A Review on Internet of Things (IoT) in Healthcare

Mustafa Abdullah Azzawi, Rosilah Hassan and Khairul Azmi Abu Bakar

Research Center for Software Technology and Management, Faculty of Information Science and Technology, University Kebangsaan Malaysia, Bangi-43600, Selangor, Malaysia.

Abstract
Internet of Things (IoT) rises as a powerful domain where embedded devices and sensors can connect and exchange information over the Internet. The importance of IoT devices and data can be critical, so security constraints are required to keep IoT data safe from intruders; authentication is one of basic and important means to confirm data privacy and security. The nature of IoT devices as a resource contains devices required a special authentication schema that does not consume high computing and energy resources. In this paper, a review for IoT healthcare usage and a novel authentication mechanism for IoT networks have been proposed. The architecture of reliable and secure healthcare architecture has been proposed. ECC algorithm over the CoAP protocol has been used. The proposed authentication approach provides an efficient authentication mechanism with high security.

Keywords: CoAP, ECC, authentication, security.

INTRODUCTION
Internet of things (IoT) is one of the most common research topics. Advances in electronics, IPv6 and wireless networks deployment have led to growing IoT technology. With the running developing of IoT devices and technologies [1]. IoT has spread widely and used in different environments including homes, health care institutes, aerospace and various transportations. Controlling systems and IoT combination is one of the main concerns of researchers. Different approach has been proposed to control IoT devices. IoT security has the highest priority concerns and became the first topic for research in the field of IoT [2].

Data protection is a critical issue for networks devices. In the field of IoT, security plays a vital role where malicious attack or interference with IoT devices can cause a threat to human life especially with critical IoT applications. The main answer for IoT data security is authentication. To trust command from the control system, identity confirmation is required. Different researches have been proposed to provide authentication mechanisms for normal networks and IoT. These mechanisms are not designed to fully fit the requirements of IoT environment and devices, where IoT devices have limited resources regarding to memory, processing and energy. The IoT controlling system has its own requirements [3]. The end devices which are used to control the IoT devices usually have higher resources related to storage, memory, processing and energy that simple IoT devices have, these capabilities devices which are used to control the IoT devices usually have higher resources related to storage, memory, processing and energy that simple IoT devices have, these capabilities provides new features for controlling system of IoT. Researchers working on authentication need to make a combination of end devices characteristics and make a balance between its available resources to provide efficient, secure and suitable authentication mechanism that fits IoT environment.

INTERNET OF THINGS FOR HEALTHCARE
A rising interest of body wearable sensors has recently emerged as powerful tools for healthcare applications and different devices are currently available commercially for different purposes including personal healthcare, activity awareness and fitness.

Researchers also have proposed new clinical applications of such technologies for systems of remote health monitoring which include functionalities for long term status recording, and medical access to physiological information of the patient [4]. Most remote health monitoring proposed frameworks has architecture of a three tier: body sensor network tier which includes a wearable sensors works as units for data acquisition such as blood pressure, heart status and body temperature, the second tier include communication and networking and the service which collects data from sensors and forwarded it [5, 6]. The third tier includes the processing and analyzing nodes. Figure 1 shows the architecture of healthcare system [7, 8] which include three phases environment monitoring to acquire data, this data is then gathered and transfer for the third phase for data analysis and investigation.

Figure 1: Healthcare monitoring system architecture
REVIEW
The main challenges those researchers face is not only to propose new authentication mechanisms, but also to propose an authentication that supports various IoT devices. The methods for authentication that work for smartphones will also be used to authenticate watches, thermostat, and wide range of sensors and microchips [9, 10].

Two main types of device identity security solutions have been proposed: physical protection solution and cryptography based authentication solution. Physical protection approach is designed to protect device from being damaged or attacked in the level of physical layer by applying physical concepts [11, 12]. On the other hand, cryptography based authentication approach is designed based on IoT radio frequency identification devise (RFID) device identity security field. It has great security features, many algorithms have recently been proposed based on IoT RFID [13].

