Wajid et al. LGURJCSIT 2024

LGU Research Journal of Computer Science & IT

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

doi: 10.54692/lgurjcsit.2024.081484

Vol (8): Issue (1), January – March 2024

Guardians of the iot realm: a comparative analysis of cryptographic security solutions for bolstering IoT device networks

Sana Wajid[1], Zafar Iqbal[2*]
Deptartment of Cyber Security Air University, Islamabad, Pakistan.

Email: zafar.iqbal@mail.au.edu.pk

ABSTRACT:

The "Internet of Things" (IoT) is an emerging technology that allows electronic devices and sensors to connect over the Internet. The IoT is a network of smart devices, such as sensors, that are connected through cables or wirelessly. Today, IoT devices are commonly used in medical science, industrial automation, and smart home automation, among other applications. Easy accessibility and the open-source environment of IoT devices are major threats to privacy and security. In this research, we briefly discuss areas of IoT, including architecture and details of IoT layers concerning security algorithms, protocols, attacks, and their mitigation. The primary purpose of this research is to provide an efficient and cryptographically proven algorithm scheme with appropriate hardware to improve IoT device network security. This research enhances the network security of IoT devices by presenting a key agreement protocol (ECDSA) with data integrity and a unique key in every session instead of a fixed key or password for authentication of devices with centrally controlled device/server (CCD/S) and data encryption supported by the finest hardware options. After evaluating several cryptographic algorithms and hardware options, the proposed solution is more secure by using separate key pairs for authentication and a unique shared secret for each message between IoT devices and CCD/S. This research is an important step towards ensuring the integrity and security of IoT devices in a networked environment, with the primary goal of increasing the protection of sensitive data and interactions.

KEYWORDS: IoT, Network Security, Encryption, Cyber Attacks, Architecture.

1. INTRODUCTION

According to the ”State of IoT—Spring 2023” report [1], there were 14.3 billion active IoT endpoints worldwide in 2022, a rise of 18% in the number of IoT connections. Based on IoT Analytics, there is 16.7 billion active endpoints globally in 2023, a further 16% increase in connected IoT devices. IoT is evolving into a crucial, globally detectable aspect of human lives. Nowadays, IoT develops a new platform for smart devices, systems, and sensors. The IoT creates standards to improve communication between electrical equipment and sensors [2]. IoT offers a wide range of uses [3]. A central IoT device connected to the internet allows all this communication. The availability of many different manufacturers, affordable sensors, and wireless communication technologies that can exchange relevant information and transfer it to a centralized system has recently increased the number of IoT devices. The IoT includes many devices, including laptops, tablets, smartphones, personal digital assistants (PDAs), and other hand-held embedded devices. The IoT devices' fundamental purpose is to build a better society for people in the future, where anything can be accessed from anywhere. The accepted format of IoT architecture is a three-layer architecture consisting of the Physical, Network, and Application layers. Physical Layers consist of sensors, actuators, and IoT devices like NFC and RFID tags. The main task is to collect information

and prepossessing for the network layer. Network Layers mainly communicate with all sensors and actuators from the field through network switches, routers, and servers. The Application Layer is the front-end layer for a user interacting with different IoT services, like a mobile app with a button to unlock the door or turn on AC, light fans, etc. With extensive research and development in IoT, the architecture has been expanding. For example, the network layer and application layer are expanded into sublayers. The network layer is split into middleware and the network layer. A middleware layer exists between IoT devices and applications to handle compatibility problems. Different network companies like Cisco, Huawei, and Oracle offer IoT middleware with the network layer. The Application layer is also extended into application and business layers. The business layer performs data analysis and builds a business model to manage the IoT system.

According to HP research, the Open Web Application Security Project (OWASP) demonstrates how manufacturers disregard security considerations when creating these devices [4]. So, IoT devices are more vulnerable to cyber safety and have become potentially vulnerable targets for cybercriminals. Hence, multiple layer-wise security challenges and attacks exist in IoT infrastructure. Physical layer attacks include unauthorized access, side-channel attacks, replay attacks, false data injection, and eavesdropping. In contrast, the network layer attack includes spoofing, Man in the Middle attack (MitM), Sinkhole attacks, Denial Of Service (DOS) attacks, and unauthorized access. The application layer attacks include phishing attacks, authentication, malicious scripts, and policy enforcement weaknesses. Some solutions proposed against these attacks include introducing Blockchain as a decentralized technology to avoid a single point of failure and provide security and privacy against some issues. This article provides an in-depth study of the IoT ecosystem, including architectural intricacies, numerous layers, security techniques, protocols, and vulnerabilities. A revised solution using efficient key agreement protocol and unique session key against each transmission between the IoT devices and CCD/S to avoid fixed passwords and the same key for every transmission may lead to a potential attack in the IoT network. The proposed solution enhanced the IoT infrastructure after assessing a variety of cryptographic algorithms and hardware alternatives. Notably, this research recommends a at all levels of the IoT ecosystem. With the primary goal of improving the security of sensitive data and interactions, this study represents a critical step toward maintaining the integrity and security of IoT devices in an increasingly linked world. The rest of the paper is organized as follows. Section II discusses the associated work. The proposed framework was then provided in section III. In part IV, we discussed the evaluation of the suggested system. Section V then discussed the advantages and disadvantages of the proposed approach. Finally, in section VI, the conclusion and future work are offered.

