International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Jan-2022)
https://dx.doi.org/10.12785/ijcds/110107

Elliptic Curve Cryptography based Centralized Authentication Protocol for Fog enabled Internet of Things

Upendra Verma[1], Diwakar Bhardwaj[2]

[1,2]*Department of Computer Engineering and Applications, GLA University, Mathura, India*

Received 19 Jan. 2021, Revised 18 Apr. 2021, Accepted 23 Apr. 2021, Published 9 Jan. 2022

Abstract: Internet is playing indispensable role in our daily lives. With recent advancement of communication technologies, Internet of Things (IoT) became vital part of human life. IoT devices may be easily compromised and incapable of defending & securing themselves due to resource constrained nature. Since, the integration of devices with resource rich pool such as cloud is required. The ability of current cloud model is insufficient to handle requirements of delay sensitive IoT applications. Cloud-IoT integration model does not support the features e.g. geographical distribution, low latency and location awareness etc. that features are necessary for some IoT applications includingtraffic light management, smart healthcare management and smart home energy management. Fog computing is still an evolving architecture that demands more research. Security is one of the major issue in fog computing. In this paper, we proposed an anonymous mutual authentication scheme based on ECC for fog enabled IoT environment. The proposed protocol ensures device anonymity and achieves mutual authentication between IoT device and fog node with the help of trusted third party (TTP) called centralized authentication protocol. Security analysis of proposed authentication protocol shows that the protocol is vigorous against various cryptographic attacks. The performance analysis shows that the protocol is efficient and computationally feasible in terms of storage and communication overhead for resource constrained environment.

Keywords: Internet of Things, Fog Computing, Centralized Authentication Protocol, Elliptic Curve Cryptography, Cryptographic attacks, Mutual Authentication Protocol

1. INTRODUCTION

The mission and vision of IoT is to build a smart and clever environment by utilizing embedded devices/things/physical objects that have communication capabilities to generate vast amount of data and also transmit data using Internet for the analysis and decision making [1]. The IoT plays an essential role in revolutionizing several sectors e.g., agriculture, transportation, healthcare etc. [2]. The first IoT infrastructure "Internet connected coke machine" realized in 1982 and was installed in Carnegie Mellon University [3].

The term "IoT" has been defined by different authors in different ways and preeminent definition is proposed by ITU-T defined IoT as "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [4]. Global infrastructure, Physical &Virtual object, Information society, Interoperability and Communication technologies are the keywords of proposed definition. The term "IoT" was devised by Kevin Ashton [5], which was the co-founder of Auto-ID Center at MIT. Cisco estimated that there will be 3.5 networked devices per capita in 2021 [6].
Fig. 1 shows the abstract view of IoT.

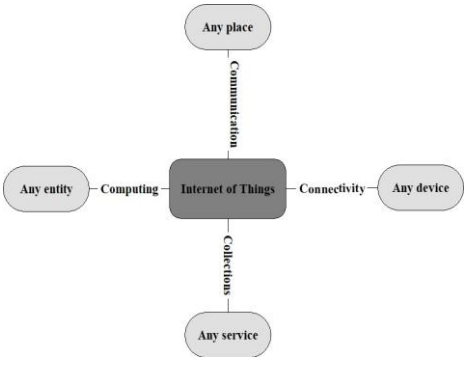

Figure 1. Abstract View of IoT

Security is the indispensable issue in Internet of Things. The barrier for exponential growth of IoT is

E-mail:upendra4567@gmail.com, diwakar.bhardwaj@gla.ac.in

security issue. IoT devices have limited security functionalities due to resource constrained environment. Security for IoT devices are very hard to implement due to their openness and very less human intervention [7]. HP study reveals 70% of IoT devices are susceptible to various kinds of cryptographic attacks [8]. In 2014, Kaspersky detected malwares on more than 1 million consumer gadgets [9].Cloud computing is based on distributed computing and virtualization [10]. The storing and accessing of files to remote server is possible through cloud deployment model. The cloud computing is integrated with IoT called IoT-Cloud computing model to provide various intelligent and smart applications to human being such as smart healthcare [11], smart home [12], smart transportation [13], smart city [14] etc. In IoT-Cloud model, cloud computing acts as a front end to access services of internet of things [15]. This hybrid model has several severe issues in context of response intensive IoT applications. The geographical distance between IoT device and Cloud server has higher impact on communication cost, network congestion, processing of data, end to end delay. The ability of Cloud-IoT model is insufficient to handle requirements of delay sensitive IoT applications [16]. Fig. 2 shows the current cloud model.

