{FU-FS} =H $(ID_{FU}, ID_{FS}, K_{FU})$.

Step 5: Upon receiving the message from *RA*. The *FS* verify the signature using *RA* public key PK_{RA}. After successful verification, decrypts the received tuple and stores ID_{FU} and K^{FU-FS}.

C. Mutual Authentication Phase

This phase executes several steps to achieve mutual authentication and session key establishment for all parties involved in the fog network. All the steps of this phase is discussing below which is shown in Fig. 2.

Step 1: FU picks a random number r_{FU} and broadcast the message $(Hello, ID_{FU}, r_{FU})$.

Step2: When fog server FS is within the range of the fog user FU, the fog server FS checks the identity of fog user FU which is ID_{FU} . If the identity ID_{FU} of fog user FU is registered, the communication is continuing otherwise abort the communication.

Step3: FS fetches the key K^{FU-FS} for fog user FU.

Step 4: FS picks a random number r_{FS}.

Step 5: The FS encrypts the r_{FS} and r_{FU} using symmetric key K^{FU-FS} , replies with message $(ID_{FU}, ID_{FS}$, ID_F $E(K^{FU-FS}, r_{FS}$, $r_{FS})$ to fog user FU.

Step 6: Upon receiving the message from FS , FU calculates the symmetric key K^{FU-FS} locally where $K^{FU-FS} = H$ $(ID_{FU}, ID_{FS}, K_{FU})$. Secondly, FU decrypts the received tuples and checks for the validity of random number r_{FU}. If the check is failed the session is aborted. Otherwise, fog user picks the session key K_S. Encrypt the session keyK_S by using symmetric key K^{FU-FS} send the tuples ID_{FU}, ID_{FS}, K_{FU} , E $(K^{FU-FS}$, K_S , $r_{FS})$ to the FU.

Step 7: Upon receiving the message from *FU*, the *FS* decrypt the received tuples and check for validity of r_{FS} if the matched of r_{FS} successful the session key K_s will be accept otherwise session is rejected.

D. Weakness of Maged Hamda Ibrahim Scheme

The main drawback of the Maged Hamada Ibrahim is the identity of each *FU* and *FS* is publically transmitted on unsecure channel. Therefore, the attacker may perform a middle attack during communication between fog user and registration authority. When fog user sends their identity to the registration authority, the attacker compromised the identity of fog user and obtain the master secret key from the registration authority. While in the authentication phase, the identity of fog user is also transmitted on unsecure channel. The attacker in the middle get the identity of fog user and fog server and reached to obtain the session key among fog users and fog servers. Therefore, this scheme is unsecured due to man in the middle attack (MitM).

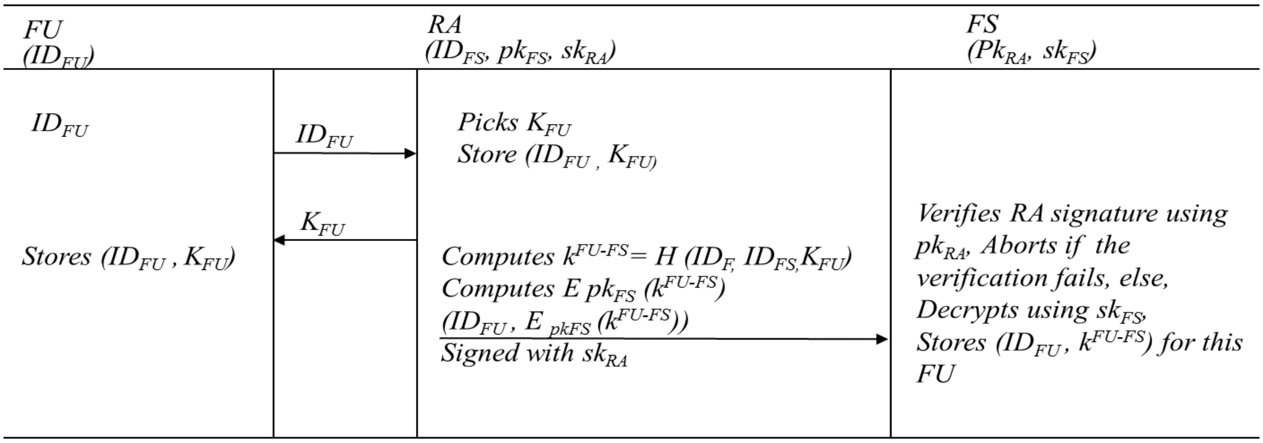
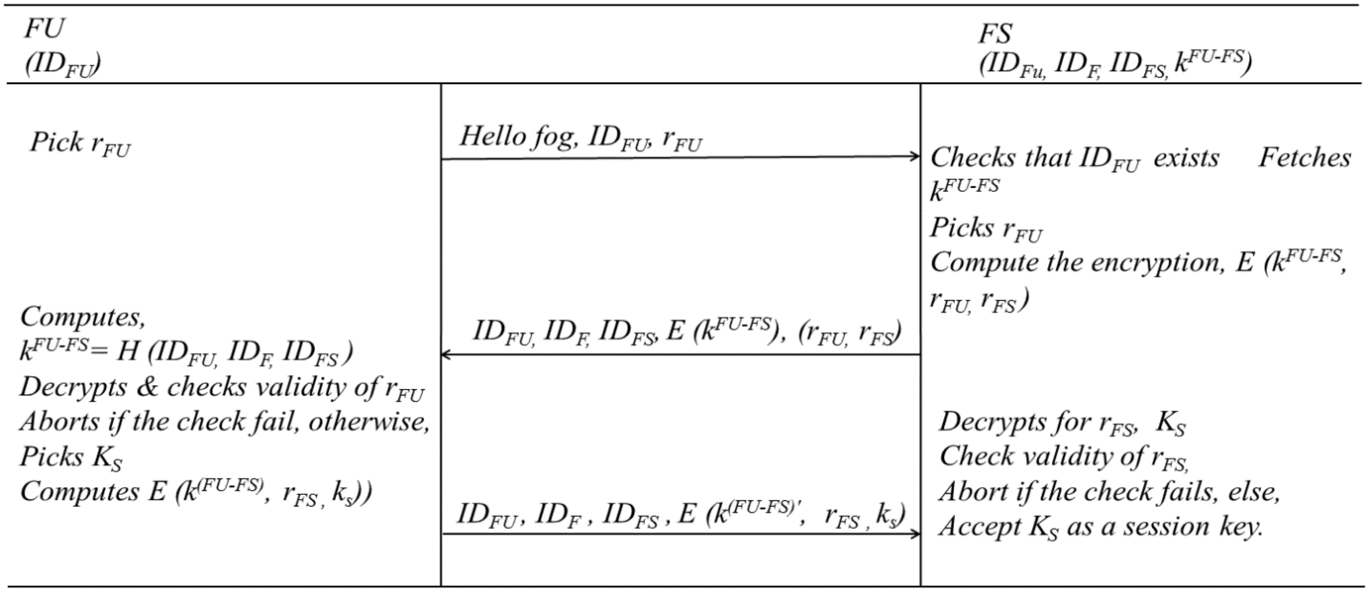