IoT devices have limited resources and these devices are connected to the internet. These expose these devices to huge number of attacks and make it vulnerable. Authentication is required to guarantee security and identify identities to prevent attacker and malicious attacks [14]. Traditional networks authentication methods and approaches require high resources regarding processing [15]. IoT is considered a constrained resource environment where processing and energy resources are limited. A light weight authentication approach with robust security features is required to preserve energy and fit processing capabilities. So in this thesis we will propose a robust and light weight authentication method to meet the requirements of IoT environment and provide a solid security features to prevent malicious attacks and preserve its privacy [16, 17].

Figure 2 shows Internet of Things Reference Architecture.

![Internet of Things Reference Architecture](image)

Figure 2: Internet of Things Reference Architecture

Latest proposed authentication approaches have used different mechanisms to provide secure communication [18]. Approaches use HTTP protocols for authentication communication suffer from high overhead resulted from using HTTP protocol which is not optimized for resource limited IoT environment. Other approaches use AES for communication encryption [19]. AES uses long encryption keys and complex calculation which resulted in high power consumption and does not fit the requirements of IoT restricted energy resources [20].

RELATED WORK
Different algorithms have been proposed to provide authentication for IoT devices. In [21] an enhanced mutual authentication model has been proposed for IoT environment. They proposed some improvements to the algorithm of authentication of Challenge-response based RFID authentication protocol for distributed database environment [22]. They made it more suitable to IoT control system environment. Their approach has three main steps: add backup device for each terminal devices used for controlling, add monitor devices to follow and monitor terminal devices and finally add a push in alarm mechanism for alarming for any failed authentication process.

In [23] Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications has been proposed. This protocol is a certificate based authentication approach, two phase authentication allow both IoT devices and the control station to authenticate and recognize each other, a secure connection is established and data is transferred securely. They used protocol supports resource limitation of sensor nodes and takes into consideration network scalability and heterogeneity. Certificate authority (CA) has been used to issuing certificates. Existing nodes can move and change their location after they get their own certificate. CA can validate sensors identity and communicate with other entities of the network. Network members to initialize a connection, they connect to the CA firstly to confirm destination identity. This approach is considered as an end to end application layer authentication approach and depends on other lower layer security features.

In [24] Secure authentication scheme for IoT and cloud servers have been proposed, this schema mainly depends on Elliptic Curve Cryptography (ECC) based algorithms which supports better security solutions when it is compared with other Public Key Cryptography (PKC) algorithms [25] because of its small key size. This authentication protocol uses EEC for embedded devices which use HTTP protocol. Using the cookies of HTTP to authenticate smart devices is a novel approach. These devices need to be configured with TCP/IP. The proposed authentication protocol is designed to use HTTP cookies which are implemented to fit embedded devices that have constrained environments and controlled by cloud servers. The proposed protocol has three main phases Registration phase, Pre-computed and login phase and authentication phase. In registration phase the embedded devices are registered with the cloud server and it in turn send back a cookie which is stored on the embedded devices. In Pre-computation and Login Phase, the devices before connecting to the server need to send a login request [26]. Finally the authentication phase both embedded device and cloud server mutually authenticate each other using EEC.
algorithm. Despite EEC algorithm has a small encryption key but it increases the size of the encrypted message significantly. ECC algorithm also is more complex and more difficult to implement than other cryptographic algorithms and required more processing resources.

In [27] Threshold Cryptography-based Group Authentication (TCGA) scheme for the IoT is proposed. This model provides authenticity for all IoT devices based on group communication model. TCGA is designed to be implemented for Wi-Fi environment. It creates a secret channel or session key for each group authentication and it also can be used for group application. Each group has a group head which is responsible for key generation and distributing these new keys every time when a new group member is added to preserve group key leakage this group head is referred to as Group authority. Proposed algorithm has five main modules: key distribution, key update, group credit generation, authentication listener and message decryption.

