ENHANCING SECURITY IN INTERNET OF THINGS ENVIRONMENT BY DEVELOPING AN AUTHENTICATION MECHANISM USING COAP PROTOCOL

Samah Mohammed S ALhusayni and Wael Ali Alosaimi, Ph.D.

Taif University, Saudi Arabia

ABSTRACT

Internet of Things (IoT) has a huge attention recently due to its new emergence, benefits, and contribution to improving the quality of human lives. Securing IoT poses an open area of research, as it is the base of allowing people to use the technology and embrace this development in their daily activities. Authentication is one of the influencing security element of Information Assurance (IA), which includes confidentiality, integrity, and availability, non repudiation, and authentication. Therefore, there is a need to enhance security in the current authentication mechanisms. In this report, some of the authentication mechanisms proposed in recent years have been presented and reviewed. Specifically, the study focuses on enhancement of security in CoAP protocol due to its relevance to the characteristics of IoT devices and its need to enhance its security by using the symmetric key with biometric features in the authentication. This study will help in providing secure authentication technology for IoT data, device, and users.

KEYWORDS

Authentication , authorization, key agreement, anonymity, traceability, Security, Cybersecurity, Secure by Design, Next Generation Internet, Smart City, wireless sensor networks, 5G network, the Internet of Things, CoAP, symmetric key and biometric.

1. INTRODUCTION

This research introduces research background of authentication mechanism in Internet of Things (IoT). It explains the concept of IoT, and how networks and computers have evolved until IoT appeared and merged with blockchain and artificial intelligence, homes, cars, smart cities and more than that. An example of smart cities is the technical city of NEOM, which illustrates the Kingdom's role in adopting technical projects and its leadership in this field, which requires awareness of members are of the importance of this stage and their role in it.

1.1. Overview of IoTs

Internet of thing (IOT) means a network which joined many things via internet[3] which help to achieve the end users goals [4]. The Internet of Things is a combination of technologies that work to connect many things over wired and wireless networks which handle by people, machines, or both[3] These things are connected to a platform that is manage within certain rules, analyze, process and store data, detect security threats, respond to any thing[5]. The level of competency

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 35-54, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111103

is measured according to the level of achievement of the tasks[5]. IOT system will be good as it can true response in any alteration there[6, 7].

Communication technology has developed very greatly in this era, where it started with a device that is no longer used now such as the telegraph, then the phone, and then the computer appeared that created another world as it began to solve complex mathematical operations and codes and was very large in size[3].Then, it developed and shrunk its size and increased its speed then appear of the personal computer which serves business offices and people through word processing programs, tables, and the like, and then to laptops, tablets, and smart devices with various applications where the combination of the Internet and WWW is important of IoT[3].

Internet also developed little by little, so the Internet of things was formed, starting from small closed networks to integrating more than one network, due to the emergence of microcontrollers with low cost and complexity ,and adequate processing power, so appeared educational websites, videos, forums and blogs .The Internet of things was not limited to commercial projects and extended to the Internet of things to consumers, and companies contributed provided smart home tools such as Google Apple and Siemens. The Internet of things developed to Hundreds of platforms and thousands of applications appeared, including the industrial Internet of things to automate many industrial then IoT evolved from a large infrastructure to the Next Generation Internet (NGI) that integrates with Internet systems for things such as augmented and virtual reality, machine learning, artificial intelligence, and blockchain to obtain professional tools[3]. The Internet and advanced wireless networks have a significant role to play in the widespread use of mobile devices that play a major role in consumer access and power over the different devices and services of the Internet of Things across Wi-Fi networks and mobile networks[8]. Such as fifth generation networks that are an active choice for IoT implementations like smart house, smart cities , smart healthcare, smart grids, etc.[9]. such as the city of Neom in Saudi Arabia, which depends on artificial intelligence and provides development and investment solutions to become a famed center in the region and there is a great trend for other smart cities and most services have been automated to become electronic. This was an example in a country as well as many countries, which means many users and applications and big data.

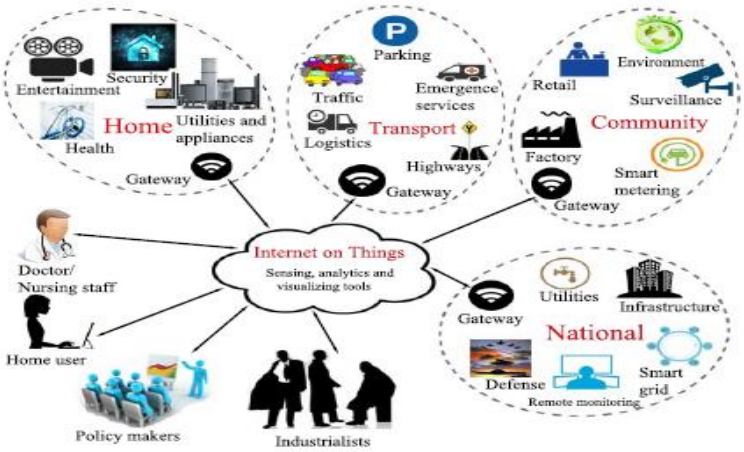

Figure1. IoT network architecture[1]

The above figure represents a summary of the structure of the network in IoT which has many applications transportation, smart homes and cities, community and industrial services, as well as

multiple users enter the system via the Internet through a portal in which the user is authenticated, which is the first stage and an essential part of the safety of the Internet of things.

Thus, within this development and the large number of users, it has become a target for adversary and owners of illegal targets and hackers, which required states and decision-makers to put in place laws and legislation that protect everyone and deter everyone who takes an irregular way to achieve his goals. Among the scholars and researchers are preparing studies for various possible security attacks, gaps that are a pathway to them, motives and points related to the subject, and providing security solutions that keep pace with this development and help in raising the level of security, responding to attacks, overcoming problems, and recovery.

1.2. Overview of IoTs

The spread of Internet of things networks in different milieus and for various purposes represents a security challenge that requires securing networks from any attack. IoT-linked protection problems are becoming more and more concerning due to the ubiquity of IoT and use at sensitive implementation, where intensify the effects at every security breaches to the degree that they are life-threatening [10]. The report [11] indicated that 20% of the institutions were attacked once at least, and exploited to be through which to attack [12, 13]. From this standpoint, and by looking at the graph in the picture 2, which shows that there is an increase of nearly a third of the number of devices for the year 2025, which means an increase in the probability of attacks significantly. The security specifications of the IoT rely greatly at the amount of providing services; the necessity to secrecy, integrity and authentication relies specifically about the security requirements at the IoT network app [10]. In special, authentication is known to be a critical prerequisite for IoT [14].

