Design of Lightweight Authentication Protocol for Fog enabled Internet of Things - A Centralized Authentication Framework

Upendra Verma[1], Diwakar Bhardwaj[2]

Department of Computer Engineering and Applications, GLA University Mathura, India

***Abstract*:** Internet is a large network of networks that spans the entire globe. Internet is playing indispensable role in our daily lives. The physical things are connected to internet with the help of digital identity. With recent advancement of information and communication technologies IoT became vital part of human life. However, IoT is not having standardized architecture. Nowadays IoT is integrated with fog computing which extends platform of cloud computing by providing computing resources on edges of computer network. Fog computing is motivated by IOT and It is decentralized solution for IoT. In addition, Fog computing has supported features like geographic distribution, low latency, location awareness, operate on premise, installed on heterogeneous hardware. IoT with cloud computing does not have such features. Therefore, in this paper, at first we discuss about the distributed fog computing architecture. Subsequently, we address the problem of authentication and design a new authentication framework for fog enabled IOT environment. It is stated that the proposed authentication framework will be useful in many IoT applications such as healthcare system, transportation system, smart cities, home energy management etc.

***Keywords*:** Authentication, Fog Computing, Cloud Computing, IoT

1. Introduction

IoT can be defined as a large network of networks connecting billions of devices to exchange real time information for providing intelligent services [1]. Many author proposed different definitions of IoT. The most popular definition of IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interface and are seamlessly integrated into the information network, often communicate data associated with users and their environments [2] and this definition has many keywords such as Self Configuring, Integrated into Information Network, Unique Identity, Interoperable Communication, Self-adapting and Dynamic Network. IoT is motivated by fog computing. Fog computing is a prototype campaigned by a few of the leading IoT technology players such as Dell, IBM, Cisco etc. Basically, fog computing is responsible for enabling quick response time, reducing network latency and traffic and supporting the backbone bandwidth saving to achieve a better QoS (Quality of Service) [3]. It is also supposed to selectively relay applicable data to the cloud. IDC predicts that by the end of 2025 about 45 percent of world's data would be moved closer to the network edge [4]. It is believed that fog computing is the only technology that can withstand AI, 5G, and IoT in the years to come. Fog Computing is not a replacement of Cloud computing but it's a complementary technology to cloud computing [5]. Fog computing is closer to IoT devices and provides computation and storage features nearer to the devices [6]. Table 1 illustrates the difference between Cloud Computing and Fog Computing and Table 2 provides the IoT challenges & how fog can help to overcome challenges.

Table 1. Comparison between Cloud Computing and Fog Computing

Cloud Computing	Fog Computing
Multiple hops	Single hop
No location awareness	Location awareness
No user defined security	User-defined security
Servers within Internet	Servers on edge of network
High latency	Low latency
Limited Mobility	Supported
Centralized Geographical Distribution	Distributed Geographical Distribution

Table 2. IoT Challenges and how fog assist challenge

IoT Challenges	How fog can assist the challenge
IoT Security and Privacy Challenges	Fog Computing acts as a proxy to update the software of resource constrained devices and privacy and security credentials.
Latency constraints	Fog act as an intermediary between cloud and resource constrained device. The fog server performs all computation operation close to IoT devices.
Network bandwidth constraints	Fog computing process data on edge of the network. Therefore, data does not travel from device to cloud and vice versa. This reduces the network traffic that needs to be sent to the cloud. This process saves consumption of network bandwidth.
Resource-constrained devices	Fog computing perform computation operations on the behalf of resource-constrained devices.

Authentication has achieved a great consideration within IoT security [7]. Authentication is important to check the validity of devices before sharing information with each other [8]. Mutual authentication between IoT devices and Fog server is an important part of secure fog computing enabled internet of things environment. In this paper TTP (trusted third party)

used as an authentication platform. In other words, TTP uses to attain registration of device, fog and cloud before they are installed in distributed network. In this paper, Three-way authentication procedure is adopted where central authority authenticates the two communication entities and provides help to mutually authenticate them. The authentication mechanism can provide following benefits to IoT:

- Strong anti-tampering and anti-counterfeiting
- Avoidance of humiliating data breaches
- Reduce risk of third party services
- Secure communication for users

The public key certification is widely used in current internet. This type of authentication is impracticable for constrained environment. Due to physical constraints of IoT devices such as limited computing power, limited memory space, limited energy etc., the heavy cryptographic schemes like asymmetric key based algorithm is not suitable for authentication. So, this type of algorithm is used between resource rich devices like fog-cloud communication. Therefore, in this paper we propose a framework for the authentication of IoT devices (Things), which are resource constrained in nature.

