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

Upendra Verma¹, Diwakar Bhardwaj²

¹²Department 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 including traffic 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 a 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.

![Fig. 1. Abstract View of IoT](http://journals.uob.edu.bh)
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.

![Cloud Computing Model](image)

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.

http://journals.uob.edu.bh
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 lists the 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.
<table>
<thead>
<tr>
<th>Layers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Layer (Tier-1)</td>
<td>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.</td>
</tr>
<tr>
<td>Fog Layer (Tier-2)</td>
<td>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.</td>
</tr>
<tr>
<td>Cloud Layer (Tier-3)</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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, by performing XOR operation between random number \( r_{tp} \) and original identity of device Id. TTP stores MId, to memory of device and fog server. It is computationally infeasible to break MId, 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 \( P_{A_1'} \), 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 \( P_{A_1'} \) and \( P_{A_1} \).

### 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 2 illustrates that ECC is the appropriate cryptographic solution for resource constrained system [31].

<table>
<thead>
<tr>
<th>Key Size</th>
<th>Key Size ratio</th>
<th>Security Level (bits)</th>
<th>Cost Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC</td>
<td>RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>160</td>
<td>1024</td>
<td>1:7</td>
<td>80</td>
</tr>
<tr>
<td>224</td>
<td>2048</td>
<td>1:10</td>
<td>112</td>
</tr>
<tr>
<td>256</td>
<td>3072</td>
<td>1:12</td>
<td>128</td>
</tr>
<tr>
<td>384</td>
<td>7680</td>
<td>1:20</td>
<td>192</td>
</tr>
<tr>
<td>521</td>
<td>15360</td>
<td>1:30</td>
<td>256</td>
</tr>
</tbody>
</table>

### 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 AUTHENTICATION PROTOCOL

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>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E_p )</td>
<td>Elliptic curve over finite field ( \mathbb{Z}_p )</td>
</tr>
<tr>
<td>( \text{Id}_i )</td>
<td>Identity of device</td>
</tr>
<tr>
<td>( \text{Mid}_i )</td>
<td>Masked Identity of device</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third Party</td>
</tr>
<tr>
<td>( r_{\text{ftp}} )</td>
<td>Random number generated by TTP</td>
</tr>
<tr>
<td>FS</td>
<td>Fog Server</td>
</tr>
<tr>
<td>( G )</td>
<td>Generator Point</td>
</tr>
<tr>
<td>( r_{fs} )</td>
<td>Private Key of Fog Server</td>
</tr>
<tr>
<td>( \text{CP}_{fs} )</td>
<td>Public Key of Fog Server</td>
</tr>
<tr>
<td>( r_{\text{iotd}} )</td>
<td>Random number of device</td>
</tr>
<tr>
<td>( V_{\text{iotd}} )</td>
<td>Curve point of device</td>
</tr>
<tr>
<td>Hash</td>
<td>Cryptographic one-way hash function</td>
</tr>
<tr>
<td>(</td>
<td>)</td>
</tr>
<tr>
<td>( \oplus )</td>
<td>XOR Operation</td>
</tr>
</tbody>
</table>

The protocol contains two phases: Initialization phase and authentication phase.

A. Initialization Phase

1. Trusted third party (TTP) determines the masked identity \( \text{Mid}_i \) for the IoT devices. TTP selects \( \text{Id}_i \) of the device and random number \( r_{\text{ftp}} \) to generate \( \text{Mid}_i \) using XOR Operation as:

\[ \text{Mid}_i \rightarrow \text{Id}_i \oplus r_{\text{ftp}} \]

2. TTP stores \( \text{Mid}_i \) 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 \( \text{CP}_{fs} \) as \( \text{CP}_{fs} = r_{fs} \cdot G \). Curve point \( \text{CP}_{fs} \) is a public parameter and stored in the memory of device.

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

The authentication phase follows the following steps:

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

2. Fog server receives the request message and verifies Mid_i. If it is matched, then the fog server continues to prepare a response message; otherwise, it terminates 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 the fog server. To initiate the authentication process with the IoT device, the fog server sends the response message \{Response, C_1'\}.

4. The device receives the response message from the fog server, 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: \(P_A = \text{Hash}(C_3 \parallel C_4)\) and sends \{Response, C_1'\} to the fog server.

5. The fog server receives \{Response, C_1'\} and computes \(P_A' = \text{Hash}(n_1 \cdot r_{fs} \cdot C_2 \parallel r_{iotd} \cdot C_2)\) if \(P_A = P_A'\) then the authentication process continues; otherwise, it is terminated. The fog server selects a random nonce n_3 and computes curve point as: \(C_5 = n_3 \cdot G\) and computes \(P_{A1} = \text{Hash}(n_3 \cdot V_{iotd})\) and sends \{Response, C_1'\} to the IoT device.