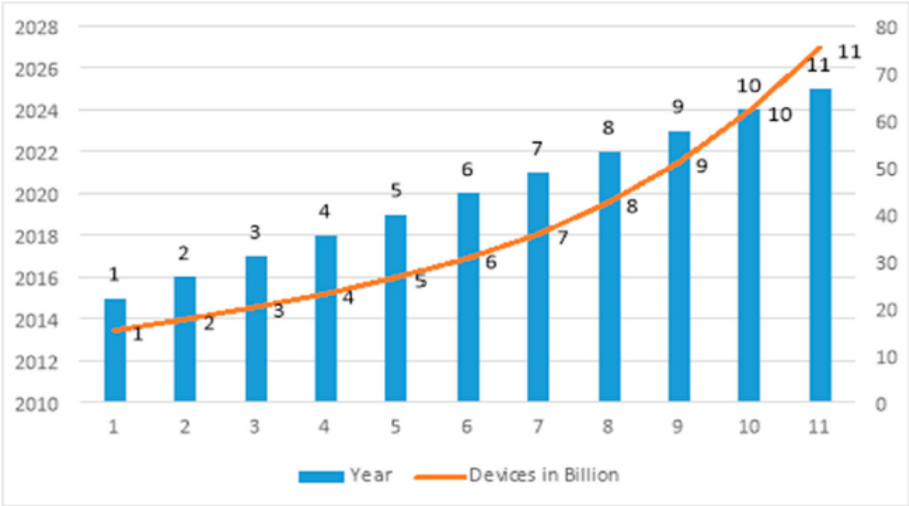

Figure 2. Awaited devices in the Internet of Things by 2025[2]

1.2.1. Elements of Authentication

According to what is in [10], a set of points related to authentication and its relationship to the Internet of Things can be presented as following:

-Identity: data submitted by an entity to another in order to trust itself and one or a mixture of hash, symmetric or asymmetric encryption methods may be used for identity-based authentication schemes.

– Bodily: biometric features depending on a person's physical features, like fingerprinting, hand geometry, retina scanning.

– Behavior: biometric depends on social behavioral features, e.g. keystroke dynamics, walk analysis, speech ID.

1.2.2. Using Tokens

-Token-based Authentication: validates the user or computer on the basis of an identity key generated by the server.
-Non-Token-based authentication: requires the use of user id and password tokens any moment the content needs to be shared.

1.2.3. Authentication Method

-A-way authentication: just one entity can validate the other, but the other will not be validated.
-Two-way authentication: the two organizations authorize one to another.
-Three-way authentication: essential authority verifies the two entities and allows them to validate each other.

1.2.4. Architecture of Authentication

Distributed direct authentication between the entities to the correspondence.

A central server or a trusted third party to spread and maintain authentication certificates.

1.2.5. IoT layer

The layers how where an authentication mechanism is implemented.

-Perception Layer: Liable to storing and dealing out the data obtained via the entities on the IoT network.
-Network layer: liable to obtaining and manipulating the obtained information of the perception layer.
-Application layer: liable of collecting information of the second layer and then availability service demanded of the customer.

1.2.6. Hardware-based

The authentication method may involve the physical properties of the devices or devices to be used.

-Implied hardware-based: applies hardware physical features to improve authentication, like Physical Unclonable Method (PUF) or Valid Random Number Generator (TRNG).
-Outright hardware-based: Several authentication methods were dependent at the utilization from the Trusted Platform Modules (TPM), a device which holds and manages the codes applied in device authentication.

1.3. Problem Statement

The development of the Internet of Things technology and the people's dependence on it in many matters of their lives requires securing it against any attack and revealing its vulnerabilities and

immunizing them. The first step of securing any technology is by conducting an effective authentication technique. Therefore, this study will review the existing authentication techniques in IoT environment in order to propose a harder authentication technique.

2. LITERATURE REVIEWS

This section includes a summary to the current authentication mechanisms inside IoT environment. Specifically, CoAP protocol components, characteristics, and mechanism is presented

2.1. Existing Authentication Mechanisms

Table (1) summarizes existing authentication mechanisms in terms of their aims and approach.

Table 1. Previous Authentication Mechanisms

Research Title	Year	Aim	Research Approach
Authentication of IoT Device and IoT Server Using Secure Vaults[15]	2018	Solve problem of Single password-based authentication mechanisms which put IOT vulnerable of many attack	Provides a reciprocal authentication method consists of multi-key or passwords where named the shared secure between the IoT server and the IoTclient as secure vault. After each successful session among the server and the IoT equipment, the collection of passwords is modified.
Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks[1]	2018	Design of a new secure remote user authentication scheme	Design user authenticated key management protocol UAKMP which based on three variables are smart consumer card password, and private biometrics. Compared to other existing systems, UAKMP is more stable, supports the nodes addition process, and even the key and biometrics change process internally without the GWN's mediation.
Multi-level Trust based Intelligence Schema for Securing of Internet of Things (IoT) Against Security Threats Using Cryptographic Authentication[16]	2020	Reduction of gray hole attacks using check node information with detection rate of 94.5percent against gray hole attack	Depend on AODV routing protocol and is offered below the MTISS-IoT. The suggested solution is based on cryptography authentication and consists of four steps, like checking node trust in the IoT, path monitoring, detection of gray whole attacks, and the removal of malicious attacks in MTISS-IoT.
A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments[17]	2020	Developed LBCbAP a modern encryption protocol based on lightweight block ciphers agnist hidden exposure and desynchronization attack.	A latest stable protocol established on lightweight block ciphers, LBCbAP, backed via formulated or not formulated security evidence, was introduced. In this protocol we use a block cipher CRAFT as the central primitive security that illustrates its security against different forms of threats, including hidden exposure and desynchronization threats.

Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments[18]	2020	Suggests an easy and reliable authentication scheme for WSNs in IoT systems based on temporal credentials and dynamic IDs.	It follows the standards for the authentication system's basic architecture specifications and enhances security efficacy in real-world IoT settings. In comparison with the other systems, the performance review showed high reliability and better performance for the method.
Smart card-based secure authentication protocol in multi-server IoT environment[19]	2017	Suggested a smart card-based authentication protocol and tested it using AVISPA by visualizing a structured validate scenario	It authenticates each entity via letting people to use a smart card transferred via invalidation server to go through the verification process and access to an IoT-connected server and the authentication protocol is used in different applications such as key exchanges, using smart card, and more.
BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology[20]	2020	Suggestion a Machine to Machine Authentication Protocol for Smart City Apps leveraging 5 G Technologies (BIDAPSCA5 G) built on the Blockchain Internet of Things (IoT).	The registration process of connected devices is carried out via secret blockchain accessible only by authorized individuals. Shared authentication was conducted without RAC, Gate-Way-Node (GWN) intervention to minimize the cost of processing location-based authenticate process, blockchain-based repeal.Step and IoTD registration, device-level IoTD confidentiality property.
A secure authentication scheme for IoT application in smart home[21]	2020	Presented a secure addressing and authentication (SCSAA) framework based on a smart card by changing the existing IPv6 method to minimize security issues in the IoT.	By issuing a special 64-bit Interface Identifier (IID) to smart phones or programs and authenticating them securely in the IoT system, it presents a strong way of addressing and using the hidden session key to block unauthorized access to the network. It is tested by model ROR and the method AVISPA.
A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment[22]	2019	In order to solve security issues such as session key leakage, impersonation and replay attacks, a stable and flexible three-factor authentication solution for IoT in the cloud computing world	This authentication protocol can stand multiple attacks and provide protected mutual authentication between user Ui, cloud server Sj, and server CS control using BAN logic analysis and protection using hidden and biometric parameters using only bitwise exclusive or (XOR) and hashing functions to make it more powerful than the schemes of Pelaez et al.
Secure Authentication Protocol for 5G Enabled IoT Network[23].	2018	Supply an appliance layer authentication protocol to minimize all attacks emanating as of the public access network. and examine the security protocol by An advanced security monitoring platform Scyther	Introduce an effective protection protocol in the Application layer, among client-Equipment and Mobility Management Feature (AMF) that is taking charge of the ration of resources after the verification of Network Slice Collection Association Details (NSSAI) of 5G network. Where the request for user passwords and services is secretly shared, thereby maintaining anonymity and the protocol is immune