2. BACKGROUND

To understand our proposed research, readers need to know IoTs. Therefore, we are sharing brief details about the architecture of the IoT and attacks and threats in the following paragraphs.

2.1. Architecture

To describe the architecture of IoT, there are two protocol base concepts available, as shown in Figure 1: one is three layers, and the second is five-layer architecture.

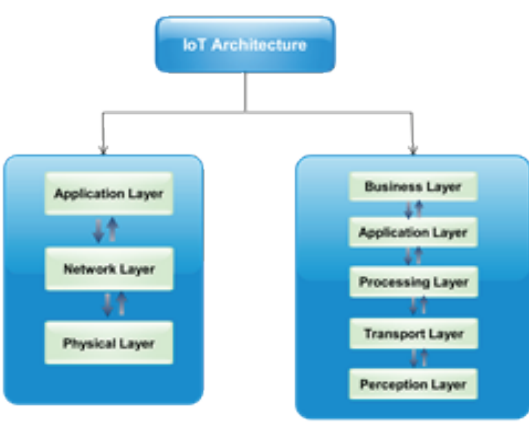

Figure 1: Architecture of IoT, three layers and five layers

Three Layer components are the Perceptions Layer (the physical layer sense physical parameter or identifies object gathering data), Network Layer (responsible for transmitting information and connecting other things), and the Application Layer (Application deliverable like Home automation, Geological positioning identification, etc.). According to functionality and technology, each layer is different from the others, so every layer has its security weakness and concerns. Each IoT

layer differs from the others in terms of the technologies it uses and the functions it performs, so each layer has related security concerns [9].

i) Perception Layer: This layer is responsible to get data, processes it, and then sends it to the network layer. This layer shows IoT devices/equipment cooperation in limited-range networks hence also used to represent the sensor network. Mostly used technologies are Radio Frequency Identification (RFID) technology, positioning system, and sensors [10].

ii) Network Layer: This layer forwards data on various hubs over IoT and the Internet. The important building components of the network layer include Switching, cloud platforms, routers, and gateways. LTE, wireless networks, Bluetooth, and ZigBee, are the most often utilized technologies. By collecting, process, and transferring data between sensors, gateways at this layer serve as the interface between nodes. [10].

iii) Application Layer: At this layer, the IoT's goals are accomplished by giving users access to applications for smart environments. The different applications are smart home, smart city Home automation, Geological positioning identification, etc.

In the following section, we thoroughly analyzed the IoT layers with protocol stack, the cryptographic security aspect of each layer, the requirement of cloud computing in the processing layer, selection of suitable cryptographic algorithms with respect to hardware. Details of the five layer architecture are provided in the following subsections.

i) Physical Layer: This layer is also called the perception layer. It is the first layer that interacts with hardware devices like sensors and actuators. It collects the data via outer equipment and sends it to the next network layer. Moreover, in case of any decision from the top layer, i.e., the business layer, it executes appropriate action, e.g., power on activates relay, etc. The protocol of this layer is 802.15.4, BLE 4.2, WPA2, and WPA with TKIP, which belongs to wifi, blue tooth, and its access rights. The cryptographic algorithms used in this layer are AES for payload encryption. At the same time, the ECCDHE (DH with ephemeral) is used as a key exchange and agreement protocol, which SHA-256 uses as message integrity.