FU
(ID_{FU})
RA
$(ID_{FS}, pk_{FS}, sk_{RA})$
FS
(Pk_{RA}, sk_{FS})
ID_{FU}
ID_{FU}
Picks K_{FU}
Store (ID_{FU}, K_{FU})
K_{FU}
Stores (ID_{FU}, K_{FU})
Computes $k^{FU\text{-}FS}= H (ID_F, ID_{FS}, K_{FU})$
Computes $E\ pk_{FS}\ (k^{FU\text{-}FS})$
$(ID_{FU}, E_{pkFS}\ (k^{FU\text{-}FS}))$
Signed with sk_{RA}
Verifies RA signature using pk_{RA}, Aborts if the verification fails, else, Decrypts using sk_{FS}, Stores $(ID_{FU}, k^{FU\text{-}FS})$ for this FU

Fig. 1. Registration Phase of the Maged Hamda Ibrahim Scheme [17].

RMC Universiti Tun Hussein Onn Malaysia (UTHM)



FU *(ID_{FU})*		*FS* *($ID_{Fu,}$ $ID_{F,}$ $ID_{FS,}$ $k^{FU\text{-}FS}$)*
Pick r_{FU}	*Hello fog, ID_{FU}, r_{FU}* →	*Checks that ID_{FU} exists Fetches $k^{FU\text{-}FS}$* *Picks r_{FU}* *Compute the encryption, E ($k^{FU\text{-}FS}$, $r_{FU,}$ r_{FS})*
Computes, *$k^{FU\text{-}FS}$= H ($ID_{FU,}$ $ID_{F,}$ ID_{FS})* *Decrypts & checks validity of r_{FU}* *Aborts if the check fail, otherwise,* *Picks K_S* *Computes E ($k^{(FU\text{-}FS)}$, $r_{FS\,,}$ k_s))*	← *$ID_{FU,}$ $ID_{F,}$ ID_{FS}, E ($k^{FU\text{-}FS}$), ($r_{FU,}$ r_{FS})* *ID_{FU}, ID_F , ID_{FS} , E ($k^{(FU\text{-}FS)'}$, $r_{FS\,,}$ k_s)* →	*Decrypts for r_{FS}, K_S* *Check validity of $r_{FS,}$* *Abort if the check fails, else,* *Accept K_S as a session key.*

Fig. 2. Mutual Authentication Phase of the Maged Hamda Ibrahim Scheme [17].

IV. Proposed Scheme

This section briefly discussed the proposed mutual authentication scheme for fog computing to overcome the security weaknesses of Maged Hamada Ibrahim that is discussed in Section 3. The proposed scheme provides a lightweight strong mutual authentication among the fog users and fog servers. Our proposed scheme also divided into three phases as in the Maged Hamada Ibrahim, namely, 1) System initialization phase, 2) fog user registration phase, 3) Mutual authentication and session key exchange phase. Table I referred to the notations used the proposed scheme. Each phase of the proposed scheme is discussing below in details.

A. System Intialization

Before fog user registration, the registration authority RA has to perform system initialization phase. The *RA* has public key PK_{RA} and private keys SK_{RA} and K_{FU-RA}. The *RA* public key PK_{RA} is known to the *FS*. Fog server *FS* has also public key PK_{FS} and private key SK_{FS}. We assumed that, the *RA* private key $\mathrm{K_{FU-RA}}$ is shared with *FU* in advance.