In order to design the authentication framework for fog enabled IoT, we use some of the cryptographic primitives like one-way hash function, random nonce and asymmetric cryptographic operations. In proposed framework, devices are authenticated with the help of fog and cloud server. So, the authentication procedure adopted here is three-way authentication procedure. This paper deals with the centralized authentication framework along with a protocol for fog computing enabled IoT environment. Figure 1 illustrates the architecture of fog enabled IoT environment.

The Authentication Procedure is composed of two parts-

i. Centralized authentication framework using cloud server, fog node and devices

ii. Lightweight Authentication protocol for fog enabled IoT environment

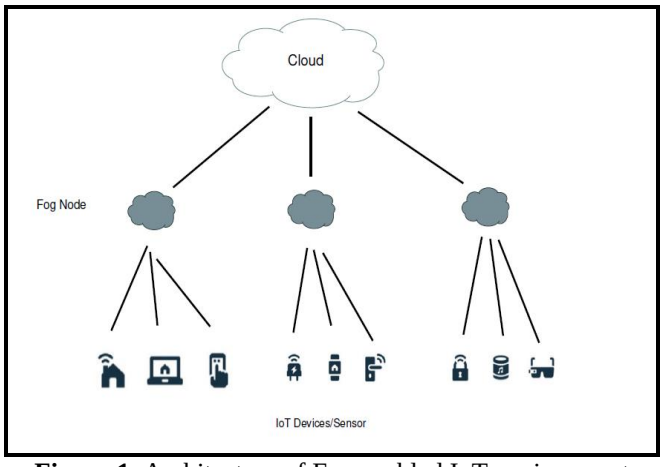

Figure 1. Architecture of Fog enabled IoT environment

The benefaction of this paper is manifold:

- An authentication framework for fog computing enabled IoT environment has been presented. An Authentication between fog node and cloud server using digital certificate has been presented.
- In centralized authentication, fog node is responsible to authenticate smart IoT devices.
- If smart device moves from one cluster to another cluster, then authentication in inter-cluster movement is invoked. In that case, cloud server is responsible to authenticate device.
- Authentication is achieved by using one-way cryptographic hash function and random nonce for IoT devices as they are resource constrained. On the other hand, concept of digital certificate is applied for fog server and cloud server as they have more resources.
- The authentication framework used Tree-Cluster strategy for the formation of distributed IoT architecture.
- In this paper, we consider dynamic topological environment for IoT device called Inter Cluster movement of devices.
- Finally, the Informal Security Analysis is presented.

The paper is organized as follow:

Section 2 provides the related research work. Section 3 proposes an authentication framework and security goals are discussed. Section 4 provides workflow of proposed authentication scheme along with the phases of authentication protocol. The security analysis and evaluation of authentication scheme are given in Section 5 and Section 6 respectively. Finally, concluding comments is given in Section 7.

2. Related Research Work

Recently many research articles have been reviewed state of the art of authentication scheme and framework and discussed promising distributed IoT application in various domains such as smart healthcare system, smart grid system, smart city, smart industrial automation, smart transportation etc. Authentication is the topmost countermeasure that have been proposed by researchers in order to prevent IoT security attacks [9]. Authentication is the vital issues for the security of fog computing enabled Internet of Things environment.

Li et al. [10] discussed a definition of fog computing, application scenario, big data analysis and potential issues in context of fog computing. Varghese et al. [11] presented comparison of cloud computing & fog computing and highlighted how fog computing can reduce the response time and data traffic between edge smart devices and cloud server. Sarkar and Mishra [12] presented a theoretical modelling of fog computing and given a comparison between fog computing and cloud computing in terms of energy consumption and service latency. Das et al. [13] demonstrated a lightweight authentication protocol which provides mutually authentication between wearable device and mobile terminal. Tiwari and Gupta [14] proposed a mutual authentication scheme between IoT device and server based on elliptic curve cryptography (ECC).