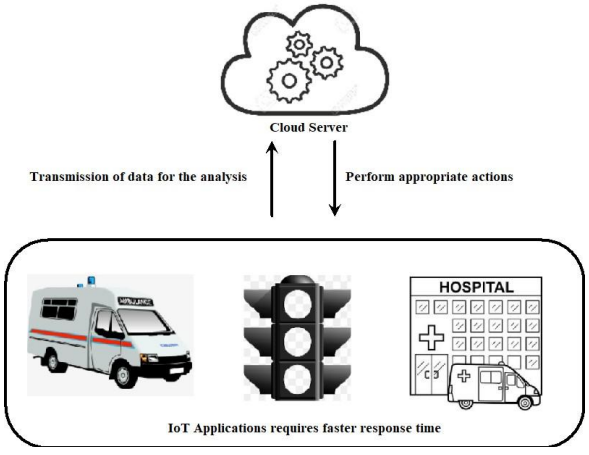

Figure 2. Cloud Computing Model

The critical issues of present cloud computing model are network bandwidth and response time (latency).The Cloud-IoT model cannot fulfill the minimum latency demands of IoT devices. Therefore, communication and network latency must be reduced for IoT data transmission. Fog computing paradigm is able to address and solve the challenge facing by Cloud-IoT model. Fog enabled IoT system called Fog-IoT integrated model provides storage and computation at edge of the network instead of doing computation in center of cloud and high priority data needs to be addressed immediately. Fog enabled IoT environment has some challenges apart from benefits. Security is the crucial issue in fog computing [17]. Authentication is the pertinent security issue in Fog-IoT model. Authentication plays indispensable role to prevent the entry of unauthorized devices. In this paper, we address the authentication issue for fog computing environment and proposed identity based anonymous authentication scheme. The mutual authentication between IoT device and fog server is achieved by trusted third party called centralized authentication procedure or three-way authentication procedure. In centralized authentication procedure, two entities mutually authenticate each other and trusted third party helps to authenticate themselves [18]. In this paper, we proposed ECC based centralized authentication protocol for fog assisted delay sensitive IoT applications.

The research contributions of the proposed work are outlined below:

- The proposed authentication approach overcomes the flaws in existing related literature.
- The proposed authentication approach employs the concept of fog computing, which brings cloud services closer to the IoT devices and fog computing provides services with faster response.
- Our proposed authentication approach ensures mutual authentication between IoT device and fog server with the help of trusted third party (TTP) called centralized authentication protocol.
- Our proposed authentication protocol utilizes XOR operation, concatenation operation, hash function and random nonce in order to provide cost effective operations.
- The several security requirements such as device anonymity, man-in-the-middle attack, mutual authentication, certificated based authentication and eavesdropping has been analyzed.
- ECC has been adopted to provide security with smaller key size, which is suitable for resource constrained network.
- The performance is evaluated and compared with exiting protocols in terms of storage and computational cost.
- Our proposed authentication approach outperforms the related work in terms of performance and security analysis.

The rest of paper is organized as follows: Section 2 discusses the Fog computing architecture. Section 3 discusses security goals. Section 4 presents the motivation for ECC. Section 5 discusses related works. Section 6 explores the proposed protocol. The Section 7 shows the correctness and security proof of proposed protocol. Section 8 presents security analysis. Section 9 explains the performance evaluation. Finally, Section 10 concludes the research work.

A. Security Challenges in IoT

IoT has security issues that must be taken into consideration. In this section, we address the security challenges in context of IoT in order to realize the necessity of security for IoT networks. The security challenges in terms of cryptographic attacks are summarized below:

- Eavesdropping: Messages to be intercepted and read by the malicious entity, who can inject fake messages into the network.
- Collision: The attack is performed through interfering signal. The attacker listens transmitting frequency of IoT device and forwards its own signal, it causes the collision and receiver obtains an incorrect message.
- Sinkhole attack: The attacker offers a false sink to nodes to prevent the delivery of messages to the base station, causing a partial or total damage of IoT networks.
- Man in the middle attack: Attacker intercepts the communication between two entities to steal the information of IoT networks.
- DoS attack: Denial of Service attack makes the application services unavailable to the IoT networks.
- Routing attack: The attack targeting the exhaustion of network resources.
- Node capture attack: Attacker takes over the control of IoT device by physical attack.
- Replay attack: Attacker can replay old messages and gain access to personal data by acting as the original sender.
- Botnets: The IoT devices turned into remotely controlled bots, which can be used as a part of botnet.
- Tampering: It is the physical access to the devices performed by attacker and attacker can obtain the confidential information.
- Sybil: In this attack, malicious node presents multiple false identities.
- Repudiation: This type of attack presents a partial or full denial participation of specific IoT device to the communication.
- Traffic analysis attack: The adversary intercepts and examines the messages in order to obtain network information.

2. FOG COMPUTING ARCHITECTURE FOR INTERNET OF THINGS

Fog computing is the technology that brings processing and storing capabilities closer to end user [19]. The first fog computing architecture was proposed by Bonomi et al. [20].The characteristics preserved by fog computing are response time, mobility support, interoperability, wireless connectivity, distributed nature, real time analysis of data, interconnectivity with cloud, supports large number of devices. The universally accepted fog computing architecture is not defined till now. In literature, authors have proposed several architectures based on the requirements of type of service and application [21, 22, 23, 24, 25, 26, 27,28].