ii) Network Layer : This layer manages the connectivity of physical layer equipment to the network devices and servers. Its functionality is transmitting and processing sensor data. Because of lower power, memory, and processing resources in the physical layer, the normal network protocol, e.g., IPv4 and IPv6 are not suitable; therefore, the 6LoWPAN Working Group, IPv6 in Low-Power Wireless Personal Area Networks, was established by the Internet Engineering Task Force (IETF) to define the IPv6 modifications required for networks using the IEEE 802.15.4 physical and MAC layers. 6LoWPAN is the more suitable network protocol for IoT solutions. As a result of IoT applications, sensor nodes connected to wireless personal area networks can communicate with one another. The top layer application receives real-time data from these sensor nodes. However, 6LoWPAN is still considered a big data layer for IoT solutions. The Internet Engineering Task Force proposed and implemented an adaptation layer to enable the efficient transmission of information in such a constrained network (IETF). This additional layer is positioned between the physical layer and the network layer. The adoption layer basically fragments compresses, and reassembles the 6LoWPAN data in small packets and then replies to the physical layer. In some cases, it also provides routing services. AES-CCM and ECC are also applicable to provide necessary information security.

3) Processing Layer: This layer is also called middleware layer. It gets huge quantities of data from the application layer, which it then stores, analyses, and processes. It can administer and provide a wide range of services to the lower layers. It employs a variety of technologies, such as big data processing modules, cloud computing, and databases.

For IoT solutions where cloud services are adopted because of lower processing and memory available in the physical layer, there is a concept to avail fog network for quick processing and mist computation. These services are also providing security mechanisms to ensure the secrecy of data. Cloud computing plays an important role during the IoT era, where IoT devices can be connected through the Internet from anywhere.

Every day these smart devices produce enormous amounts of data. , according to the most recent survey, 20 million users of the IoT health system contribute 2600 tuples of data every second. To Manage this data and take processing not appropriate for the traditional system, so advanced system proposed a Cloud computing design for resolving storage and computational matters. Here the

concept of centralized cloud arises as data is transmitted from different sources as large bandwidth is required; due to this issue, interruption in the computational process occurred; as a result, high latency rates have been observed. Overcoming this matter means reducing bandwidth and network latency and introducing new technology named Fog and Mist computing to create a direct connection between a cloud server and local storage and limited computational power of equipped. To increase throughput and reduce network latency by using an initial filtering filter on this computing method [11, 12]. High-performance servers that give maximum computation, high storage area with analytic data service, and high connectivity are the main features of Cloud computing. Still, limitations on security, Power consumption, and offline mode still need to be created. Privacy and legal issues exist in cloud computing as raw data move from the Internet to the cloud. While for processing data at ground level or edge level, fog computing is used, which makes the main communication and computation process easy. In fog computing, it mainly decreases network latency and data transmission rate [13] as it is a cost-saving saving solution but relies on multiple links to transport data from the physical to the digital layer. Similarly, for Time-centric applications, Mist computing has been developed. Using Mist computing, pre-processed data comes from the heterogeneous system; as a result, less bandwidth processing time has been observed. Mainly used smart medical care and smart traffic control system where deciding with minimum delay [14]. These computing technologies have a distinct architecture from conventional systems. It provides application-specific services like Serverless Computing, Software as service (SaaS), Platform as a service (PaaS), Function as Service (FbaaS), and Infrastructure as a Service (IaaS), as these services are used as per application requirements [15].

A. Three Layer Architecture

Its components are the Perceptions Layer (the physical layer senses physical parameters or identifies objects gathering data), the Network Layer (responsible for transmitting information and connecting other things), and the Application Layer (Application deliverables like Home automation, Geological positioning identification, etc.). Each layer differs according to functionality and technology, so every layer has security weaknesses and concerns. Each IoT layer differs from the others in terms of its technologies and functions, so each layer has related security concerns [9].

i) Perception Layer: This layer is responsible for getting, processing, and sending data to the network layer. This layer shows IoT devices/equipment cooperation in limited-range networks; hence, it is also used to represent the sensor network. The most commonly used technologies are radio frequency identification (RFID) technology, positioning systems, and sensors [10].

ii) Network Layer: This layer forwards data on various hubs over IoT and the Internet. The important building components of the network layer include Switching, cloud platforms, routers, and gateways. LTE, wireless networks, Bluetooth, and ZigBee are the most often utilized technologies. By collecting, process, and transferring data between sensors, gateways at this layer serve as the interface between nodes. [10].

iii) Application Layer: At this layer, the IoT's goals are accomplished by giving users access to applications for smart environments. The different applications are smart home, smart city Home automation, Geological positioning identification, etc. In the following section, we thoroughly analyzed the IoT layers with protocol stack, each layer's cryptographic security aspect, the cloud computing requirement in the processing layer, and the selection of suitable cryptographic algorithms concerning hardware.