6. The IoT device calculates \(P_{A1}' = \text{Hash}(r_{iotd} \cdot C_5)\). If \(P_{A1}' = P_{A1}\) then the authentication process is completed; otherwise, it is terminated.

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

7. SECURITY PROOF OF AUTHENTICATION PROTOCOL

1. Fog Server authenticates IoT device by comparing \(P_{A1}'\) and \(P_A\).

\[
P_{A1}' = \text{Hash}(r_{iotd} \cdot C_5)
\]

\[
P_A = \text{Hash}(n_1 \cdot r_{fs} \cdot C_2 \parallel r_{iotd} \cdot n_2 \cdot G)
\]

\[
P_A' = \text{Hash}(n_2 \cdot C_1' \parallel n_2 \cdot V_{iotd})
\]

\[
P_{A1}' = \text{Hash}(n_3 \cdot V_{iotd})
\]

\[
P_{A1} = P_A
\]

If \(P_{A1}'\) is equivalent to \(P_A\), then the authentication process continues; otherwise, it is terminated.

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

\[
P_{A1}' = \text{Hash}(r_{iotd} \cdot n_3 \cdot G)
\]

\[
P_{A1} = \text{Hash}(r_{iotd} \cdot n_3 \cdot G)
\]

\[
P_{A1}' = \text{Hash}(n_3 \cdot V_{iotd})
\]

\[
P_{A1} = P_{A1}
\]
If \( P_{A1} \)’ is equivalent to \( P_{AI} \) 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 identity of IoT device in order to create a clone of a device. Attacker cannot obtain real identity 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 \( Mid_\), \( C_1 \), \( C_2 \), \( C_5 \), \( P_A \), \( P_{AI} \). 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 server 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 \( P_{AI} \).

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>
<thead>
<tr>
<th>Authentication Protocols</th>
<th>Security attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Device Anonymity</td>
</tr>
<tr>
<td></td>
<td>Cloning attack</td>
</tr>
<tr>
<td></td>
<td>Man-in-the-middle attack</td>
</tr>
<tr>
<td></td>
<td>Eavesdropping</td>
</tr>
<tr>
<td></td>
<td>Mutual Authentication</td>
</tr>
<tr>
<td></td>
<td>Certificate based authentication</td>
</tr>
<tr>
<td>Jiang et al. (2013)</td>
<td>x  x  x  x  ✓  ✓</td>
</tr>
<tr>
<td>Liao et al. (2014)</td>
<td>✓  x  x  x  x  x</td>
</tr>
<tr>
<td>Kalra et al. (2015)</td>
<td>x  x  x  ✓  x  x</td>
</tr>
<tr>
<td>Bhubaneswari et al. (2018)</td>
<td>✓  ✓  x  ✓  x  x</td>
</tr>
<tr>
<td>Proposed protocol</td>
<td>✓  ✓  ✓  ✓  ✓  x</td>
</tr>
</tbody>
</table>

✓: supports an attribute or prevents the cryptographic attack
x: 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 \( C_{IoT} \) be the communication cost of device. The communication parameters exchange between device and fog server are:
i. \( \{ \text{MID}_i \} \): 128 bits
ii. \( \{ C'_1 \} \): 224 bits
iii. \( \{ P_{A1}, C_2 \} \): (128 + 224) bits
iv. \( \{ P_{A1}, C_3 \} \): (128 + 224) bits

Therefore, total communication cost \( C_{\text{IoTD}} \) = 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](image)

### B. Storage Cost

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

\[
M_{\text{IoTD}} = 128 + 224 + 224 + 128
\]

\[
M_{\text{IoTD}} = 704 \text{ bits}
\]

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

![Figure 6. Storage Cost](image)

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.

### C. Discussions

The whole reviews of the security analysis and performance evaluation have 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.

<table>
<thead>
<tr>
<th>Authentication Protocols</th>
<th>Communication Cost (in bits)</th>
<th>Storage Cost (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jiang et al. (2013)</td>
<td>1218</td>
<td>352</td>
</tr>
<tr>
<td>Liao et al. (2014)</td>
<td>1680</td>
<td>652</td>
</tr>
<tr>
<td>Kalra et al. (2015)</td>
<td>1760</td>
<td>320</td>
</tr>
<tr>
<td>Bhubaneswari et al. (2018)</td>
<td>1760</td>
<td>320</td>
</tr>
<tr>
<td>Proposed protocol</td>
<td>1352</td>
<td>704</td>
</tr>
</tbody>
</table>

**TABLE V. PERFORMANCE EVALUATION AMONG FIVE AUTHENTICATION SCHEMES**
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


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 and QoS Aware Routing Protocol.