The most basic and generic architecture as shown in Fig.3.

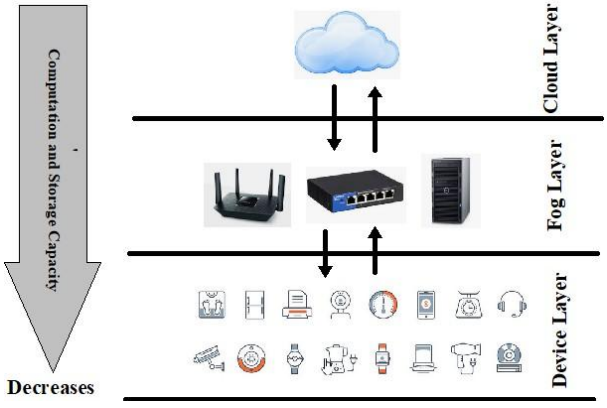

Figure 3. Fog Computing Architecture

Fig. 3 shows the computation and storage capability decreases from top to bottom in a layered architecture. In the proposed protocol, cloud layer acts as a TTP. Table 1 shows a brief description of layers in fog computing architecture.

TABLE I. LAYERS IN FOG COMPUTING ARCHITECTURE

Layers	Description
Device Layer (Tier-1)	This is the bottom layer, which involves fixed and mobile IoT devices. The devices have limited computing and storage capability, so that devices cannot respond to emerging conditions.
Fog Layer (Tier-2)	This is the middle and core layer, which comprises devices that can play a role of fog node such as switches, gateway and routers. Fog devices can be any network device capable of doing computation, networking and storage from local perspective. In general, fog node can be deployed to edge of the network (network of devices).Fog node possess local knowledge of devices and responsible for sending data to cloud server on regular basis. This layer offers many services to device layer with or without involvement of cloud layer.
Cloud Layer (Tier-3)	This is top most layer in fog computing architecture. Cloud layer performs computation, networking and storage from global perspective. The layer comprises data centers and servers, which performs global analysis on data that received by fog layer.

3. SECURITY GOALS OF AUTHENTICATION PROTOCOL

Security goals are the most important facet of authentication protocol. The security goals must be fulfilled by authentication protocol to protect cryptographic attacks.

- **Provides Device Anonymity:** Trusted third party (TTP) generates masked identity MId_i by performing XOR operation between random number r_{ttp} and original identity of device Id_i. TTP stores Mid_i to memory of device and fog server. It is computationally infeasible to break MId_i because illegitimate fog server cannot know the device details.
- **Provides Mutual Authentication:** The IoT device and fog server are mutually authenticated with each other using the computed parameter P_A' and P_{A1}', which exchanges during authentication phase. Fog Server authenticates IoT device by comparing P_A' and P_A. Similarly, IoT device authenticates fog server by comparing P_{A1}' and P_{A1}.

4. ELLIPTIC CURVE CRYPTOGRAPHY: PRELIMINARIES AND MOTIVATION

This section discusses brief motivation to the ECC [29]. ECC offers similar security level compared to others with smaller key size [30]. For example, RSA uses 3072-bit key size for achieving security and ECC uses 256-bit key size for achieving equivalent security level. ECC provides faster processing of cryptographic operations with smaller key size. Table 2illustrates that ECC is the appropriate cryptographic solution for resource constrained system [31].

TABLE II.COMPARISON BETWEEN RSA AND ECC

Key Size		Key Size ratio	Security Level (bits)	Cost Ratio
ECC	RSA			
160	1024	1:7	80	1:3
224	2048	1:10	112	1:6
256	3072	1:12	128	1:10
384	7680	1:20	192	1:32
521	15360	1:30	256	1:64

5. RELATED WORK

Authentication is being widely used in IoT and many authors proposed authentication protocol for resource constrained environment.

In [32], author proposed mutual authentication protocol between sensor node and base station in wireless sensor network. In the protocol, information is exchanged between communicating entities in the form of plain text. In [33], authors proposed an authentication scheme for wireless sensor network. Author presented an authentication approach using Zero Knowledge Proof (ZKP) model for the authentication of sensor nodes. In [34] provided distributed authentication for wireless sensor networks. Fully distributed authentication might not be suitable for dynamic WSN/IoT environment. In [35] author proposed authentication scheme for generic IoT applications. The authentication scheme provides distributed authentication. In [36] discussed rekeying process by centralized entity and proposed distributed approach for secure group communication. Fully distributed approach is not suitable for resource constrained environment.

In [37], a certificate based authentication approach is proposed. This approach makes used of

certificate in order to ensure mutual authentication. The communication and computation overhead are high due to the use of certificate. In [38], author proposed authentication protocol for fog enabled IoT application. The authentication protocol offers mutual authentication between all the communicating parties. The security analysis is not carried out for the protocol. In [39], proposed ECC based RFID authentication approach that makes used of ID-verifier scheme. In [40], authors proposed scalable and efficient authentication protocol for dynamic WSN. The protocol does not provide mutual authentication between all communicating entities.