			to numerous attacks that which arise from secrecy, honesty and availability.
A three-factor anonymous user authentication scheme for Internet of Things environments[24]	2020	suggest an upgraded three-factor user authentication mechanism to overcome security problems which find in Dhillon and Kalra schema	Indicate a three-factor anonymous user authentication method for IoT environments that follow a specific four stages: registration, login and authentication, changing of password, and user revocation stage, and use the random oracle model, BAN logic, and ProVerif tool to conduct informal and structured security assessments. The findings of the study suggest that the proposed system is protected from different documented attacks and meets all protection criteria and is compliant with relatively low-cost IoT systems.
Dynamic Authentication Key Agreement Scheme for Effective Path Selection in I IoT Systems[25]	2020	Provides a new solution that uses an active authentication key agreement system in which only legitimate users can access data in the IIoT setting from IoT sensor nodes.	For key validation and protected data transmission, the Dynamic Authentication Key Agreement System (DAKAS) and the Efficient Route Selection and Access Control Logic System (EPSSCLS) are used. It is support add of new nodes after the state of before-process of deployment in the network, the process of the complex node IoT sensing system and the transmission route are revoked in the event of any intrusion detection or stolen and leaked information by an opponent. Using the true or random (ROR) model and AVISPAA, structured security checking is carried out.
Smart Contract-Based Cross-Domain Authentication and Key Agreement System for Heterogeneous Wireless Networks[26]	2020	Formulate a cross-domain authentication and key approval scheme setup on a blockchain smart knot.	Cross-domain authentication and key agreement protocol are configured. The smart contracts are used to handle the shared keys of the nodes, and the device parameters are checked by contract demand. Customers can pick momentary authentication specifications based on the roaming domain system specifications to complete the encryption and authentication arrangement, and users are private in the operation. The protocol does not have complex encryption and certificate authentication processes, that reduced overhead of computing and connectivity.
On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks[27]	2020	Provides a stable and effective authentication protocol depending on 3-factor authentication using biometric data and employs the honey	suggest an effective protocol to defend against brute force and theft smartcard attacks which uses only hashing algorithm, except public key Elliptical Curve Cryptography and Conduct informal vulnerability scanning,

		list technique and provide protection even though two of the three factors are hacked.	model-based Real-Or-Random (ROR) and logic-based Burrows Abadi Needham (BAN) official security evaluation, and conduct formal verification employing (AVISPA) simulation tools.
A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things[8]	2020	Introduce system design by proposing the incorporation of WSNs and 5 G into IoT. Centered on the crypto analysis of Adavoudi-Jolfaei et al.'s scheme and device architecture, we present a privacy-based elliptical curve encryption (ECC) Keeping the WSN verification, authorizing, and mutual authentication framework in 5G incorporated IoT.	They studied the three-factor authentication and control access scheme of Adavoudi-Jolfaei et al. and highlighted its vulnerabilities, and then implemented a device implementation appropriate for WSNs in 5G-integrated IoT. On the basis of thestructural design, An ECC-based three-factor verification, authorizing, and mutual authentication framework was proposed.
A Security Approach for CoAP-based Internet of Things Resource Discovery[28].	2020	Provides a protection strategy employing TACACS+ to security improving of the CoAP which Assists entrance check , identity verification and auditing	A protection solution to the CoAP technique utilized explore resources in the IoT field. The protection strategy is focused on the Utilization of the TACACS+ protocol to enhance the security of the CoAP.

The table above shows a recent set of authentication techniques in the Internet of Things. This secure authentication of IoT objects is done in several ways

Using two factors such as[15] which use AES encryption and HMAC and have more saving power compared with ECC algorithm. In[18]based on temporal credentials and dynamic IDs which depend on MAC to secure translate of data. In [20] using ECC and SHA-1 algorithm to mutual authentication between tow IOT devices. In [25] using the Dynamic Authentication Key Agreement System (DAKAS) and the Efficient Route Selection and Access Control Logic System (EPSSCLS)for key validation and protected data transmission. In [26] cross-domain authentication and key agreement protocol are configured and the smart contracts are used to handle the shared keys of the nodes.

Or three factors as in[1] proposed UAKMP which based on three variables are smart consumer, card password, and private biometrics. In [22]using hidden and biometric parameters, only bitwise exclusive or (XOR) and hashing functions. In [24] indicate a three-factor anonymous user authentication method for IoT environments that follow a specific four stages: registration, login and authentication, changing of password, and user revocation stage. In[27]using biometric data and employs the honey list technique and provide protection even though two of the three factors are hacked. In [8]introduced a three verification, authorizing, and mutual authentication framework built through ECC.

By using these technologies, many attacks are countered and security goals achieved like in [16]detection rate of 94.5 percent against gray hole attack. In [17] approach secure agnist hidden exposure and desynchronization attack. In [19] protected from identity plagiarism and exposure of key. In [21] using strong way with hidden session key to block unauthorized access to the network. In [22]solve security issues such as session key leakage, impersonation and replay attacks. In [23]maintaining anonymity and the protocol is immune to numerous attacks that which arise from secrecy, honesty and availability. In [27]defend against brute force and theft smartcard attacks. In [28]separator security amidst users depend on the permissions available to them to ensure authentication, authorization, management of access and auditing services.

2.2. Constrained Application Protocol (CoAP) protocol

Constrained Application Protocol (CoAP) has a constant byte header of only 4 bytes, but constrained assets are used[29]. The cost-saving availability of RESTful resources in Low-Power Lossy Networks (LLNs) combined with limited sophistication in form head of protocol , message decoding, asynchronous transfer framework and built-in asset exploration renders it an optimal option for IoT deployers. So for These characteristic aspects make CoAP an optimal substitute for current IoT devices like MQTT and XMPP[29]. CoAP is therefore implemented in a variety of products, like transportation logistics, housing automation, intelligent cities and shipment monitoring[29].