B. Five Layer Architecture

Details of the five-layer architecture are provided in the following subsections.

i) Physical Layer: This layer is also called the perception layer. The first layer interacts with hardware devices like sensors and actuators. It collects the data via outer equipment and sends it to the next network layer. Moreover, in case of any decision from the top layer, i.e., the business layer, it executes appropriate action, e.g., power on activates relay, etc. The protocol of this layer is 802.15.4, BLE 4.2, WPA2, and WPA with TKIP, which belongs to Wi-Fi, Blue Tooth, and its access rights. The cryptographic algorithms used in this layer are AES for payload encryption. At the same time, the ECCDHE (DH with ephemeral) is used as a key exchange and agreement protocol, which SHA-256 uses as message integrity.

ii) Network Layer: This layer manages the connectivity of physical layer equipment to the network

devices and servers. Its functionality is transmitting and processing sensor data. Because of lower power, memory, and processing resources in the physical layer, the normal network protocols, e.g., IPv4 and IPv6, are not suitable; therefore, the 6LoWPAN Working Group, IPv6 in Low-Power Wireless Personal Area Networks, was established by the Internet Engineering Task Force (IETF) to define the IPv6 modifications required for networks using the IEEE 802.15.4 physical and MAC layers. 6LoWPAN is the more suitable network protocol for IoT solutions. As a result of IoT applications, sensor nodes connected to wireless personal area networks can communicate with one another. The top layer application receives real-time data from these sensor nodes. However, 6LoWPAN is still considered a big data layer for IoT solutions. The Internet Engineering Task Force proposed and implemented an adaptation layer to enable the efficient transmission of information in such a constrained network (IETF). This additional layer is positioned between the physical layer and the network layer. The adoption layer fragments, compresses and reassembles the 6LoWPAN data in small packets and then replies to the physical layer. In some cases, it also provides routing services. AES-CCM and ECC are also applicable to provide necessary information security.

iii) Processing Layer: This layer is also called the middleware layer. It gets huge amounts of data from the application layer, which stores, analyses, and processes. It can administer and provide a wide range of services to the lower layers. It employs various technologies, such as big data processing modules, cloud computing, and databases. For IoT solutions where cloud services are adopted because of lower processing and memory available in the physical layer, there is a concept to avail fog network for quick processing and mist computation. These services are also providing security mechanisms to ensure the secrecy of data. Cloud computing plays an important role in the IoT era, where IoT devices can be connected through the Internet anywhere. Every day, these smart devices produce enormous amounts of data. , according to the most recent survey, 20 million users of the IoT health system contribute 2600 tuples of data every second. To manage this data and take processing inappropriate for the traditional system, an advanced system proposed a cloud computing design for resolving storage and computational matters. Here, the concept of a centralized cloud arises as data is transmitted from different sources as large bandwidth is required; due to this issue, interruption in the computational process occurs; as a result, high latency rates are observed. Overcoming this matter means reducing bandwidth and network latency and introducing new technology named Fog and Mist computing to create a direct connection between a cloud server and local storage and limit the computational power of the equipped. To increase throughput and reduce network latency by using an initial filtering filter on this computing method [11] [12]. High-performance servers that give maximum computation, high storage area with analytic data service, and high connectivity are the main features of Cloud computing. Still, limitations on security, Power consumption, and offline mode need to be created. Privacy and legal issues exist in cloud computing as raw data moves from the Internet to the cloud. Fog computing is used for processing data at ground or edge levels, making the main communication and computation process easy. Fog computing mainly decreases network latency and data transmission rate [13]. It is a cost-saving solution but relies on multiple links to transport data from the physical to the digital layer. Similarly, for Time-centric applications, Mist computing has been developed. Using Mist computing, pre-processed data comes from the heterogeneous system; as a result, less bandwidth processing time has been observed. Mainly used smart medical care and smart traffic control systems, deciding with minimum delay [14]. These computing technologies have a distinct architecture from conventional systems. It provides application-specific services like Serverless Computing, Software as service (SaaS), Platform as a service (PaaS), Function as Service (FbaaS), and Infrastructure as a Service (IaaS), as these services are used as per application requirements [15]. In this paper, the author proposed a modified ECDSA method to mitigate the attack on random private integers used in the ECDSA signature. The author used Shamir's Secret Sharing (SSS) containing reconstruct participant is 2, i.e., first is its central server, and the second is the IoT device. During the registration process of IoT devices with the central server, the central server generates another integer, processes this number using SSS, and saves the device part into the IoT device, which will be used during the verification process[16]. The writer proposed the ECDSA against the direct storage of private keys in IoT devices [17]. The valid signature can be