In [41] proposed ECC based authentication protocol. In Kalra and Sood's scheme, the authors claimed it can obtain mutual authentication and resistant to security attacks. Authors in [42], found that the authentication protocol developed by Kalra et al.can not achieve mutual authentication.

In 2019 [43] proposed an authentication scheme which provides fog security services (FSS). The proposed authentication scheme used Rivest-Shamir-Adleman (RSA) algorithm, which has higher computation cost as compared to ECC. In [44], authors presented an authentication scheme based on the idea of digital signature and device capability. The authentication scheme is proposed without comparison of existing related authentication scheme and security analysis is not performed in order to represent robustness of proposed scheme. In [45], proposed an authentication protocol and analyzed the protocol developed by Kalra and Sood. However, the Kalra and Sood's scheme not provide mutual authentication. In [46] author proposed authentication protocol using X.509 mechanism and IoT devices are integrated with X.509. Security analysis is not considered in the proposed scheme.

Keeping in view of the previous study on authentication scheme, we proposed mutual authentication protocol based on ECC for fog enabled IoT network. The proposed protocol is able to satisfy all security goals.

6. PROPOSED AUTHENTICAITON PROTCOL

We illustrate the various phases of proposed authentication scheme. The proposed protocol achieves mutual authentication between IoT device and fog node with the help of trusted third party called centralized authentication protocol. The notations have been listed in Table 3. The proposed authentication protocol is appropriate for delay sensitive IoT application.

TABLE III. NOTATIONS AND SYMBOLS USED IN PROPOSED PROTOCOL

Notation	Description
E_p	Elliptic curve over finite field Z_p
Id_i	Identity of device
Mid_i	Masked Identity of device
TTP	Trusted Third Party
r_{ttp}	Random number generated by TTP
FS	Fog Server
G	Generator Point
r_{fs}	Private Key of Fog Server
CP_{fs}	Public Key of Fog Server
r_{iotd}	Random number of device
V_{iotd}	Curve point of device
Hash	Cryptographic one-way hash function
$\|\|$	Concatenation Operation
$\oplus$	XOR Operation

The protocol containstwo phases: Initialization phase and authentication phase.

A. Initialization Phase

1. Trusted third party (TTP) determines the masked identity (Mid_i) for the IoT devices. TTP selects Id_i of the device and random number r_{ttp} to generate Mid_i using XOR Operation as:
   $Mid_i \rightarrow Id_i \oplus r_{ttp}$

2. TTP stores Mid_i to fog server's and device's memory.

3. Fog server determines equation $y^2 = x^3 + ax + b$ over a finite field with generator point G of order n.
   .

4. Fog server selects random number r_{fs} and computes elliptic curve point CP_{fs} as $CP_{fs} = r_{fs}$. G. Curve point CP_{fs} is a public parameter and stored in the memory of device.

5. Fog server selects a random number r_{iotd} and V_{iod} for each IoT device as $V_{iotd} = r_{iotd}$. G. The values (V_{iotd}, r_{iotd}) are stored in the memory of device.

B. Authentication Phase

The authentication phase follows following steps:

1. To initiate the authentication phase, device sends a request message to fog server {Request, Mid_i}

2. Fog server receives request message and verifies Mid_i. If it is matched, then the fog server continues to prepare response message otherwise terminate the authentication process.

3. The fog server selects a random nonce n_1 and computes curve point as $C_1 = n_1 \cdot G$. The fog server computes curve point as $C_1' = r_{fs} \cdot C_1$, where r_{fs} is the private key of fog server. To initiate the authentication process with IoT device, fog server sends response message to IoT device {Response, C_1'}

4. Device receives response message from fog server, device generates a random nonce n_2 and computes curve point as $C_2 = n_2 \cdot G$. The device also calculates two more curve points as: $C_3 = n_2 \cdot C_1'$ and $C_4 = n_2 \cdot V_{iotd}$. Now the parameter for authentication P_A is computed as: $P_A = Hash (C_3 \| C_4)$ and sends $\{P_A, C_2\}$ to the fog server.

5. Fog server receives $\{P_A, C_2\}$ and computes $P_A' = Hash (n_1 \cdot r_{fs} \cdot C_2 \| r_{iotd} \cdot C_2)$ if $P_A == P_A'$ then authentication process continues otherwise process is terminated The fog server selects random nonce n_3 and computes curve point as: $C_5 = n_3 \cdot G$ and computes $P_{A1} = Hash (n_3 \cdot V_{iotd})$ and sends $\{P_{A1}, C_5\}$ to IoT device.

6. IoT device calculates $P_{A1}' = Hash (r_{iotd} \cdot C_5)$. If $P_{A1}' == P_{A1}$ then authentication process is completed otherwise process is terminated.

   If any step of authentication protocol fails, then process of authentication is terminated. The Fig. 4 shows the summary of proposed authentication protocol.