TABLE. I. Notations used in the Proposed Scheme

Symbols	Description
$K_{FU\text{-}FS}$	Master secret key
$K_{FU\text{-}RA}$	Secret key shared between *RA*, and fog user
PK_{FS},SK_{FS}	Public and private key of the fog server
ID_F	Identity of fog network
ID_{FS}	Identity of fog server
ID_{FU}	Identity of fog user
n_1,n_2, n_3	Random numbers
Ks	Session key
Ts	Timestamp
Hmac	Hash message authentication code
kdf	Key derivation function
||	Concatenation operator

B. Registration Phase

Registration phase is *FU* and *FS* registering themselves with *RA* as shown in the Fig. 3. The authentication process is carried out between *FU* and *FS* with the registration authority *RA* as follows:

Step1: $FU \to RA$: $E(K_{FU-RA}, ID_{FU}||n_1) = c$, $Hmac(K_{FU-RA}, c) = T_1$.

Each fog user *FU* generate a random number n_1. Compute c and T_1 . Bothe c and T_1 sends to the *RA*.

Upon receiving message, c ,T_1 . The *RA* computes the valid tag $\mathrm{T_1}'$. Compared with the received tag T_1. If it is valid tag *RA* decrypts the message $c, D(K_{FU-RA}\,, c)$ and stored the identity of fog user ID_{FU}.

Step 2: $RA \to FU$: $E(K_{FU-RA}, K_{FU-FS}||n_1) = c_1$,

$Hmac(K_{FU-RA}, c_1\,) = T_2$

RA picks a long-term master secret key K_{FU-FS} and encrypts it with random number n_1 by using shared symmetric key K_{FU-RA}. *RA* Sends the parameter $\mathrm{c_1}$ with the $Hmac$ tag T_2 where tag T_2= $Hmac(K_{FU-RA}, c_1\,)$ to *FU*.

Upon receiving the message c_1 and T_2. *FU* verifies the $\mathrm{T_2}'$ and compares it with the received tag T_2. If the verification successful, the *FU* decrypts c_1 using K_{FU-RA} and stored the long-term secret key K_{FU-FS} and ID_{FU}.

Step: 3: $RA \to FS$: $E(PK_{FS}, ID_{FU}, ID_{FS}, ID_F, K_{FU-FS})\ = c_2$,

$Sign(SK_{RA}, c_2) = sig_{C2}$

RA picks the ID_{FU}, ID_{FS} and long term secret key K_{FU-FS}. Encrypts it by using the public key of *FS*. *RA* signs the encrypted message by using his own secret key SK_{RA} and sends to the fog server FS . Upon receiving message c_2 and sig_{C2} . *FU* verifies the signature sig_{c2} by using public key

PK_{RA} of the *RA*. If the signature verified the *FS* decrypts the received message and stored the ID_F, ID_{FS} and long term secret key K_{FU-FS}.

C. Mutual Authentication

When a registered fog user *FU* want to access the services of fog server *FS, FU* needs to exchange a mutual authentication key request message to the *FS*. Fig. 4 shows the mutual authentication process and brief detail of the steps as follows.

Step1: $FU \rightarrow FS$: $Hmac(K_{FU-FS}, ID_{FU}||n_2 = T_3$.

FU generates the random number n_2 and sends the tag T_3 to FS where T_3=$(K_{FU-FS}, ID_{FU}||n_2$. Upon receiving the tag T_3. If tag T_3 is valid *FS* picks a random number n_3, identity ID_{FS}, and the identity of fog network ID_F.

Step2: $FS \rightarrow FU$: $Hmac(K_{FU-FS}, ID_{FU}||\ ID_F\ ||\ n_3) = T_4$

FS Computes tag T_4 where tag T_4= $Hmac(K_{FU-FS}, ID_{FU}||\ ID_F\ ||\ n_3))$ and sends tag T_4 to *FU*. Upon receiving the received tag T_4 from FS.The FU calculates and if the tag T_4 is valid FU generates current timestamp T_S and calculate the session key by using *KDF*. $kdf\ (\ ID_{FS}\ ||\ ID_F||\ K_{FU-FS}||T_S) = K_S$.

Step 3: $FU \rightarrow FS$: $Hmac(\ K_{FU-FS}\ , T_S) =\ T_5$.

FU sends the tag T_5 to FS, where the tag T_5= $(\ K_{FU-FS}\ ||T_S)$. FS calculates T_5' and verifies tag T_5. If the tag is valid *FS* calculates the session key K_S' such that $kdf\ (\ ID_{FS}\ ||\ ID_F||\ K_{FU-FS}||T_S) = KS'$ and store the session key for commutation between fog users and fog servers.