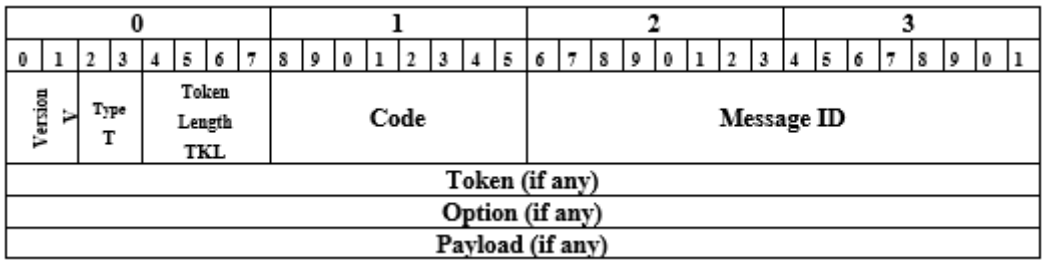

Figure 3. CoAP packet with 4 bytes.

CoAP is a constraint state that caused a terrible package transfer and a large overhead, such as a limited hub with small RAM or Processor power, and is a request/response technique [30]. It is designed by the Internet Engineering Task Force (IETF) by an idea of device to device applications and platform automation to minimize overhead, optimize packet transference and increase work simplicity by using the main HTTP application [31]. The main characteristic of CoAP is an integrity and reliability [32], as it supports unicast and multicast demands by leveraging User Datagram Protocol (UDP), and gives the ability to exchange asynchronous messages [30]. It is able to interoperate with HTTP because it introduces an internet transfer protocol dependent on the Representational State Transfer (REST) above the HTTP features [33]. But because CoAP is dependent on REST, the CoAP-REST proxy provide a direct transference of these protocols. CoAP/HTTP assists CoAP users to connect HTTP server assets using a reverse proxy that converts the HTTP state key to the CoAP response code [34]. CoAP helps devices with mini power, connection, and computing capacity systems to use RESTful activities [35]. CoAP is proposed by scholars, owing to its light properties, to be used in a variety of fields from applied of smart cities to the commercial WSNs [36].

CoAP is a simple device layer request/response protocols for both synchronized and unsynchronized answers[35]. CoAP has the below data packets and answer forms: provable, needs an acknowledgment inside the ACK or with an independent message. Non-confirmable (no

need for ACK), restart (verified receipt of a text that could not be executed) and acknowledgment (proven receipt of have a provable message), Piggy-backed answer (receiver answer is piggybacked to ACK) and independent answer (receiver answer in a text other than ACK after some moment)[35]. As HTTP, CoAP utilizes GET, PUT, POST and DELETE methods for generating, restoring, modifying and removing processes[35].

The researcher in[35] mentioned the elements of CoAP and its distinguishing properties as follows:

2.2.1. Components of CoAP protocol

1. Last node Determined by IP and UDP port number. The last node is the target or origin of the CoAP packet.
2. Dispatcher who creates message.
3. Receiver message.
4. Consumer who put an order rather than a message
5. Server the recipient last node of the demand and the source node of the reply.
6. Source server: A service is generated or exists on this server.
7. Intermediate: is a last node that can perform as a host and a consumer to a source server.

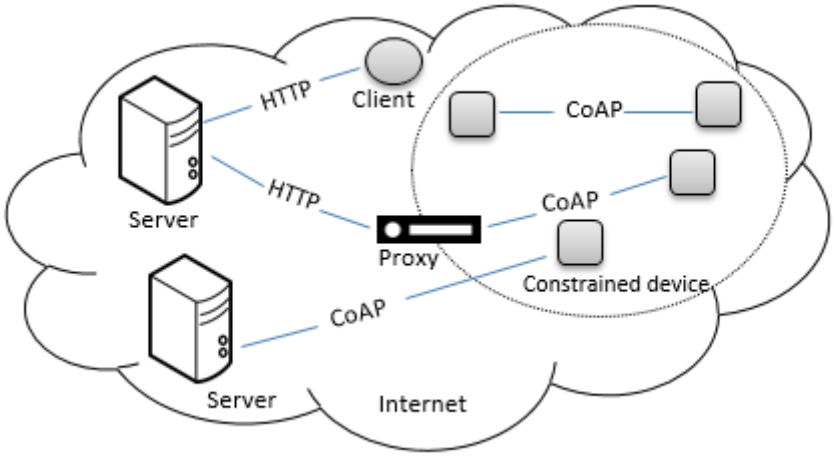

Figure 4. CoAP transaction

Figure 4 explained CoAP interaction between elements with more cases of them.

2.2.2. CoAP protocol characteristics

1. Assets monitoring: on-request subscriptions utilizing publish/subscribe system for tracking online services
2. Move of the block resources: without refresh the entire data in order to transmitter data and receive. This minimize cost communications.
3. Asset exploration: URI patterns are utilized which utilize website domains in the CoRE link format to allow the exploration of resources for consumer.
4. Dealing directly with HTTP: CoAP is simple communicate with HTTP according to the standard REST structure that contributes to flexible interaction.
5. Most programming languages like C, C #, Javascript, erlang, Ruby contain CoAP libraries as well as for iOS and Android.
6. CoAP has smaller processor and Capacity consuming and is easy to use[35].

2.2.3. Drawback of CoAP

The CoAP protocol does not include trusted standards for secure structures and its messages are secured on top of the UDP in the Datagram Transport Layer Security (DTLS)[37] that was not initially designed for resource-limited devices so it is not suitable for a CoAP agent[36]. Like , in executing a handshake procedure, DTLS requires six travel messaging that raise workload information exchange and consume restricted power from machines[36].

A number of scholars have undertaken DTLS research to protect the protocol, but substantial work remains to understand how securing CoAP is controlled and applied[38, 39] with maintaining large efficiency after having the requisite security for transmissions[36].

CoAP protocol is defined as large inertness, terrible packet transmission, and its inability to be used on a complicated category of data[30].

2.2.4. Security for CoAP protocol

The DTLS protocol is running over UDP and gives for encrypted CoAP exchanges [33]. Supports validation, auto key management, secrecy, encryption technologies and data integrity but DTLS not support multicasting like CoAP [33] and we know all that CoAP protocol is one of routing application layer witch related with authentication directly. CoAP protection is a significant factor owing to the unavailability of trustable specifications to protect the CoAP structure[36]. DTLS offers security services, including anonymity, honesty, authentication and non-rejection facilities using the essentials of the AES/CCM[38]. According to[36] DTLS handles key protection aspects such as authentication, anonymity, password retention, and message integrity in four forms:

1- No Sec Type: where it expects that the protection function will be enforced with other protocol layer, and therefore data will be transferred without security.
2-PreSharedKey Type: which machines that are permitted to applied itself system with a singular symmetric key which allows to connect with other machine?
3-RawPublicKey Type: is known to be important for the working of the CoAP and usually adopts the machines that needed authentication, and utilizes the asymmetric password for each machine to identify and communicate with these machines.
4-Certificates Type: is known to be an authentication method for machines that execute CoAP via an X.509 certificate.

2.2.4.1. Challenges of using DLTS

It needs four transmission and return transmissions, three of which are for DTLS and one for COAP, which supports multiple transmissions and which distinguishes the Internet of Things while not supported by DTLS this one of disadvantages of using DTLS [40].