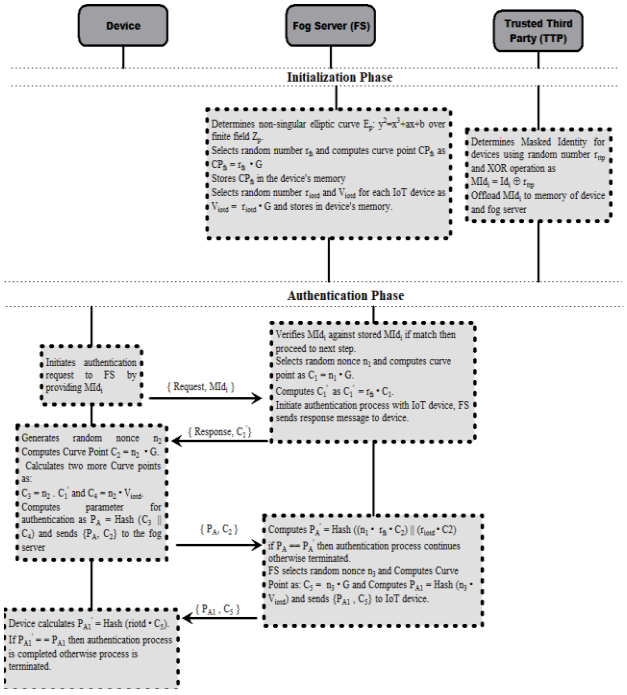

Figure 4. Summary of Proposed Authentication Protocol

7. SECURITY PROOF OF AUTHENTICATION PROTCOL

1. Fog Server authenticates IoT device by comparing P_A' and P_A.

$P_A' = Hash ((n_1 \cdot r_{fs} \cdot C_2) \| (r_{iotd} \cdot C_2))$
$P_A = Hash ((n_1 \cdot r_{fs} \cdot n_2 \cdot G) \| (r_{iotd} \cdot n_2 \cdot G))$ [Where $C_2 = n_2 \cdot G$]
$P_A' = Hash ((n_2 \cdot C_1') \| (n_2 \cdot V_{iotd}))$ [Where $C_1' = r_{fs} \cdot C_1$ and $V_{iotd} = r_{iotd} \cdot G$]
$P_A' = Hash (C_3 \| C_4)$ [Where $C_3 = n_2 \cdot C_1'$ and $C_4 = n_2 \cdot V_{iotd}$]
$P_A' = P_A$

If P_A' is equivalent to P_A then authentication process continues otherwise authentication process terminated.

2. IoT device authenticates fog server by comparing P_{A1}' and P_{A1}.

$P_{A1}' = Hash (r_{iotd} \cdot C_5)$
$P_{A1}' = Hash (r_{iotd} \cdot n_3 \cdot G)$ [Where $C_5 = n_3 \cdot G$]
$P_{A1}' = Hash (n_3 \cdot V_{iotd})$ [Where $V_{iotd} = r_{iotd} \cdot G$]
$P_{A1}' = P_{A1}$

If P_{A1}' is equivalent to P_{A1} then authentication process continues otherwise authentication process terminated.

8. SECURITY ANALYSIS

In this section, we represent the cryptographic strength of proposed authentication protocol against various attacks. The basic goals of the proposed authentication protocols are device anonymity and mutual authentication.

1. Device Anonymity: It is the most vital security goal. TTP generates Masked Identity Mid by using XOR operation with random number and stored Midi to the device's memory. Attackers cannot obtain the real identity of device because TTP uses random number in order to generate Midi, which is computationally infeasible.

2.Resistance to man-in-the-middle attack: The proposed protocol attains authentication. Hence, man-in-the-middle attack is not achievable due to the attainment of mutual authentication between IoT device and fog server. The MITM attack is viable for the existing protocols [38, 40, 44] because the existing protocols do not achieve mutual authentication.

3. Resistance to Cloning attack: The proposed authentication scheme is resistant to cloning attacks. Attackers have to obtain real identify of IoT device in order to create a clone of a device. Attacker cannot obtain real identify of device that computation of Mid_i, which is computationally infeasible.

4. Resistance to Disclosure attack: The proposed authentication protocol is resistant to disclosure attacks. The transferred messages between device and Fog server are Mid_i, C_1', C_2, C_5, P_A, P_{A1}.If an attacker intercepts these messages, then unable to process without random nonce n_1, n_2 and n_3. The computationally infeasible to find random nonce.

5. Resistance to Eavesdropping: IoT device and fog sever exchange the message during authentication phase. Each time a new message generates by using hash function and random nonce, which is computationally infeasible.

6. Provide Mutual Authentication: The proposed authentication protocol attains mutual authentication between device and fog server with the help of trusted third party. Fog server verifies the IoT device by computing value P_A'. IoT device verifies fog server by computing the value P_{A1}'.

A. Analysis of Security Attributes

The result and outcome of security analysis is illustrated in the Table 4.This section analyses and compares the security attributes with the other related protocols.