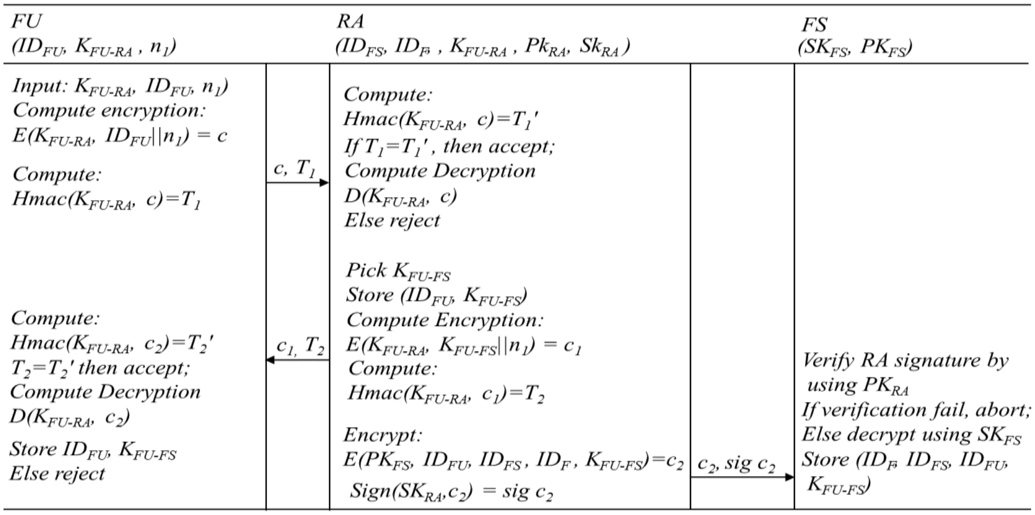


Fig. 3. Registration Phase of the Proposed Scheme.

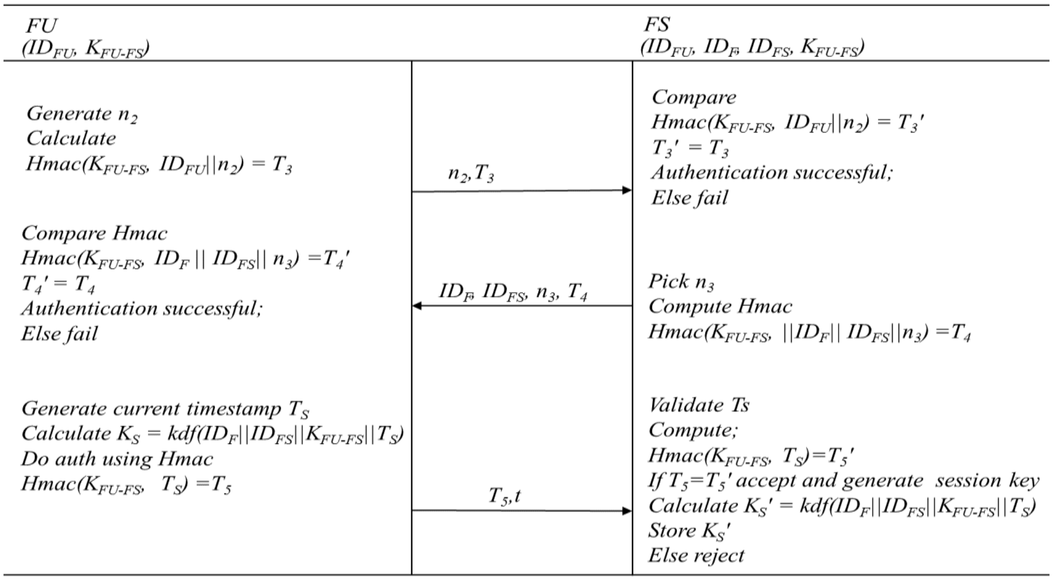

FU
(ID_FU, K_FU-FS)
FS
(ID_FU, ID_F, ID_FS, K_FU-FS)
Generate n_2
Calculate
Hmac(K_FU-FS, ID_FU||n_2) = T_3
n_2,T_3
Compare
Hmac(K_FU-FS, ID_FU||n_2) = T_3'
T_3' = T_3
Authentication successful;
Else fail
Compare Hmac
Hmac(K_FU-FS, ID_F || ID_FS|| n_3) =T_4'
T_4' = T_4
Authentication successful;
Else fail
ID_F, ID_FS, n_3, T_4
Pick n_3
Compute Hmac
Hmac(K_FU-FS, ||ID_F|| ID_FS||n_3) =T_4
Generate current timestamp T_S
Calculate K_S = kdf(ID_F||ID_FS||K_FU-FS||T_S)
Do auth using Hmac
Hmac(K_FU-FS, T_S) =T_5
T_5,t
Validate Ts
Compute;
Hmac(K_FU-FS, T_S)=T_5'
If T_5=T_5' accept and generate session key
Calculate K_S' = kdf(ID_F||ID_FS||K_FU-FS||T_S)
Store K_S'
Else reject

Fig. 4. Mutual Authentication Phase of the Proposed Scheme.

V. Security Services of the Proposed Scheme

A. Secure Mutual Authentication and Key Establishment

In our proposed scheme, the mutual authentication among fog users and fog servers is ensured based on hash message authentication code *Hmac*. During the registration phase, the fog user using random number encrypted with the identity of fog user. Similarly, *Hmac* tag is sent to the registration authority with cipher text, the attacker cannot deduce the valid tag. Thus the proposed scheme ensured the mutual authentication among fog servers and fog users. Also for mutual authentication phase the adversary may not be able to compute the valid tag because the adversary has no knowledge about the *Hmac* key. Thus in our proposed scheme, fog user securely start communication with the fog server using session key.

B. Resistance to Man in the Middle Attack (MitM)

In MitM attack, the active attacker attacks in the middle when two entities (*FU* and *FS*) exchange secret information. The attacker secretly forwards and receives secret parameters and messages. Suppose an attacker intercept the communication between the *FU* and the *RA*. The *FU* and *RA* using the message c, T_1. The aim of the attacker is to modify this message and make another valid message for example c' ,T_1' the attacker is not able to compute the valid tag $T_1{}'$ because the attacker does not know the Hmac secret key K_{FU-RA}. Similarly, the attacker also cannot modify other messages such like message 2, c_1, T_2 , message 3 , c_2,sig_{C2} message 4, T_3, message 5, T_4 and message 6 T_6. It is then clear that our improved mutual authentication scheme resist (MitM).