SEA [28] which is a Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. This architecture mainly depends on certificate-based DTLS handshake protocol. This architecture includes the following main parts: medical sensor network which gather information from patients body or rooms to help in treatment process and medical diagnosis. The second component is Smart e-Health Gateway which enables various system communication and acts as intermediate for MSN and the internet. The third part is Back-End System which receives, processes and stores collected information.

In [29] a lightweight mutual authentication schema has been proposed, this schema validate the identities of IoT devices participated in the environments before participating in the network. They proposed decreased communication overhead. Constrained Application Protocol (CoAP) has been chosen as under layer protocol for providing communication between IoT devices. Authentication is completed using the 128-bit Advanced Encryption Standard (AES). The identity of the clients and server is firstly identified. Then it provides different resources to the clients based on specific conditions determined in the request. The conditional specific data transmission minimized the transmitted packets number which results in reducing energy consumption and computation. Bandwidth utilization of the communicating is also decreased.

In [30] proposed a new CoAP option. The Constrained Application Protocol (CoAP) which works at the application layer provides the ability to retrieve data from devices like metadata and its sensor measurements. Various real time applications utilize these informations. But, sometimes it is a security requirement to not retrieve raw communication data. But only abstractions, including high level state of the observed entities. In addition to the nature of the resource constrained devices which can be accessed by anyone on the Internet, energy consumption reduction mechanism plays a critical role. Proposed mechanism contributes to these two requirements which can result in high-level states creation of readings the raw sensor. Proposed option reduces the messages number when observing a sensor resource which can result in energy consumption reduction and increasing lifetime of the device.

PROPOSED AUTHENTICATION MECHANISM

Prevent resource exhausting in IoT environments has the highest concerns in developing approaches. The resource restricted nature of IoT environment devices requires authentication mechanism that fit the limited memory, processing and energy of IoT devices. In this research proposal, an authentication mechanism depends on Constrained Application Protocol (CoAP) [31] and Elliptic Curve Cryptography [32].

CoAP has been designed IETF working group of Constrained Restful Environment (CoRE). The goal of this CoRE is to provide an efficient architecture for the highly constrained networks of sensor nodes. CoAP provides these constrained nodes to implement web transfer which can be used for IoT communication. As shown in Figure 3 different protocol stack has been used with IoT environment with different new protocols that have been designed to fit the limited resources of IoT environment including 6LoWPAN [33], CoAP, MQTT and XMPP.

![Figure 3: IoT Protocol Stack](image)

There are many differences between CoAP and HTTP protocol. CoAP allow machine to act as both client and server. It also exchange messages in an asynchronous nature, these messages are transferred over a datagram oriented transport protocol like UDP. An optional Request/Response layer is added with the CoAP messaging to provide reliable connection like TCP as shown in Figure 4. This optional layer can be used to deal with both UDP and asynchronous interactions. The packet overhead is minimized by enforcing a 4 byte header field. CoAP also provides some HTTP methods like GET, POST, PUT and DELETE and it also provides similar response codes to reflect the execution status based on client request.
CoAP provides four different types of messages:

**CON Message** which refers to “Confirmable” request. When a source node sends a CON request, the recipient has to respond with ACK message.

**NON Message**: which refer to “Non-Confirmable” request that when a source node sends a NON request, the recipient is not required to respond back.

**ACK Message**: which refer to “Acknowledgement” messages which is send back as a response to a CON message. When processing succeeds, the recipient of a CON message should respond back with an ACK. The ACK message can also contain result of the processing along with.

**RST Message**: which refer to “Reset” message this type of messages is sent back when the recipient of a message encounters an error, does not understand the message or is no longer interested in the message sender.

Elliptic Curve Cryptography (ECC) cryptography algorithm was first proposed by Miller and Koblitz in the late 80’s. It is an asymmetric cryptographic system which implements similar security to popular RSA cryptography system but with much smaller key sizes [34].