Roman et al. [15] studied several security challenges in distributed IoT application. As per their study, authentication and access control are vital security issues in distributed IoT architecture. Kothmayr et al. [16] introduced and discussed two-way authentication scheme for IoT. DTLS based authentication scheme is presented and in this scheme, the network is overloaded due to completion of DTLS handshake using transformation of eight message. Jang et al. [17] proposed a device authentication protocol without using CA for IoT. Author proposed a keyed hash algorithm in which Merkle hash tree is not appropriate for resource constrained devices in distributed IoT application. Ibrahim [18] presented a hierarchical architecture for edge, fog and

cloud computing. Three phases of authentication are discussed. Shahzad and Sing [19] investigated two strategies of authentication. First strategy focused on the authentication on devices that maintains continuous physical contact and Second strategy discussed authentication on devices that don't maintain permanent physical contact. Based on their study, providing authentication is difficult for those devices that don't maintain permanent physical contact. Chen et al. [20] proposed a three-phase authentication scheme called PriAuth. The scheme based on elliptic curve diffie-hellman (ECDH) key exchange protocol to ensure the secrecy of key and the scheme helps to secure smart healthcare system. PriAuth is a centralized authentication scheme and central point may be compromised due to single point of attack. Hou and Yeh [21] illustrated sensor tag based communication architecture for future IoT based healthcare service system. In this scheme, author proposed SSO based authentication scheme and TTPA is responsible to authenticate devices. SSO based authentication is not suitable for resource constrained environment and TTPA may be compromised due to single point of attack. The aforementioned authentication schemes have some problem such as single point of attack, they don't support resource constrained nature of IoT application.

Keeping in view of the previous study on authentication scheme in the field of Internet of Things, we proposed a new centralized authentication framework for Internet of Things. The proposed framework and authentication protocol is suitable for fog enabled IoT environment.

3. The Proposed Authentication Framework, Security goals and Notations

3.1 Authentication Framework

Figure 2 illustrates the proposed system framework, where our proposed authentication scheme is modelled. In the given framework, Assume that N_c Cloud Server CS_i ($i=1,2,3,\ldots..N_c$), N_f fog servers FS_j ($j=1,2,3\ldots..N_f$) and N_d smart devices SD_k ($k=1,2,3\ldots\ldots..N_d$) are deployed in the network. In network, SD_k (smart devices) are group within a cluster.

In the proposed framework, two types of communication are existing:

(i) Cloud to Fog communication and vice versa

(ii) Fog to Device communication and vice versa.

With respect to various IoT application domain such as smart transportation system, smart healthcare system etc., our proposed framework exists as centralized approach, not a distributed approach. So the proposed scheme is known as centralized authentication framework for fog computing enabled IoT environment. The proposed framework is designed for the authentication of device with the help of lightweight cryptographic primitive's hash function and random nonce.

All smart device will get security credentials from fog server. On the other hand, fog servers will get security credentials from cloud server. In this framework, fog node is responsible to authenticate IoT device when device moves from one cluster to another. Only the particular fog server where device has been registered can know the original id and movement. On the other hand, In our proposed framework each cluster is assumed as network region. When a device moves from one cluster to another then the fog server verifies the device with the help of cloud server and then decided whether IoT device can join into cluster or not.

In the proposed framework, two network elements are resource rich elements (i.e. fog server and cloud server) and one highly resource constrained network element (i.e. IoT device) are considered. Here Tree-Cluster formation of network is assumed, where fog node is the controlling device for IoT devices in a particular cluster. The major concern of proposed framework is the authentication between resource constrained entity (IoT device) and resource rich entity (fog server). Here one of the known IoT protocol 6LoWPAN is considered for the identity of IoT device. Device and fog server can mutually authenticate and establish secure communication link in centralized environment. Our proposed system framework can be useful in various distributed IoT application such as smart healthcare based distributed IoT system, Mobile oriented distributed IoT system, Distributed IoT application for factory automation etc.