C. Anonymity

In our proposed scheme, the identity of *FU* and *FS* is transmitted in secure channel. During the registration phase of the *FU*, the identity is encrypted by using symmetric key K_{FU-RA} . While mutual authentication phase, the identity of *FU* and *FS* are associated with message authentication code (*Hmac)*. The attacker cannot recognize the transmitted identity during the registration phase because the attacker does not know the secret key used by the *FU* and *RA*. While during mutual authentication phase the attacker cannot extract the valid identity from the associated *Hmac* value. Therefore, our proposed scheme ensures the anonymity of the *FU.*

VI. Security Proof based on Ban Logic

To prove that our modified mutual authentication scheme fulfil the requirement of mutual authentication, we are using the Ban logic postulates (BAN) [27]. The notation of Ban logic is given in Table II.

A. Ban Logic Postulate

The logical postulates (rules) of the BAN logic are giving below.

1) Message meaning rules

$$\frac{A| \equiv A \overset{K}{\leftrightarrow} B \lhd \{C\}K}{A| \equiv B|{\sim}C}$$

2) The nonce verification rules

$$\frac{A| \equiv \#(C), A| \equiv B|{\sim}C}{A| \equiv B| \equiv C}$$

3) The belief rules

$$\frac{A| \equiv B| \equiv C, A| \equiv (C, D)}{A| \equiv C}$$

4) The freshness rules

$$\frac{A| \equiv \#(C)}{A| \equiv \#(C, D)}$$

5) The jurisdiction rules

$$\frac{A| \equiv B \Rightarrow C, A| \equiv B| \equiv C}{A| \equiv C}$$

To conduct the security of the modified mutual authentication scheme, the following process should be performed. First, we make the idealized messages of our improved mutual authentication scheme in the formal logic.

Second, we present the initial assumption based on the initial status of the improved mutual authentication scheme. Third, we set goals based on the improved mutual authentication scheme. Fourth, we prove the mentioned goals by using Ban logic postulate.

B. Idealized Messages of the Proposed Scheme

$$Message_1 : FU \rightarrow RA : \{n_1, FU \xleftrightarrow{ID_{FU}} RA\}K^{FU\text{-}RA}, (FU \xleftrightarrow{HMAC(K_{FU-RA,C})} RA)$$

$$Message_2 : RA \rightarrow FU : \left\{n_1, RA \xleftrightarrow{K_{FU\text{-}FS}} FU\right\} K_{FU\text{-}RA}, (RA \xleftrightarrow{HMAC(K_{FU\text{-}RA,C_1}} FU)$$

$$Message_3 : RA \rightarrow FS : (\{ID_{FU}, ID_F, ID_{FS}, K_{FU\text{-}FS}\}PK_{FS})SignSk_{RA}$$

$$Message_5 : FS \rightarrow FU, (FS \xleftrightarrow{HMAC(K_{FU\text{-}FS,ID_F,ID_{FS},n_3})} FU)$$

$$Message_6 : FU \rightarrow FS, (FU \xleftrightarrow{HMAC(K_{FU\text{-}FS,T_S})} FS)$$

TABLE. II. BANLOGIC NOTATIONS

Notation	**Descriptions**
A, B	Principals
C, D	Formulas
$A\| \equiv C$	A believes C
$\#C$	C is fresh
$A\| \sim C$	A one said C
$A \Rightarrow C$	A control over C
$A \lhd C$	A sees C
$A \overset{K}{\leftrightarrow} C$	A and B use the shared key K to communicate
$\{C\}K$	C is encrypted under K key
K_S	Represent Session key

C. Assumptions

Second the following assumption are made about the initial state of the scheme to analyse the proposed protocol where we have five assumption (*A1-A5*) which related with the public and private keys shared between the registration authority *RA*, fog user *FU* and fog server *FS*. The assumptions *A6-A9* shows that fog server *FS* and fog user *FU* believe that timestamp and random generated numbers elsewhere are fresh. This indicates that the protocol trusts heavily on the use of in time clocks. The final assumption *A10* indicates that both party have control the session keys shared between fog user and fog server.

$A1: FU \mid\equiv \left(FU \xleftrightarrow{K_{FU-RA}} RA\right)$

$A2: RA \mid\equiv \xrightarrow{PK_{FS}} FS$

$A3: FS \mid\equiv \xrightarrow{PK_{RA}} RA$

$A4: FU \mid\equiv \left(FU \xleftrightarrow{K_{FU-FS}} FS\right)$

$A5: FS \mid\equiv \left(FU \xleftrightarrow{K_{FU-FS}} FS\right)$

$A6: FU \mid\equiv \#(n_1))$

$A7: FU \mid\equiv \#(n_2)$

$A8: FS \mid\equiv \#(n_3)$

$A9: FU \mid\equiv \#(T_S)$

$A10: FS \mid\equiv FU \Rightarrow \left(FU \overset{KS}{\leftrightarrow} FS\right), \# \left(FU \overset{KS}{\leftrightarrow} FS\right)$

D. Goals

Third, we set four goals for our proposed scheme as shown below. The goals of our improved mutual authentication scheme contributes to exchange shared secret key K_{FU-FS} , session key K_S and identity of fog user ID_{FU} between two entities. Both entities have to believe that the other entity also believe on secret key K_{FU-FS} , session key K_S and identity of fog user ID_{FU}. The goal *G1* and *G3* is related to the identity of fog user *FU*. *G2* is related to the shared secret key between fog user *FU* and fog server *FS*. *G4* is related to session key shared between two parties (*FU*, *FS*).