The DTLS interaction protocols may (yet including the ungoverned cookie) lead to an aggressive assault on battery-operated system resources. As a response, nodes may miss their position in the connection and interrupt the whole network.

Although DTLS will secure from replay attack through the bit image frame, packets must be received initially via nodes, translated, and often transmitted. The probability of this threat may cause the network to overflow without scanning proxies as 6LoWPAN Border Router (6LBR).

Separation of handshake packets also has a problem Too the hashing is important to execute everything to validate handshake packets Messages that indicate a big buffer to several nodes are necessary and in each situation this does not applied

Security in DTLS does not do well with CoAP so all messages need to be resend if one is lost also when all packets in-flight transmission transfers in a UDP packet, much assets needed big buffers for managing.

2.2.4.2. Object Security for Constrained RESTful Environments

OSCORE is a new universal solution which offers cover-to-cover protection for CoAP transactions on the application layer [41]. OSCORE is a good choice to security in CoAP protocol than DTLS. Where the presence of the DTLS layer requires step-by-step security between both the transfers between the server and the proxy and also the enforcement of protection between the agent and the client [41]. While OSCORE provides secure two-way Contact among the client and the server is secured by using a proxy [41]. The security solution allows proxies to perform their functions as forwarding and scheduling CoAP queries connected to servers. OSCORE's effectiveness at protecting and decoding messages is superior to DTLS using HMAC and authenticated encryption associated data AEAD [41]. OSCORE reaches this outcome through a very better execution of the AES encryption [41]. OSCORE consumes greater RAM than CoAP but DTLS consumes greater than OSCORE [41]. Its outcomes in a per-exchange power usage of around 8–28 percent greater than that of CoAP [41]. This means that OSCORE is most power saving than CoAP, which outcomes in a power demand of around 17–59 per cent increaser than COAP [41]. OSCORE execution shows simple improved efficiency than TinyDTLS in respect of overload network messaging, RAM utilization, transmission round-trip time and effort consumption. Thus, offering security enhancements to OSCORE without extra efficiency dragging [41]. OSCORE accomplishes that result using a highly robust execution of the AES CCM 128 methodology [41].

3. RESEARCH METHODOLOGY

The proposed security solution aims to authenticate IoT users using symmetric key with biometric features. Biometric is a strong mechanism to authenticate user because it is a unique code which is hard to be hacked. Biometric features have a high demand due to its true effect in software and precision in performance[42].Symmetric key via AES-128-CCM bits is a suitable state for security with a natural IoT constrained devices when implementing CoAP protocol. The presented solution adopts these two methods to create a secure authentication mechanism between the server and the client. So that the agent verifies the client's authenticity and then begins the process of transmissions and processing of requests via original CoAP method.

3.1. Registration step

The scenario of this solution will be as the following. Assume there is a server and a client who has biometric features according to requirements of the application, as well as a symmetric key known between them. When the client wants to connect IoT devices, he sends request for the server to initiate a connection. The server requests the biometric and the shared key from the client. The customer takes the biometric image and then enters the shared key. The biometric is encrypted with the shared key until it reaches the destination. The key is decrypted then when the shared key is true, the biometric is verified and biometric stored there (for the first time). By the end of the process, object authentication and data exchange are done.

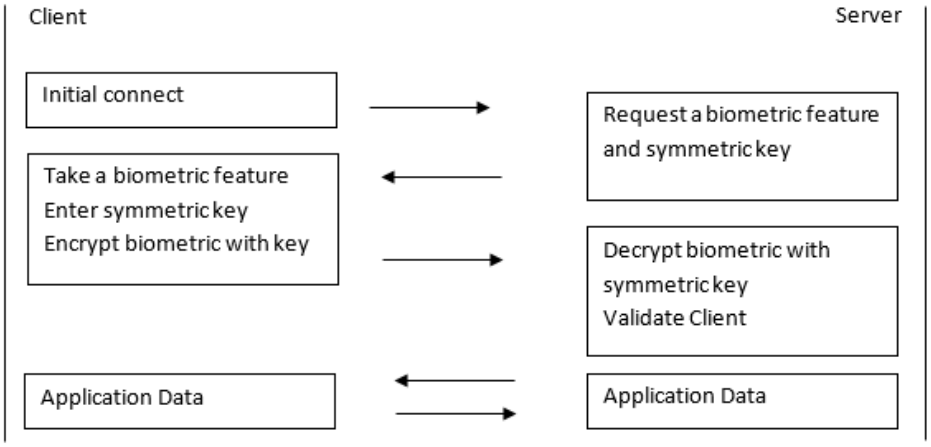

Figure 5.Senario of the Proposed Solution

3.2. Second step

Suppose that when the client wanted to connect again, the client did not need a request to start a connection and had previously contacted the server. He will send his request loaded with the encrypted biometric with the shared key to the server, which in turn receives the request and finds it loaded with the authentication part, so he verifies the validity of the biometric that stored in first step by decrypting the shared key. The validity of the key means decryption, it will verify the validity of the biometric and authenticate the client. These steps are explained in Figure 6.

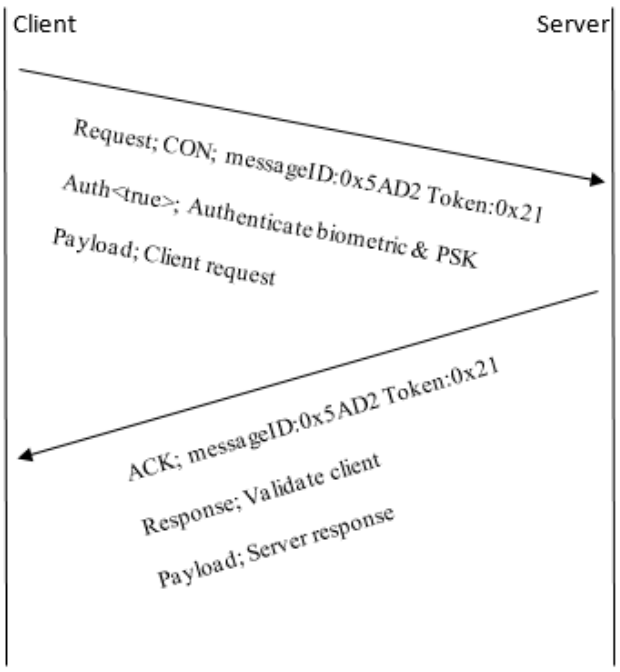

Figure 6. Authentication handshake

3.3. Transfer Data

As for what is related to the other party, which is the limited resource devices that cannot deal with encryption such as a biometric and complicated matters, the transfers between it and the server will be dependent on simple CoAP transfers because we have secured the server by securing all his clients. Thus the validity of such an assumption will provide energy and optimal use of resources in a safe environment.