TABLE IV.COMPARISON OF SECURITY REQUIREMENTSAMONG FIVE AUTHENTICATION SCHEMES

Authentication Protocols	Security attributes					
	Device Anonymity	Cloning attack	Man-in-the-middle attack	Eavesdropping	Mutual Authentication	Certificate based authentication
Jiang et al. (2013)	×	×	×	×	✓	✓
Liao et al. (2014)	✓	×	×	×	×	×
Kalra et al. (2015)	×	×	×	✓	×	×
Bhubaneswari et al. (2018)	✓	✓	×	✓	×	×
Proposed protocol	✓	✓	✓	✓	✓	×

✓: supports an attribute or prevents the cryptographic attack

×: does not support an attribute or unable to prevent the cryptographic attack

9. PERFORMANCE EVALUATION

In this section, we evaluate the performance of proposed authentication approach in resource constrained environment. The size of device Id, nonce and random numbers are considered as 128 bits. The output of hash function is considered as 256 bits. We assumed ECC-224 bits' cryptosystem i.e. the cryptosystem is equivalent to 2048 bits RSA cryptosystem [47]. IoT devices are resource constrained entities as compare to fog server. However, we consider communication and storage cost of devices only.

A. Communication Cost

Communication cost is the cost of message passing between communicating entities. It is the cost for transmission of security parameters between device and fog server. Let C_{IoTD} be the communication cost of device. The communication parameters exchange between device and fog server are:

i. $\{MId_i\}$: 128 bits
ii. $\{C_1'\}$: 224 bits
iii. $\{P_A, C_2\}$: (128 + 224) bits
iv. $\{P_{A1}, C_5\}$: (128 + 224) bits

Therefore, total communication cost C_{IoTD}= 128 + 224 + 256 + 224 + 256 + 224 = 1352 bits.Fig. 5 shows comparison of communication costs among the protocol.Table 5 shows the communication cost.

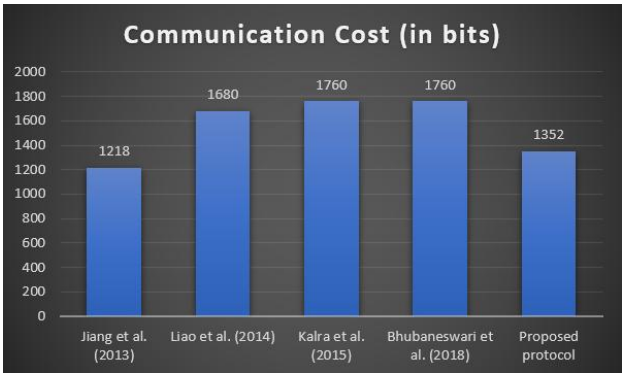

Figure 5. Communications Cost

B. Storage Cost

The following parameters are stored in a single IoT device: MId_i, CP_{fs} ,V_{iotd} , r_{iotd}. Let M_{IoTD}be the memory needed by IoT device. Therefore, total storage cost is calculated as:

M_{IoTD}= 128 + 224 + 224 + 128
M_{IoTD}= 704 bits

The comparative analysis of storage overhead for device is illustrated in the Fig. 6.

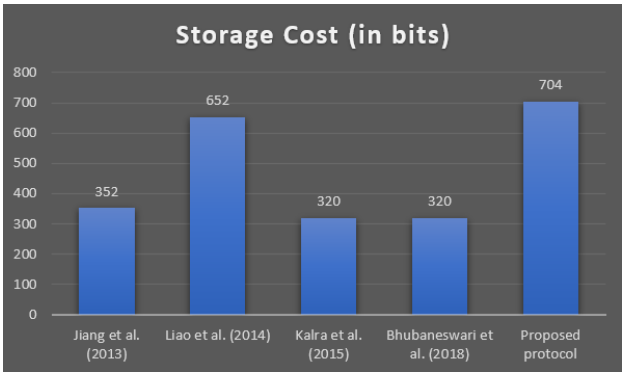

Figure 6. Storage Cost

Table 5 shows the storage overhead for the IOT device, which is larger than the related protocols [37, 39, 41, 45].The reason is that the proposed protocol ensures device anonymity which the protocols [37, 41] do not. The proposed protocol uses 256-bit hash and ECC-224-bit cryptosystem to provide mutual authentication, which the protocol [39, 41, 45] failed to provide mutual authentication.

TABLE V.PERFORMANCE EVALUATION AMONG FIVE AUTHENTICATION SCHEMES

Authentication Protocols	**Communication Cost (in bits)**	**Storage Cost (in bits)**
Jiang et al. (2013)	1218	352
Liao et al. (2014)	1680	652
Kalra et al. (2015)	1760	320
Bhubaneswari et al. (2018)	1760	320
Proposed protocol	1352	704

C. Discussions

The whole reviews of the security analysis and performance evaluationhave been summarized below:

- The proposed authentication protocol achieves mutual authentication where existing related protocols [**39, 41, 45**] do not provide mutual authentication.
- The proposed protocol achieves device anonymity where the exiting related protocols [**37, 41**] do not.
- The proposed protocol employs storage overhead more than the related protocols. The reason is that the proposed protocol attains mutual authentication and provides device anonymity. Our proposed protocol is able to defend several cryptographic attacks.
- The proposed protocol superior than the existing protocols **[39, 41, 45]** in terms of communication cost.