$G1: FU \mid\equiv RA \mid\equiv \left(FU \xleftrightarrow{ID_{FU}} RA\right)$

$G2: FU \mid\equiv FS \mid\equiv \left(FU \xleftrightarrow{K_{FU\text{-}FS}} FS\right)$

$G3: FU \mid\equiv FS \mid\equiv \left(FU \xleftrightarrow{ID_{FU}} FS\right)$

$G4: FS \mid\equiv FU \mid\equiv \left(FU \overset{K_S}{\leftrightarrow} FS\right), \# \left(FU \overset{KS}{\leftrightarrow} FS\right)$

Fourth, the idealized form of the proposed protocol is analysed based on the BAN logic postulate. The main proof is stated as follows.

Step1: According to message 1, assumption A1 and message meaning rule we obtain L1.

$$\text{L1: } \frac{RA \lhd \{ID_{FU}, n_1\}K_{FURA}, (FU \xleftrightarrow{HMAC(K_{FU-RA,c})} RA}{RA \mid\equiv FU \mid\sim (ID_{FU}, n_1), (FU \xleftrightarrow{HMAC(K_{FU\text{-}RA,C})} RA}$$

Step2: According to message 2, assumption A1, and message meaning rules we obtain L2.

$$\text{L2: } \frac{FU \lhd, \{n1,\ K_{FUFS}\}K_{FURA}\ RA \xleftrightarrow{HMAC(K_{FU\text{-}RA,c_1})} FU\Big)}{FU \mid\equiv RA \mid \sim\{n1,\ K_{FUFS}\}K_{FURA}, RA \xleftrightarrow{HAMAC(K_{FU\text{-}RA},c_1)} FU}$$

Step3: According to message 3, assumption A2, A3, and public key-shared rules we obtain L3.

$$FS \mid\equiv \left(\xrightarrow{PK_{FS}} RA\right),$$

$$\text{L3: } \frac{FS \lhd (\{ID_F, ID_{FS}, ID_{FU}, K_{FU\text{-}FS}\}PK_{FS})SignSk_{RA}}{FS \mid\equiv RA \mid \sim(ID_F, ID_{FS}, ID_{FU}, K_{FU\text{-}FS})SignSk_{RA}}$$

Step4: From derivation of L2, L3, Assumptions A4, A5 and belief rules, we obtain L4.

$$\text{L4: } \frac{FU \equiv FS \mid\equiv \left(FU \xleftrightarrow{K_{FU\text{-}FS}} FS\right), ID_{FU,} ID_{FS, ID_{F,}}}{FU \equiv FS \mid\equiv \left(FU \xleftrightarrow{K_{FU\text{-}FS}} FS\right)}$$

This satisfied *G2*

Step5: According to assumption, A6 and freshness rule we obtain L5.

$$\text{L5: } \frac{FU \mid\equiv \#(n_1)}{FU \mid\equiv \#(ID_{FU}, n_1)}$$

Step6: From derivation of L1, L4 and belief rule we obtain L6.

$$\text{L6: } \frac{FU \mid\equiv RA \mid\equiv (ID_{FU}, n_1)}{FU \mid\equiv RA \mid\equiv (ID_{FU})}$$

This satisfied *G1*

Step7: According to message 4, assumption A4 and message meaning rule we obtain L7.

$$\text{L7: } \frac{FS \mid\equiv \left(FU \xleftrightarrow{K_{FU\text{-}FS}} FS\right), FS \lhd (FU \xleftrightarrow{HMAC(K_{FU\text{-}FS,\ ID_{FU}||n2})} FS)}{FS \mid\equiv FU \mid \sim HMAC(K_{FU\text{-}FS,\ ID_{FU}||n2})}$$

Step8: According to message5 and message meaning rule we obtain L8.

$$\text{L8: } \frac{FU \lhd (FU \xleftrightarrow{HMAC(K_{FU\text{-}FS, ID_F, ID_{FS}, n_3})} FS)}{FU \mid\equiv FS \mid \sim(FU \xleftrightarrow{HMA(K_{FU\text{-}FS,\ ID_F, ID_{FS}, n_3})} FS)}$$

Step9: From derivation of L7, L8 and nonce verification rules, we obtain L9.

$$\text{L9: } \frac{FU \mid\equiv \#(n_2, n_3),\ FS \mid \sim(ID_F, ID_{FS}, n_3)}{FU \mid\equiv\ FS \mid \sim(ID_F, ID_{FS}, n_3)}$$

Step10: From derivation of L9, assumption A7, A8 and freshness rules we obtain L10, L11.

L10: $$\frac{FU \mid\equiv \#(n_2)}{FU \mid\equiv \#(n_2, n_3)}$$

L11: $$\frac{FS \mid\equiv \#(n_3)}{FS \mid\equiv \#\left(n_{2,} n_3\right)}$$

Step11: From derivation of L7 and belief rule, we obtain L12.

L12: $$\frac{FU \mid\equiv FS \mid\equiv (ID_{FU}, n_2)}{FU \mid\equiv FS \mid\equiv (ID_{FU})}$$

This satisfied G3.