4. REQUIREMENT ANALYSIS

Programming with pythonlanguage to produce the possibility of implementing the proposed solution. The application provides an authentication service to IoT clients. It uses COAP loT protocol, which depends on encrypting the client biometric by a symmetric key AES CCM 128 and validating the client in the server side by decrypting the symmetric key byfollowing these steps. The client sign up in the proposed application by registering his biometric and the symmetric key. The client biometric will be encrypted by a symmetric key. Then, the encrypted biometric will be sent to the server, which will decrypt the symmetric key and store the biometric. When the client login to the application in the next times, the server will validate the client by decrypting symmetric key and comparing his biometric with the stored biometric. If the decrypted biometric is the same as the stored biometric, then the client is authenticated. So, the server will grant him access to all connected devices. As a result, the client have access to the app (Camera) and any other control services (ON, OFF, TALK, and RECORD).

5. IMPLEMENTATION

The implementation of the suggested solution is based on python language, which can be run in any supported environment like anaconda, pycharm and so on. There are two main objectives that were relied on when implementing the program. The first is that the program works based on the CoAP protocol. Second, the verification data, which is the fingerprint, is encrypted with the symmetric key encryption algorithm, which is AES CCM 128.

The program was created to receive all fingerprints. In the client side, it is assumed a set of fingerprint images that added to the database so that the client can choose his fingerprint, which is encrypted with the encryption algorithm by calling it and then sending the encrypted fingerprint to the server. The server receives the encrypted image on the authentication block and decrypts it and tries to match the receiver fingerprint with the correct user. Upon verification, a message appears in the name of the user as a proof of validity of verification. This means that the server will allow the client to connect to the services that are available to him. Here, it is assumed that the service connected to the server is a camera device that shows the option to take a picture. A default picture was placed because it can accomplish the goal of the program as an evidence and using a real camera will consume long time and cost. These resources are not available at the present time.

5.1. Screenshot of the Program

1- The main interface of the program that appears when the client's code is executed where he can access by entering his biometric or exit program.

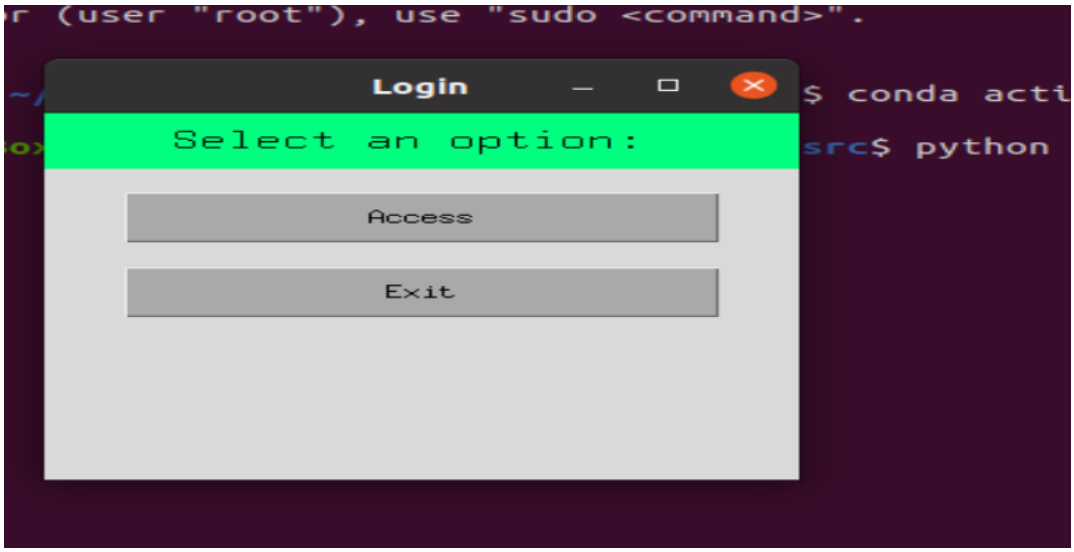

Figure 7. The main interface

2- The second screen, the client chooses his fingerprint from the set of fingerprints defined in his database, as it appears in the screen where the image is selected and then encoded with the encryption algorithm and sent to the server.

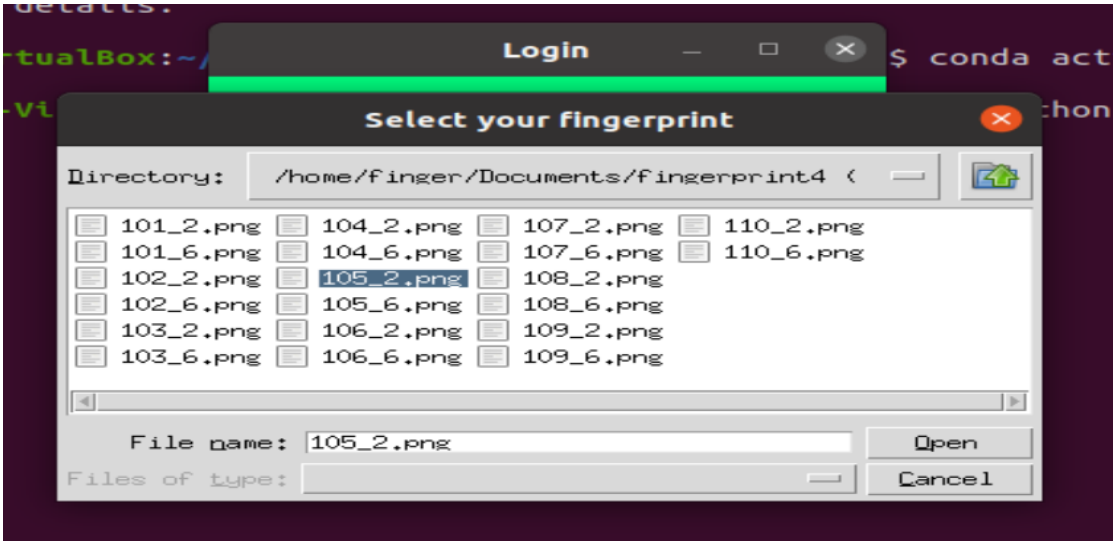

Figure 8. Second screen

3- The third screen shows the image of the received and enhanced fingerprint of the server, where it was transferred from the client side to the server via the CoAP protocol and the server decrypts the fingerprint which appear in photo as new unique message received.