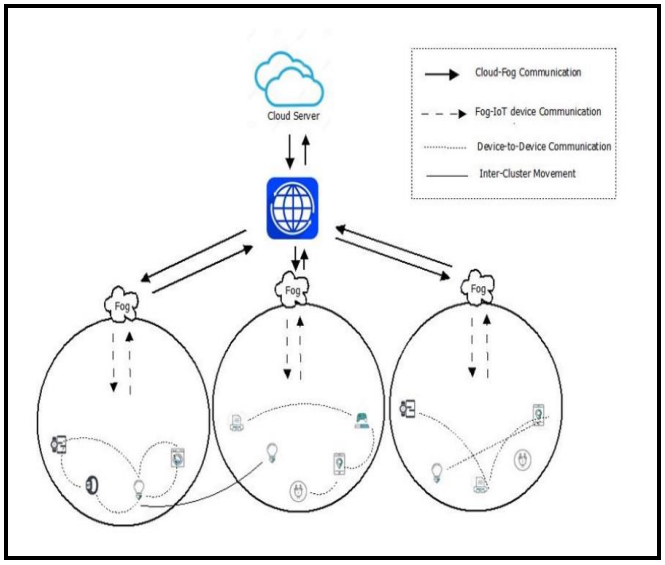

Figure 2. Proposed System Framework

3.2 Security Goals

The general security requirements that are crucial to provide security for fog enabled IoT environment-

- Confidentiality: It is about to controlling for device access.
- Integrity: Original message is not tampered.
- Availability: System should be available for legitimate entities.
- Non-repudiation: Assurance that someone cannot deny something.
- Authentication: Proof of identities.
- Authorization: Process of giving someone permission to do something
- Access Control: Regulates who or what can view or use resources in a computing environment

Based on aforesaid security requirements, various attacks should be prevented by the help of device authentication protocol for fog enabled IoT services. The following listed attacks need to be protected in the authentication scheme designed for fog computing services:

i. Replay attack: Network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

ii. Man in the middle attack: Attack where the attacker secretly relays and possibly alters the communications between two parties.

iii. Eavesdropping: Network attack where attackers try to steal your private information.

iv. Side Channel attack: Attackers extract the secrets from system through analysis of physical parameters.

v. Brute force attack: Attacks that relies on guessing possible combination of targeted password until the correct password is discovered.

The shortened form and notations used in this paper are defined in the Table 3.

Table 3. Notations used in this paper

Notation/Symbol	Definition
T_i	i^{th} Thing
F_j	j^{th} Fog
CS_k	k^{th} Cloud Server
ID_t	Identity of Thing
Ku_t	Thing Public Key
ID_f	Identity of Fog Node
Ku_f	Public Key of Fog Node
Kr_f	Private Key of Fog Node
Ku_{cs}	Public Key of Cloud Server
Kr_{cs}	Private Key of Cloud Server
H(IPV6)	Hash Identity of Thing
N1, N2, N3	Random Nonce

4. Workflow of Proposed Authentication Scheme

Figure 3 illustrates process flow diagram of proposed authentication scheme. In order to establish trusted communication in a network, efficient and effective authentication procedure should be applied between communicating elements (device, fog node, cloud server). Our proposed authentication scheme consists of five phases: Pre-deployment phase, Fog-Cloud Authentication, Thing/Device registration phase, Fog-Thing mutual authentication phase, Authentication in inter cluster movement phase. We assume that ID of fog node is preloaded into cloud server. This can be achieved easily because fog node is a part of cloud server.

A. Phase I – Pre-deployment phase

In this phase TTP (trusted third party) to attain registration of cloud, fog and device before they are installed in distributed network. In the proposed scheme, key establishment is based on asymmetric cryptography algorithm and Hash algorithm is used to generate hash value. Cloud server generates public/private key pair for device using asymmetric cryptography and Fog server generates its own pair of keys (Public/Private keys) using asymmetric cryptography. We assume that cloud public key is hardcoded in each IoT devices at the time of manufacturing.

B. Phase II – Authentication between Fog Node and Cloud Server

In this phase, fog node and cloud server are mutually authenticated with each other. Fog node sends their ID_f along with their public key which are encrypted with public key of cloud E ($Ku_{cs.}$ [ID_f || K_{uf}]). After receiving message, cloud server decrypts the message using cloud's private key and get ID of fog node and Fog Node's public key. By comparing decrypted Fog Node's ID and Fog Node's Public Key, cloud server will verify the identity of fog node. After verification of fog node's identity, cloud responds with a message which is encrypted with cloud's private key (E(Kr_{cs} [ID_f || Ku_f || H(ID_f || Ku_f)])). This message is called certificate which is generated by cloud server. Where H(ID_f || Ku_f) represents hash identity of fog node. After receiving message from cloud server, fog node decrypts the message using cloud's public key and verify the identity of cloud server because only legitimate cloud can get the ID and Public Key of fog node. In this phase, both cloud and fog are mutually authenticated with each other.