Step12: According to message 6 and message meaning rule we obtain L13.

L13: $$\frac{FS \lhd (FU \xleftrightarrow{HMAC(K_{FU\text{-}FS,T_S})} FS)}{FS \mid\equiv FU \mid\sim (FU \xleftrightarrow{HMAC(K_{FU\text{-}FS,T_S})} FS)}$$

Step13: According Assumption 9 and freshness rule we obtain L14.

L14: $$\frac{FU \mid\equiv \#(T_s)}{FU \mid\equiv \#(K_s, T_s)}$$

Step14: According to assumption A10 and jurisdiction rules we obtain L15.

L15: $$\frac{FS \mid\equiv FU \Rightarrow (FU \overset{KS}{\leftrightarrow} FS), FS \mid\equiv FU \mid\equiv \left(FU \overset{KS}{\leftrightarrow} FS\right)}{FS \mid\equiv \left(FU \overset{KS}{\leftrightarrow} FS\right)}$$

This satisfied G4.

Therefore goals *G1-G4* prove that our improved scheme achieve the mutual authentication between fog users and fog servers.

VII. Security Performance of the Proposed Scheme

Table III shows the security services of the existing schemes and our proposed scheme. The Maged Hamada Ibrahim scheme fail to provide the security services such as mutual authentication, user anonymity and cannot resist to the MitM. While the Amor model fulfils the security services, except for the lightweightedness. This model is computationally complex as compared to our scheme. It uses public-key encryption and decryption on the fog user, which is not lightweight for IoT devices In contrast; our proposed scheme provides the security services such as confidentiality, mutual authentication, message integrity, and user anonymity. We proved that our scheme can strongly resist to man in the middle attack using BAN logic as shown in section 6. Our proposed scheme and the Maged Hamada Ibrahim scheme are lightweight as they are using symmetric encryption, which requires less power for its operations and less power for its functioning.

TABLE. III. Security Performance of the Proposed Scheme

Scheme	**Maged scheme**	**Amor Scheme**	**Our Scheme**	
Services				
Mutual Authentication	no	yes	yes	
User anonymity	no	yes	yes	
man in the middle attack	no	yes	yes	
Message integrity	no	yes	yes	
Lightweight	yes	No	yes	

VIII. Computation Comparison of the Proposed Scheme with Closely Related Schemes

The computation comparison of the proposed scheme with other closely related schemes is shown in Table IV. After thorough analysis, our proposed scheme during the registration phase, the fog user only needs one encryption and decryption operations and two *Hmac* operations, while the registration authority performs one symmetric encryption and decryption operation and one asymmetric encryption. During the mutual authentication phase, the fog user needs two *Hmac* operations while on the fog server-side only two *Hmac* operation is performed. Amor model performed asymmetric encryption and decryption operations between the communication of fog user side and registration authority Thirdly the Maged Hamada Ibrahim scheme performed an asymmetric operation and one hash invocation during the registration phase, while in the authentication phase the model performed one symmetric operation and one hash invocation on the fog user. While in the fog server-side encryption and decryption process is executed. The conclusion, our scheme provides better security and less computationally as compared with the others closely related schemes.

TABLE. IV. Computation Comparison of the Proposed Scheme with Closely Related Schemes

Scheme	**Maged scheme[17]**			**Amor scheme[18]**			**Our scheme**		
Phase	***Initialization***	***Registration***	***Authentication***	***Initialization***	***Registration***	***Authentication***	***Initialization***	***Registration***	***Authentication***
FU	*-*		*1 sym enc* *1 sym dec* *1 hash*	*-*	*1 asy enc* *1 asy dec*	*asym enc*	*-*	*1 sym enc* *1 sym dec* *2Hmac*	*2Hmac* *1 KDF*
FS	*1 sign verif*	*1 sign verif* *1 asym dec*	*1 sym enc* *1 sym dec*	*-*	*1 sign verif* *1 asym dec*	*asym enc*	*-*	*1 sign verify* *1 asym dec*	*2Hmac* *1 KDF*
RA	*1 sign gen* *1 hash*	*1 asym enc* *1 hash* *1 sign verif*	*-*	*-*	*1 sign* *1 asy dec* *2 asym enc*		*-*	*1 sym enc* *1 sym dec* *2 Hmac*	

IX. Conclusion

In this paper, we have demonstrated that Maged Hamada Ibrahim scheme is vulnerable to (MitM) and it cannot provide mutual authentication and anonymity of the fog user. To overcome the weaknesses of Maged Hamada Ibrahim scheme we have proposed an improved mutual authentication security scheme for fog computing. Our modified improved scheme have resistance to various types of attacks. We proved that our modified improved scheme provides mutual authentication between fog user and fog server using BAN logic. We compared the modified mutual authentication scheme with the existing schemes and it shown that our modified mutual authentication scheme performs well in term of security and functionality requirements.

Acknowledgment

The authors would like to thank Information Security Interest Group (ISIG), Faculty of Computer Science and Information Technology (FSKTM) University Tun Hussein Onn Malaysia (UTHM) for recurrent assistance in executing this research study and, RMC UTHM, for financially supporting this Research under research Fund E15501.

References

[1] S. B. Nath, H. Gupta, S. Chakraborty, and S. K. Ghosh, “A survey of fog computing and communication current researches and future directions,” arXiv preprint arXiv, pp. 1-47, 2018.