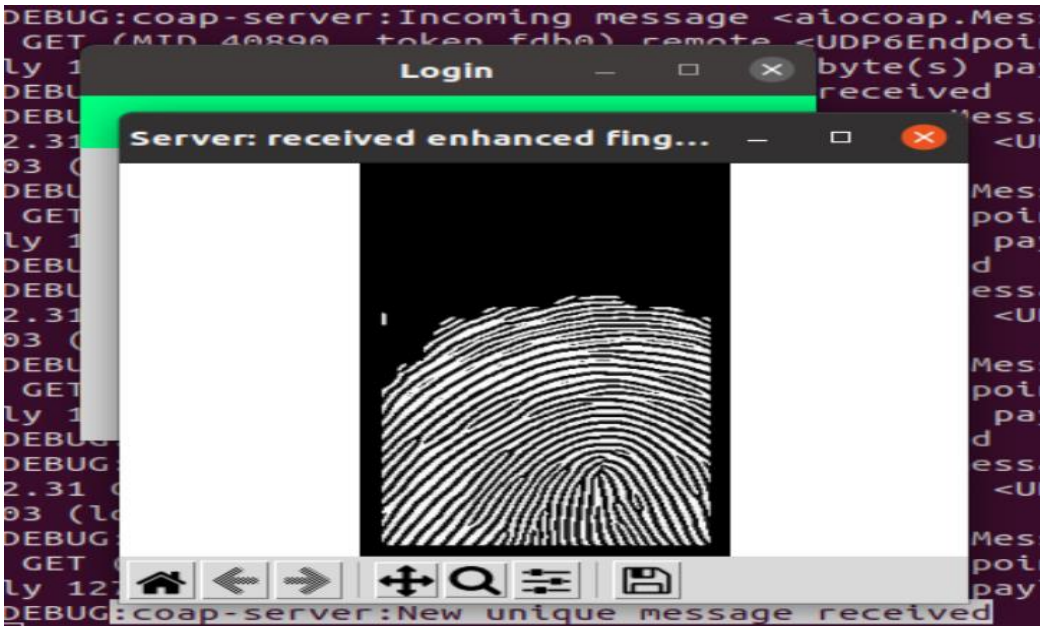

Figure 9. Third screen

4- The fourth screen shows the server verification of the client matching the received fingerprint with the correct user.

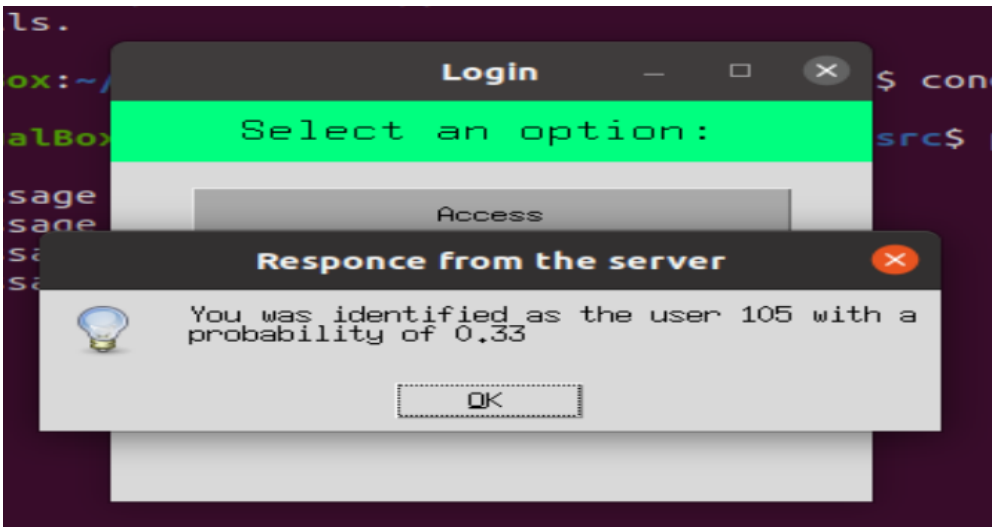

Figure 10. Fourth screen

5- The fifth screen displays linking the client to one of the server-related services, which is the camera, and allows him to take a picture.

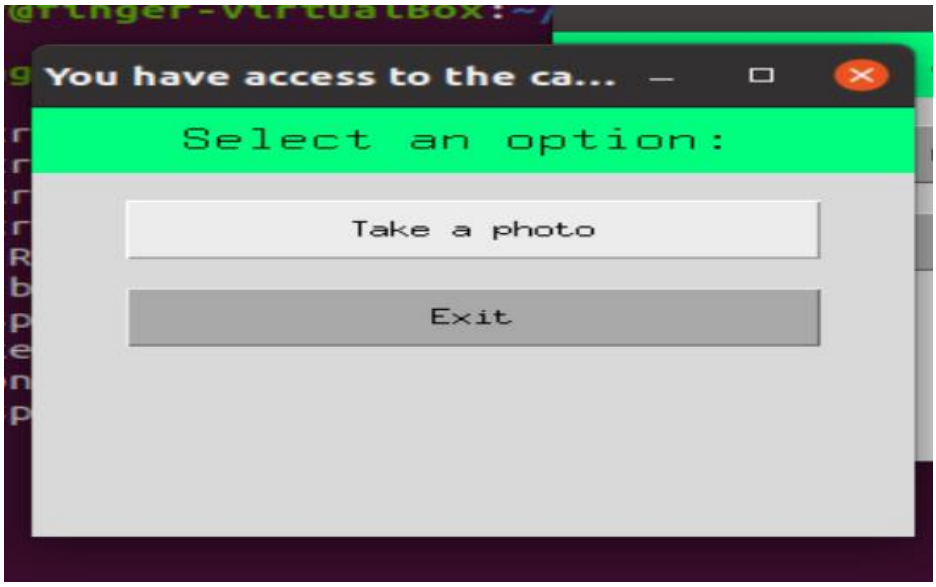

Figure 11. Fifth screen

6- The sixth screen shows the default image for the camera capture.

Figure 12. Sixth screen

5.2. Analysis of the Enhanced COAP Protocol

In this project, an authentication mechanism is applied via CoAP protocol to improve its security by using fingerprint biometric encrypted with symmetric key AES CCM. Hence, biometric feature is considered as a strong security mechanism and symmetric key AES CCM 128 is suitable for constrained devices. It is proved that the proposed solution has overcome some of the defects of the CoAP protocol, which are mentioned earlier, as its reliance on safety on DTLS is not suitable for restricted devices and costs more time. This leads to energy consumption and thus affects its effectiveness. The proposed solution is distinguished from OSCORE in that it relies on

a robust verification process, which is fingerprint, and therefore it can be said that the project have provided a good solution in this regard.

6. CONCLUSION

This project focused on enhancing security in Internet of things (IoT) by developing an authentication mechanism depending on the available features of CoAP protocol, which is the famous protocol in IoT. The study started with presenting an overview of the emergence of the Internet of things and the importance of being the focus of the study. Then, it provided a brief of authentication and its role in IoTs as the first line of defense. After that, the report summarized a list of researches to some of the authentication mechanisms in the Internet of things at the recent last years. CoAP protocol has been chosen to be the study focus because it is designed specifically for the Internet of things and its restricted devices. Python language is applied to execute the proposed security solution for authentication using a symmetric key with biometric features. The implementation proves that the proposed method enhanced security of IoT users by improving CoAP protocol performance and support CoAP library with created authentication method.

7. FUTURE WORK

As a future work, this study lays the foundation stone for the expansion of the more implementation of the authentication methods based on CoAP protocol. The proposed solution can be improved by including all kinds of biometric features, such as the iris, facial recognition and retina. In addition, the extent of its effectiveness and security when it is actually implemented in the Internet of things environment and linked to more than one device and evaluated in terms of its efficiency in enhancing security of IoT users.