10. CONCLUSIONS

Fog enabled IoT system is the fast growing paradigm for delay sensitive applications. Mutual authentication plays a vital role for fog enabled IoT system. We have designed a mutual authentication scheme based on ECC for the fog enabled IoT system. We have observed that the related authentication protocols failed to provide security requirements. However, security analyses and performance evaluation of proposed work show that the proposed protocol is vigorous against several cryptographic attacks. Hence, the proposed authentication protocol is the lightweight and well suited for resource constrained IoT networks.

REFERENCES

[1] G. Fortino and P. Trunfio, "Internet of things based on smart objects: Technology, middleware and applications", Springer Science & Business Media, 2014.

[2] M. Maksimovic, "The role of green internet of things (G-IoT) and big data in making cities smarter, safer and more sustainable," International Journal of Computing and Digital Systems, 6(04), pp.175-184, 2017.

[3] U. Verma and D. Bhardwaj, "Security Challenges for Fog Computing Enabled Internet of Things from Authentication Perspective," International Journal of Computational Intelligence & IoT, 2(1), 2019.

[4] F. Wortmann and K. Flüchter, "Internet of things," Business & Information Systems Engineering", 57(3), pp.221-224, 2015.

[5] K. Govinda and R.A. Saravanaguru, "Review on IOT technologies," International Journal of Applied Engineering Research, 11(4), pp.2848-2853, 2016.

[6] "Global-2021 Forecast Highlights," 2016 [Online]. Available: https://www.cisco.com. [Accessed 22 October 2020].

[7] A. Bashir and A.H. Mir, "Internet of things security issues, threats, attacks and counter measures," International Journal of Computing and Digital Systems, 7(02), pp.111-120, 2018

[8] "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", 2014 [online]. Available: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676. [Accessed 22 October 2020].

[9] "Top 7 Mobile Security Threats in 2020" [Online]. Available: https://me-en.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store [Accessed 22 October 2020].

[10] A.L.S. Muhammad, "Cloud Computing Enabled Data Center Infrastructure Development and Deployment by IT Firms," International Journal of Computing and Digital Systems, 9(1), 2020

[11] K. Jaiswal, K., S. Sobhanayak, A.K. Turuk, S.L. Bibhudatta, B.K. Mohanta and D. Jena, "An IoT-Cloud based smart healthcare monitoring system using container based virtual environment in Edge device," International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), pp. 1-7, 2018.

[12] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou, and C.H. Lung, "Smart home: Integrating internet of things with web services and cloud computing," International conference on cloud computing technology and science, Vol. 2, pp. 317-320, 2013

[13] P.S. Saarika, K. Sandhya and T. Sudha, "Smart transportation system using IoT," International Conference On Smart Technologies for Smart Nation, pp. 1104-1107, 2017.

[14] R. Petrolo, V. Loscri and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," Transactions on Emerging Telecommunications Technologies, 28(1), p.e2931, 2017.

[15] B. P. Rao, P. Saluia, N. Sharma, A. Mittal and S.V. Sharma, "Cloud computing for Internet of Things & sensing based applications," International Conference on Sensing Technology (ICST), pp. 374-380, 2012.

[16] U. Verma and D. Bhardwajm "Design of Lightweight Authentication Protocol for Fog enabled Internet of Things-A Centralized Authentication Framework," International Journal of Communication Networks and Information Security, 12(2), pp.162-167, 2020.

[17] S.M. Hussain, K.M. Yusof, S.A. Hussain and N.P. Eberechukwu N, P., "A Review of Interoperability issues in Internet of Vehicles (IoV)," International Journal of Computing and Digital Systems, 8(01), pp.73-83, 2019.

[18] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) Authentication schemes," Sensors, 19(5), p.1141, 2019.

[19] P. Shroff and A. Bandyopadhyay, "A Novel Matching Framework For One-Sided Markets In Fog Computing," International Journal of Computing and Digital Systems, 10, pp.1-10, 2020.

[20] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things,"

Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13-16, 2012.

[21] H.F. Atlam, R.J. Walters and G.B. Wills, "Fog computing and the internet of things: a review," big data and cognitive computing, 2(2), p.10, 2018.

[22] S. Kunal, A. Saha and R. Amin, "An overview of cloud-fog computing: Architectures, applications with security challenges," Security and Privacy, 2(4), p.e72, 2019.

[23] H.J. Cha, H.K. Yang and Y.J. Song, "A study on the design of Fog Computing architecture using sensor networks," Sensors, 18(11), p.3633, 2018.

[24] CC. Byers, "Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for fog-enabled iot networks," IEEE Communications Magazine, 55(8), pp.14-20, 2017.