C. Phase III – Thing/Device Registration Phase

This phase is the prerequisite phase for the actual authentication protocol. In this phase of proposed scheme, IoT thing sends authentication request to fog node containing its id ID_t and randomly generated nonce (N1). The identity of device depends on the specific type of networks: IP, MAC, Zigbee address etc. and nonce N1 will be used as a private key encrypted by cloud's public key: E(Ku_{cs},N1). One another nonce (N2) is also sent to prevent replay attack [IDt || E (Ku_{cs},N1) || N2]. After that, fog node received the authentication request from device and performs preliminary identity check for IoT device. Preliminary identity check means fog node check/verify technology specific source address. In this verification, fog node checks source address in the registration request because fog node aware of communication protocol used in constrained network environment. Fog node sends request to cloud along with its certificate to be authenticated by cloud server- ID_t || E (Ku_{cs}, N1) || E (Kr_{cs}, [ID_f || Ku_f || H1 (ID_f || Ku_f)]. In that case, cloud generated IPV6 address and public key for the device using asymmetric cryptography with the received nonce (N1) as a private key. The following information generated by cloud server:

- Hash identify of IPV6 address H(IPV6)
- Things public key Ku_t
- Fog public key Ku_f encrypted by things private key N1

All above information encrypted by fog public key. Fog node receive a message E (Ku_f, H(IPV6) || Ku_t || E (N1,[Ku_f]) and perform decryption on it. After performing decryption operation, fog node will store hash identity H (IPV6) and corresponding things public key. At the end of this phase, fog node sends a message to thing; which consists of following information: Things public key, hashed address and fog node public key encrypted by device private key. After receiving a message H(IPV6) || Ku_t || E (P_{rt}, [Ku_f]) by device, the device make sure that it has been registered with cloud server by receiving fog node's public key encrypted by its own private key. In that case, device decrypts the message and stores public key of fog node.

D. Fog-Device mutual authentication phase

When thing wants to authenticate itself, it sends stored H(IPV6) along with nonce (N3) signed by fog public key to prevent replay attack and to authenticate fog node: H(IPV6) || Ku_t || E (Ku_f, N_3). Upon receiving this information, fog node performs decryption and looks for its public key in its local storage. Fog node performs comparison of received

hash identity and stored hash identity of thing. If both identities of thing matches, then thing/device authenticated successfully by fog node. Finally, Fog node sends authentication response message to thing.

E. Authentication in Inter-Cluster Movement Phase

In this phase, we consider the movement of device from one cluster to another. In that case, current or visiting fog node is responsible to authenticate device with the help of cloud server. If device moves to another cluster, then current fog node will not find the hash identity of device H(IPV6) in its local database and then fog node will ask to cloud server that the visited device is registered or not. Cloud server is having global database for hash identity of registered device. If cloud found the H(IPV6) of current visited device, then it returns H(IPV6) of that device to fog node along with public key of device. After that fog node decrypts the nonce, stores it and to authenticate the device. If fog node is unable to authenticate device, then the current visited device in a particular cluster is considered as an outsider. Here, we proposed authentication protocol for only registered devices, not for the outsider devices. Outsider devices must have registered before authentication process.

In the proposed authentication scheme, three key roles are declared / defined: Cloud server, fog node and devices (IoT Things). Some certain knowledge, initial state & various transitions define in each of the role section.