ACKNOWLEDGEMENTS

I would like to thank God for his generosity in providing me the ability to perform this work. I am so grateful to my family for their love and continuous support, to my friends for their motivation, my supervisor (Dr. Wael) for his guidance and encouragement. I also sincere to express my thanks to Taif University for providing a great opportunity that allow me to accomplish my scientific goals. Especially, that coincides with the aspirations of the vision of our King the Custodian of the Two Holy Mosques.

REFERENCES

[1] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269-282, 2017.

[2] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures," *Computers*, vol. 9, no. 2, p. 44, 2020.

[3] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, 2020.

[4] S. S. Daniele Miorandi, Francesco De Pellegrini, and Imrich and Chlamtac., " Internet of Things: Vision, applications and researchchallenges," *Ad Hoc Networks 10, 7 (2012), 1497 { 1516.*, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870512000674.

[5] Google, "Technical overview of Internet of Things," update 2020/9/9. [Online]. Available: https://cloud.google.com/solutions/iot-overview.

[6] J. Manyika *et al.*, "Unlocking the Potential of the Internet of Things," *McKinsey Global Institute*, 2015.
[7] M. Botterman, "for the European Commission Information Society and Media Directorate General," in *Networked Enterprise & RFID Unit–D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic*, 2009.
[8] S. Shin and T. Kwon, "A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things," *IEEE Access*, vol. 8, pp. 67555-67571, 2020.
[9] G. Choudhary, J. Kim, and V. Sharma, "Security of 5G-mobile backhaul networks: A survey," *arXiv preprint arXiv:1906.11427*, 2019.
[10] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) Authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, 2019.
[11] D. Maresch and J. Gartner, "Make disruptive technological change happen-The case of additive manufacturing," *Technological Forecasting and Social Change*, vol. 155, p. 119216, 2020.
[12] M. E. Ahmed and H. Kim, "DDoS attack mitigation in Internet of Things using software defined networking," in *2017 IEEE third international conference on big data computing service and applications (BigDataService)*, 2017: IEEE, pp. 271-276.
[13] C. Beek *et al.*, "Mcafee labs threats report," *McAfee, Santa Clara, CA, USA, Tech. Rep*, 2017.
[14] L. Atzori, A. Iera, and G. Morabito, "" The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805," 2010.
[15] T. Shah and S. Venkatesan, "Authentication of IoT device and IoT server using secure vaults," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 819-824.
[16] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *The Journal of Supercomputing*, pp. 1-26, 2020.
[17] C. Trinh *et al.*, "A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments," *IEEE Access*, vol. 8, pp. 165536-165550, 2020.
[18] C.-T. Chen, C.-C. Lee, and I.-C. Lin, "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," *PloS one*, vol. 15, no. 4, p. e0232277, 2020.
[19] W.-i. Bae and J. Kwak, "Smart card-based secure authentication protocol in multi-server IoT environment," *Multimedia Tools and Applications*, vol. 79, no. 23, pp. 15793-15811, 2020.
[20] M. Vivekanandan and V. Sastry, "BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology," *Peer-to-Peer Networking and Applications*, pp. 1-17, 2020.
[21] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-to-Peer Networking and Applications*, pp. 1-19, 2020.
[22] S. Yu, K. Park, and Y. Park, "A secure lightweight three-factor authentication scheme for IoT in cloud computing environment," *Sensors*, vol. 19, no. 16, p. 3598, 2019.
[23] S. Sharma *et al.*, "Secure protocol for 5g enabled iot network," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, 2018: IEEE, pp. 621-626.
[24] H. Lee, D. Kang, J. Ryu authentication, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," *Journal of Information Security and Applications*, vol. 52, p. 102494, 2020.
[25] M. H. A. Venkatesh M Ka, Sukumar Sc, Dr Geetha Rd*, "Dynamic Authentication Key Agreement Scheme for Effective Path Selection in I IoT Systems," *VDGOOD Journal of Computer Science Engineering*, 2020.
[26] G. Li, Y. Wang, B. Zhang, and S. Lu, "Smart Contract-Based Cross-Domain Authentication and Key Agreement System for Heterogeneous Wireless Networks," *Mobile Information Systems*, vol. 2020, 2020.
[27] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107046-107062, 2020.
[28] K. Khalil, K. Elgazzar, A. Abdelgawad, and M. Bayoumi, "A security approach for CoAP-based internet of things resource discovery," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020: IEEE, pp. 1-6.

[29] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," *Future Generation Computer Systems,* vol. 92, pp. 1028-1039, 2019.
[30] K. Pothuganti, "Overview on Application Layer routing Protocols for the Internet of Things," *International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering,* vol. 7, no. 11, 2018.
[31] H. Kitano, "Artificial intelligence to win the nobel prize and beyond: Creating the engine for scientific discovery," *AI magazine,* vol. 37, no. 1, pp. 39-49, 2016.
[32] V. D. Soni, "Prediction of Geniunity of News using advanced Machine Learning and Natural Language processing Algorithms," *International Journal of Innovative Research in Science Engineering and Technology,* vol. 7, no. 5, pp. 6349-6354, 2018.
[33] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials,* vol. 17, no. 4, pp. 2347-2376, 2015.
[34] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," *Transaction on IoT and Cloud computing,* vol. 3, no. 1, pp. 11-17, 2015.
[35] S. Verma and M. A. Rastogi, "IOT Application Layer Protocols: A Survey," *Journal of Xi'an University of Architecture & Technology,* vol. XII, no. VIII, 2020.
[36] F. A. Alhaidari and E. J. Alqahtani, "Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey," *Journal of Communications,* vol. 15, no. 1, 2020.
[37] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2012.
[38] J. Vishwesh and M. Rajashekar, "Internet of Things (IoT): Security analysis & security protocol CoAP," *International Journal of Recent Trends in Engineering and Research,* vol. 3, no. 3, pp. 417-425, 2017.
[39] M. Zolanvari and R. Jain, "IoT security: a survey," in *Recent Advances in Networking (Data Center Virtualization, SDN, Big Data, Internet of Things)*: Nova Sci, 2015, pp. 1-15.
[40] T. A. Alghamdi, A. Lasebae, and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," in *Second International Conference on Future Generation Communication Technologies (FGCT 2013),* 2013: IEEE, pp. 163-168.
[41] M. Gunnarsson, J. Brorsson, F. Palombini, L. Seitz, and M. Tiloca, "Evaluating the Performance of the OSCORE Security Protocol in Constrained IoT Environments," *Internet of Things,* p. 100333, 2020.
[42] M. M. A. Ebtesam H Alharbi, "BIOMETRIC AUTHENTICATION SYSTEMS TOWARDS SECURE AND PRIVACY IDENTIFICATION: A REVIEW," *Electronic Interdisciplinary Miscellaneous Journal (EIMJ)* no. 23 4/2020, 2020.
[43] A. Team, "HLPSL Tutorial: A Beginner's Guide to Modelling and Analysing Internet Security Protocols, 2006," ed.
[44] R. A. Abouhogail, "A Comparative Analysis of Tools for Testing the Security Protocols," 2019.
[45] T. Genet, "A short span+ avispa tutorial," IRISA, 2015.