[2] J. Ni, k. Zhang, X. Lin, and X. S. Shen, “Securing fog computing for internet of things applications: challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601-628, 2017.

[3] N. Abubaker, L. Dervishi, And E. Ayday, “Privacy-preserving fog computing paradigm,” IEEE Conf. on Communications and Network Security, pp. 502-509, October 2017.

[4] H. Atlam, R. Walters, and G. Wills, “Fog computing and the internet of things: a review,” big data and cognitive computing, vol. 2, no. 2, pp.10, 2018.

[5] M. Verma, N. Bhardwaj, and A. K. Yadav, “Real time efficient scheduling algorithm for load balancing in fog computing environment’. Int. J. Inf. Technol. Comput. Sci, vol. 8, no. 4, pp.1-10, 2016.

[6] B. Z. Abbasi, and M. A Shah, “Fog computing: Security issues, solutions and robust practices,” Int. Conf. on Automation and Computing (ICAC), 2017, pp. 1-6, September 2016.

[7] P. Kumar, N. Zaidi, and T. Choudhury, “Fog computing: Common security issues and proposed countermeasures,” 2016 Inte. Conf. System Modeling & advancement in research trends, pp. 311-315, November 2016

[8] Y. Sun, F. Lin, and N. Zhang, N “A security mechanism based on evolutionary game in fog computing,” Saudi journal of biological sciences, 2018, vol. 25, no. 2, pp. 237-241, 2018.

[9] C. Li, Z. Qin, E. Novak, and Q. Li, “Securing SDN infrastructure of IoT–fog networks from MitM attacks,” IEEE Internet of Things Journal, vol. 4, no.5, pp. 1156-1164, 2017.

[10] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing fog computing for internet of things applications: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601-628, 2017.

[11] G.Rahman, and C.C. Wen, “Fog computing, applications security and challenges, Review,” International Journal of Engineering & Technology, vol.7, no. 3, pp.1615-1621, 2018.

[12] .Y. Desmedt, “Man-in-the-middle attack. Encyclopedia of cryptography and security,” pp. 759-759, 2011.

[13] G.Rahman, and C. C. Wen, “Man in the Middle Attack Prevention for edg-fog, mutual authentication scheme,” International Journal of Recent Technology and Engineering (IJRTE), vol.8, no 2s2, July 2019.

[14] B. N. Ekanayake, M. N. Halgamuge, and A. Syed, “Security and privacy issues of fog Computing for the internet of things (IoT),” In Cognitive Computing for Big Data Systems Over IoT, Springer, Cham, , pp. 139-174, 2018.

[15] S. Khan, S. Parkinson, and y. Qin, “Fog computing security: a review of current applications and security solutions’, Journal of Cloud Computing, vol. 6 no. 1, pp.19, 2017.

[16] Z. Chen, S. Guo, R. Duan, and S. Wang, “Security analysis on mutual authentication against man-in-the-middle attack,” First Inte. Conf. on Information Science and Engineering, pp. 1855-1858, 2009.

[17] H. M. Ibrahim, “Octopus: An edge-fog mutual authentication scheme, IJ Network Security, vol. 18, no. 6 pp.1089-1101,2016.

[18] A.B. Amor, M. Abid, and A. Meddeb, “A Privacy- Preserving Authentication Scheme in an Edge-Fog Environment,” In IEEE/ACS 14th Int. Conf. on Computer Systems and Applications, , pp. 1225-1231, October 2017.

[19] A. Albakri, M. Maddumala, and L. Harn, “Hierarchical polynomial-based key management scheme in Fog Computing,”. 17th IEEE Inte.Conf. On Trust, Security and privacy in computing and communications, pp. 1593-1597, august 2018.

[20] C. Dsouza, G. J. Ahn, and M. Taguinod, “Policy-driven security management for fog computing: Preliminary framework and a case study,” In Proc. Int. Conf. on information Reuse and integration , pp. 16-23, august 2014.

[21] Y. S. Jimoh, and M. Abdulhamid, “Dragonfly algorithm-based detection technique for man-in-the-middle attack in fog Computing Environment: A Conceptual Framework,” Proceedings of the 1st national communication engineering conference , pp.1-6, 2018.

[22] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, “An attribute-based encryption scheme to secure fog communications,” IEEE access, vol .5, pp.9131-9138, 2017.

[23] B. P. Nikkhah, H. H. S. Javadi, T. Dargahi, and A. Dehghantanha, “A hierarchical key predistribution scheme for fog networks,” Computing, vol. 6, no.1 pp 1-14,2017.

[24] K. Lee, D. Kim, D. Ha, U.Rajput, and H. Oh, “On security and privacy issues of fog computing supported Internet of Things environment,” 6th Int. Conf. on the network of the future, pp. 1-3, September 2015.

[25] R. Lu, K. Heung, A. H. Lashkari, and A. Ghorbani, “A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT,” IEEE Access, vol. 5, pp. 3302-3312, 2017.

[26] I. Stojmenovic, and S. Wen, S, “The fog computing paradigm: Scenarios and security issues,” In Federated Conf. on Computer Science and Information Systems pp. 1-8, 2014.

[27] M. Burrows, M. Abadi, and R. Needham,R “A logic of authentication’, 1990, ACM Trans. Comput. Syst , vol. 8, no. 1, pp. 18-36, 1990.