To achieve similar level of security restrictions, ECC utilize much smaller key sizes and provides higher levels of security when it is compared to other existing asymmetric cryptography techniques. Those features is more clear larger key sizes, for example a 256-bit symmetric key must be protected by more than 15,000-bit RSA, on the other hand, ECC uses an asymmetric key size of only 512 bits to ensure equivalent security level. This reduction of key size led to significant cost saving and more compact design implementation. Smaller chips or nodes can run cryptographic process faster and more efficiently with minimized power consumption. These features are suitable for environments with resource constrained. Table 1 provides a comparison of key size for equivalent security levels between ECC and RSA [35].

<table>
<thead>
<tr>
<th>Key size of ECC</th>
<th>Key size of RSA</th>
<th>Reduction ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>163</td>
<td>1024</td>
<td>1 : 16</td>
</tr>
<tr>
<td>256</td>
<td>3072</td>
<td>1 : 12</td>
</tr>
<tr>
<td>384</td>
<td>7680</td>
<td>1 : 20</td>
</tr>
<tr>
<td>512</td>
<td>15360</td>
<td>1 : 30</td>
</tr>
</tbody>
</table>

Table 1: Comparison between ECC keys and corresponding RSA keys

Proposed authentication architecture will implement an ECC authentication mechanism over CoAP connection. By combining these two approaches, optimized overhead can be added to the IoT network which leads to minimize the communication and processing required authenticating IoT devices and achieving powerful security level. Table 2 illustrates the features of both CoAP and ECC.

<table>
<thead>
<tr>
<th>CoAP Protocol</th>
<th>ECC Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Constrained Application Protocol is a web transfer protocol which is designed to fit constrained devices and constrained networks.</td>
<td>• Elliptic Curve Cryptography is an asymmetric cryptographic system and provides RSA similar security but with much smaller key sizes.</td>
</tr>
<tr>
<td>• CoAP implements a request/response interaction approach between endpoint applications.</td>
<td>• ECC utilize much smaller key sizes and provides higher level of security.</td>
</tr>
<tr>
<td>• CoAP includes key concepts of the Web including URIs and Internet media types</td>
<td>• ECC fit the requirement of constrained devices of IoT environment.</td>
</tr>
<tr>
<td>• CoAP is a very common and reliable for data transferring in IoT environment.</td>
<td>• ECC provides reliable encryption with minimized overhead.</td>
</tr>
</tbody>
</table>

Table 2: CoAP Protocol and ECC algorithm description and Features

Authentication mechanism can be passing through multiple stages.

**Stage1**: initialization phase where Control system generates a private key and a public key for its communication using ECC.

**Stage2**: device registration phase includes the pre authentication process over CoAP where IoT devices is checked if it is already authenticated or not. Control station checks the device ID and finds out if there is a corresponding entry for it. If not it uses its ID with control private key to generate an encrypted password and store it back in the IoT device.
Stage3: Mutual authentication stage, IoT device use this password to generate authentication key and send it back to the control system when it is try to connect it. Control system check these key using corresponding IoT entries stored at the control system.

Stage4: all traffic pass between IoT devices and control station then will be encrypted and secured against different types of attack.

Figure 5 proposed authentication mechanism shows the detailed steps of proposed authentication method between IoT device and control station.

Figure 5: Proposed authentication mechanism

CONCLUSION
In this paper, a review on IoT usage in healthcare has been presented. Security issues are very critical for healthcare field. These issues have been overcome using a reliable authentication mechanism. The proposed reliable authentication mechanism mainly depends on CoAP with ECC algorithms. Proposed method fit the requirements of IoT constrained devices. Small ECC key has reduced the calculation requirements while providing a powerful encryption better than other types of cryptography.

ACKNOWLEDGMENT
The authors would like to acknowledge the assistance provided by the Network and Communication Technology Research Group, FTSM, UKM in providing facilities throughout the research. This project is partially supported under the Fundamental Research Grant Scheme FRGS/1/2015/ICT03/UKM/02/2.

REFERENCES