[25] R.K. Naha, S. Garg and A. Chan, "Fog computing architecture: Survey and challenges," arXiv preprint arXiv:1811.09047, 2018.

[26] T.H. Luan, L. Gao, L., Z. L. Y. Xiang, G. Wei and L. Sun, "Fog computing: Focusing on mobile users at the edge," arXiv preprint arXiv:1502.01815, 2015.

[27] N.K. Giang, M. Blackstock, R. Lea and V.C. Leung, "Developing iot applications in the fog: A distributed dataflow approach," International Conference on the Internet of Things (IOT), pp. 155-162, 2015.

[28] M.A. Nadeem and M.A. Saeed, "Fog computing: An emerging paradigm," International Conference on Innovative Computing Technology (INTECH), pp. 83-86, 2016.

[29] D. Hankerson, A.J. Menezes and S. Vanstone, "Guide to elliptic curve cryptography. Computing Reviews," 46(1), p.13, 2005.

[30] U. Iqbal and A.H. Mir, "Efficient and Dynamic Access Control Mechanism for Secure Data Acquisition in IoT Environment," International Journal of Computing and Digital Systems, 10(1), pp.9-28, 2020.

[31] M. Bafandehkar, S.M. Yasin, R. Mahmod, and Z.M. Hanapi, "Comparison of ECC and RSA algorithm in resource constrained devices," International Conference on IT Convergence and Security (ICITCS), pp. 1-3, 2013.

[32] R. Riaz, T.S. Chung, S.S. Rizvi and N. Yaqub, "BAS: the biphase authentication scheme for wireless sensor networks," Security and Communication Networks, 2017.

[33] M. Mozumdar, M. Aliasgari, S.M.V. Venkata and S.S. Renduchintala, "Ensuring Authentication and Security using Zero Knowledge Protocol for Wireless Sensor Network Applications," International Journal of Computing and Digital Systems, 5(03), 2016.

[34] M. Bilal and S.G. Kang, "An authentication protocol for future sensor networks," Sensors, 17(5), p.979, 2017.

[35] M.A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, 82, pp.395-411, 2018.

[36] M. Bilal and S.G. Kang, "A secure key agreement protocol for dynamic group. Cluster Computing," 20(3), pp.2779-2792, 2017.

[37] R. Jiang, C. Lai, J. Luo, X. Wang and H. Wang, "EAP-based group authentication and key agreement protocol for machine-type communications," International Journal of Distributed Sensor Networks, 9(11), p.304601, 2013.

[38] P. Porambage, C. Schmitt, P. Kumar, P., A. Gurtov and M. Ylianttila, "PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," International Journal of Distributed Sensor Networks, 10(7), p.357430, 2014.

[39] Y.P. Liao and C.M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," Ad hoc networks, 18, pp.133-146, 2014.

[40] Y. Qiu, J. Zhou, J. Baek and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," Sensors, 10(4), pp.3718-3731, 2010.

[41] S. Kalra and S.K. Sood, "Secure authentication scheme for IoT and cloud servers, "Pervasive and Mobile Computing, 24, pp.210-223, 2015.

[42] C.C. Chang, H.L. Wu and C.Y. Sun, "Notes on "Secure authentication scheme for IoT and cloud servers," Pervasive and Mobile Computing, 38, pp.275-278, 2017.

[43] N. Abbas, M. Asim, N. Tariq, T. Baker and S. Abbas, S., "A mechanism for securing IoT-enabled applications at the fog layer," Journal of Sensor and Actuator Networks, 8(1), p.16, 2019.

[44] Z.A. Alizai, N.F. Tareen and I. Jadoon, "Improved IoT device authentication scheme using device capability and digital signatures," International Conference on Applied and Engineering Mathematics (ICAEM) (pp. 1-5), 2018.

[45] S. Bhubaneswari, NV Ananth, "Enhanced mutual authentication scheme for cloud of things," Internal Journal of Pure and Applied Mathematics, 119(15):1571-1583, 2018.

[46] S. Karthikeyan, R. Patan and B. Balamurugan, "Enhancement of security in the Internet of Things (IoT) by using X. 509 authentication mechanism," Recent Trends in Communication, Computing, and Electronics (pp. 217-225). Springer, 2019.

[47] N. Chikouche and F. Cherif, "EAP-SRES: An Enhanced Authentication Protocol for Secure Remote Education Systems Using NFC Technology," International Journal of Computing and Digital Systems, 9(03), 2020.

Upendra Verma received his Master of Engineering in Computer Science and Engineering from Rajiv Gandhi Technological University, Bhopal, India in 2011. Currently, he is pursuing his Ph.D. in Computer Science and Engineering from GLA University, Mathura, India. His research areas include Internet of Things, Fog Computing, Authentication techniques and Network Security.

Dr.Diwakar Bhardwaj received his PhD degree from GLA University, Mathura, India. Currently, he is working as a Professor at GLA University, Mathura, India. His research areas include Internet of Things, Mobile Ad Hoc Network andQoS Aware Routing Protocol.