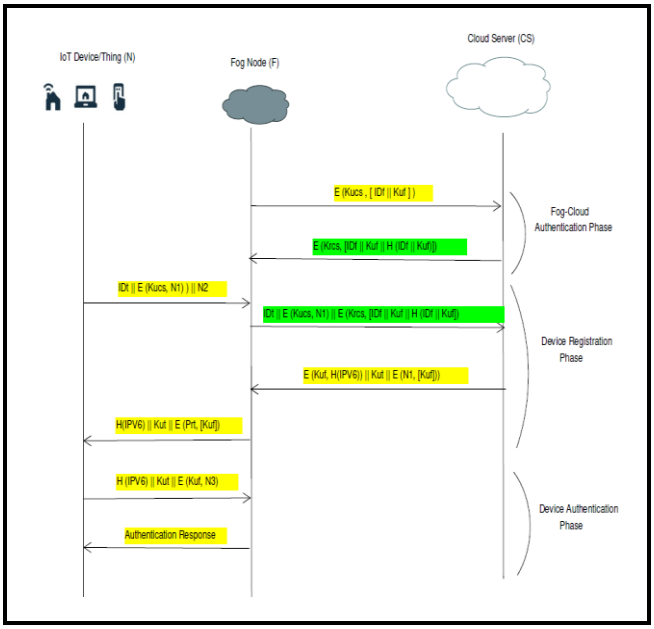

Figure 3. Process Flow Diagram of Proposed Authentication Scheme

5. Security Analysis of Proposed Scheme

The secure framework for three-way authentication procedure is proposed to prevent unauthorized access to IoT devices inside the cluster and inter movement of devices between clusters. In this section, we analyze the security properties of proposed framework in context of set of general categorized attack mentioned in section 3.2

a. Defend against Brute Force attack:

During this attack, attackers try all possible combination to guess private key. Using asymmetric cryptographic algorithm and one-way hash function in the proposed framework makes significant resist against brute force attack.

b. Defend against Side Channel attack

In which the attacker determines private exponent by calculating time with exploiting the timing variation of cryptographic algorithm. In that case, we used one-way hash and asymmetric algorithm in registration phase will protect data from this attack.

c. Defend against Man in the Middle attack

To protect the suggested framework from MIM attack encrypted nonce (N1) and mutual authentication between device and fog is required. For this purpose, device generates and computes (ID_t II E (K_{uc}, N1) || N2) & sends to the fog node and fog forwards this message to cloud for verification. This whole process prevents MIM attack.

d. Defend against Eavesdropping

This attack carried out to capture the unauthorized information that is confidential. Encryption techniques provide strong defense against eavesdropping. In the proposed framework, communication between entities like fog, cloud, things are encrypted to prevent eavesdropping. As per theoretical model of cryptography, attacker can not decrypt the information until they don't get a key. In this model, asymmetric algorithm is used for encryption along with strong one-way hash function.

e. Defend against Node Capture attack

In authentication process, IoT devices choose a random nonce that will be discarded when session terminates.

f. Defend against Replay attack

In this attack, attacker intercepts the information if attacker gains information between entities and replays it fraudulently. This attack can be disabled by using secret nonce. In every session, new nonce is used to prevent replay attack. Attacker has nonce to get information but as per previous analysis, it is impossible to gent new nonce every time.

6. Evaluation of Proposed Framework

i. Scalability and Faster Response

The proposed framework can use in many distributed IoT applications such as smart healthcare application, smart transportation system etc. where in communication delay must be low. Therefore, this type of application needs faster response as per their requirements. The proposed framework uses various techniques that make the fog enabled IoT framework more scalable in comparison with related work. Using fog-based authentication has decreased the dependency of cloud server. So, the process of authentication will be faster and more scalable. Furthermore, using three-way authentication procedure by using cloud server will increase the ability of managing authentication for large number of IoT devices.

ii. Efficiency

The process of authentication in the proposed framework has been more efficient by establishing logical and reasonable communication between fog - devices and cloud-fog severs during the process of authentication. Accordingly, fog node and IoT devices are mutually authenticated with the help of cloud server and cloud server will confirm the identity of IoT devices. In addition, the role of fog node in the process of protecting and accessing IoT devices with the help of cryptographic primitives inside a cluster is other feature of

proposed framework that increase efficiency in Fog based IoT environment considerably.

iii. Security

Security of suggested framework has been improved with the help of cryptographic primitives. By the establishment of asymmetric cryptographic algorithm and one-way hash function during the authentication will enhance the rate of trust in the framework.

7. Conclusions

IoT is the most promising technology in today scenario. Heavyweight solutions are not feasible for the authentication purpose in resource-constrained environment. Therefore, we kept resource constrained nature in mind while designing secure authentication framework. In this paper, we presented a lightweight authentication framework for fog enabled IoT devices using cryptographic primitives and asymmetric cryptographic functions. We used lightweight cryptographic primitives for the authentication between device & fog and asymmetric functions between fog & cloud server. Our proposed authentication framework satisfies the mutual authentication and confidentiality as mentioned in our security analysis. Our future work involves implementing our protocol in terms of performance overhead.

References

[1] D. Gil, A. Ferrandez, H. Mora-Mora and J. Peral, "Internet of things: A review of surveys based on context aware intelligent services," Sensors, vol. 16, pp. 1069, 2016.

[2] O. Vermessan et al., "Internet of things strategic research roadmap," Internet of things-global technological and societal trends, vol. 1, pp. 9-52, 2011.

[3] D.S. Chouhan, D. Bhardwaj and K. Kant, "QoS-aware routing protocol using adaptive retransmission of distorted descriptions in MDC for MANETs," International Journal of Ad Hoc and Ubiquitous Computing, vol. 28, pp. 55-67, 2018.

[4] M. Lanculescu, A. Alexandru, N. Nicolau, G. Neagu and O. Bica, "IoHT and Edge Computing, Warrants of Optimal Responsiveness of Monitoring Applications for Seniors. A Case Study," 22nd International Conference on Control Systems and Computer Science (CSCS), pp. 655-661, 2019.

[5] T.A. Ahanger, U. Tariq and M. Nusir, "Mobility of Internet of Things and Fog Computing: Concerns and Future Directions," International Journal of Communication Networks and Information Security, vol. 10, no. 3, pp. 534-538, 2018.

[6] U. Verma and D. Bhardwaj, "Security Challenges for Fog Computing Enabled Internet of Things from Authentication Perspective," International Journal of Computational Intelligence \& IoT, vol. 2, no. 1, 2019.

[7] A.M.A. Abuagoub, "IoT Security Evolution: Challenges and Countermeasures Review," International Journal of Communication Networks and Information Security, vol. 11, no. 3, pp. 342-351, 2019.

[8] P.R. Kumar, A.T. Wan and W.S.H. Suhaili, "Exploring Data Security and Privacy Issues in Internet of Things Based on Five-Layer Architecture," International Journal of Communication Networks and Information Security, vol. 12, no. 1, pp. 108-121, 2020.

[9] A. Amiruddin, A.A.P. Ratna and R.F. Sari, "Systematic Review of Internet of Things Security," International Journal of Communication Networks and Information Security, vol. 11, no. 2, 2019.

[10] S. Yi, C. Li and Q. Li, "A survey of fog computing: concepts, applications and issues," Proceedings of the 2015 workshop on mobile big data, pp. 37-42, 2015.

[11] B. Varghese, N. Wang, D. S. Nikolopoulos and R. Buyya, "Feasibility of fog Computing," arXiv preprint arXiv:1701.05451, 2017.

[12] S. Sarkar and S. Mishra, "Theoretical modelling of fog computing: a green computing paradigm to support IoT applications," IET Networks, vol. 5, no. 2, pp. 23-29, 2016.

[13] A.K. Das, M. Wazid, N. Kumar, M.K. Khan, K.K. Ray and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," IEEE journal of biomedical and health informatics, vol. 22, no. 4, pp. 1310-1322, 2017.

[14] A. Tiwari and B.B. Gupta, "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices," International Journal of Advanced Intelligence Paradigms, vol. 9, no. 2-3, pp. 111-121, 2017.

[15] R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013.

[16] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2710-2723, 2013.

[17] S. Jang, D. Lim, J. Kang and I. Joe, "An Efficient Device Authentication Protocol Without Certification Authority for Internet of Things," Wireless Personal Communications, vol. 91, no. 4, pp. 1681-1695, 2016.

[18] M.H. Ibrahim, "Octopus: An Edge-fog Mutual Authentication Scheme," International Journal of Network Security, vol. 18, no. 6, pp. 1089-1101, 2016.

[19] M. Shahzad and M.P. Singh, "Continuous authentication and authorization for the Internet of Things," IEEE Internet Computing, vol. 21, no. 2, pp. 86-90, 2017.

[20] Y. Chen, J.F. Martinez, P. Castillejo and L. Lopez, "A Privacy Protection User Authentication and Key Agreement Scheme Tailored for the Internet of Things Environment: PriAuth," Wireless Communications and Mobile Computing, vol. 2017, 2017.

[21] J.L. Hou and K.H. Yeh, "Novel authentication schemes for IoT based healthcare systems," International Journal of Distributed Sensor Networks, vol. 11, no. 11, pp. 183659, 2015.