generated without the whole private key. The author claimed that this single key pair of ECDSA can be effectively used in the IoT Fog environment (the environment uses limited power and time). Instead of employing the conventional signature-based authentication process, the author introduces a hash-based authentication scheme for IoT devices in this paper, which is incorporated into the 5G authentication framework[19]. In this paper, the author proposed a remote authentication method against the tampered IoT device hardware or detection of firmware alteration of the IoT device [20]. They use Root of Trust for Measuring and Reporting (RoTMR) by using a physical unclonable function (PUB) and hash-based signature to confirm ROM data [21].

i) Application Layer: It is the first interactive layer concerning the end user. This layer consists of services like analysis and reporting of data coming and provides device access to the end user. This layer may also comprise any industrial technologies required by the user. In the application layer, protocols such as Constrained Application Protocol (COAP), MQ Telemetry Transport (MQTT), and Advanced Message Queuing Protocol (AMQP) are utilized. The main characteristic of these protocols is they can execute at low bandwidth and low availability with machine-to-machine (M2M) interaction and usually run over TCP/IP. From a security point of view, payload encryption algorithms, e.g., AES and key agreement ECC, are used as per the requirement.

Table 1: Iot layer-wise cipher mechanism

Encrypt (Mechanism)	Layer	Protocol	Technology
AES (CCM, CTR, CBC-MAC) [22]	Physical	802.15.4	
AES [23],[24], ECC/ECDH [23]	Physical	BLE 4.2	
AES [23],[25]	Physical (Link Layer)	WPA2	802.11
RC4 [23],[25]	Physical (Link Layer)	WPA2 with TKIP	802.11
KASUMI [23]			GSM, UMTS, GPRS, ISO/ IEC 29192
CLEFIA [26],[27]			
AES-CCM [28]	Network	RPL	
AES,DES [23]	Network	IPSec, IPv6	
ECC [24],[29]	Network	6LoWPAN	
AES [7]	Adoption	6LoWPSec	
AES [30],[31], ECC [23]	Application	CoAP	

ii) Business Layer: An IoT solution's business layer is its last layer. It collects data from the application and creates a business model, such as a flowchart and graph. It provides a decision-making environment for high-end-user management by using big data analysis. Determining future activities and corporate strategy is the goal of the business layer. Any office application suit may generate a graph or flow chart in this, and there isn't any essential requirement for the cryptographic algorithm.

2.2. Attacks and Threats

IoTs attacks & threats are as follows:

- ***DOS/DDoS***

In a network layer assault known as a denial of service, the attacker tries to overwhelm a server with as much traffic as possible. At the same time, the victim cannot utilize its resources.

- ***Spoofing***

In this attack, the attacker tries to control the smart device by gaining access and behave a legitimate user to transmit a fake message to the network.

- ***Man-in-the middle attack***

It can be either active or passive, with the attacker trying to sniff data while being passive or creating a pattern to which the victim will be exposed.

- ***Network Injection (SQL Injection)***

As IoT devices record and store various data in the database, attackers inject malicious code to down the SQL server.

- ***Flooding Attack***

Flooding attack belongs to the communication layer in which the attacker harness power of this device results in extra damage.

- Sinkhole Attack

The attacker reroutes the message as it travels via several paths in this routing assault.

- ***Unauthorized Access***

It is also called Impersonation Attack. In this assault, attacker gets the authorized credential to access the network in this attack.

- ***Routing Attack***

The attacker introduces an intermediate malicious node for data forwarding and collection perspective (WSN, RSN).

3. LITERATURE REVIEW

This research summarizes the relevant areas after clustering them into three categories:y, the application of IoT, threats and attacks, and IoT security and privacy. Details are provided in the following subsections.

3.1. Applications

Building a smart city has become attractive within the last decade [5]. The smart home business economy has crossed 100B dollars [6]. It benefits the house owner and the living member of the allocated house by reducing costs belonging to various sides, for example, lower electricity bills gained by lower energy consumption. In [8], the authors analyzed the problem of urbanization in cities. People moved from non-developed to modern, resulting in increasing growth of the cities. That's why offering IoT-based intelligent solutions for the movement, energy, medical, and framework is essential. IoT developers provide important application areas solutions for it: Smart city. It learns about various things, including smart parking, smart lighting, smart garbage collection, smart public safety solutions, and smart traffic and air quality management.

3.2. Attacks

IoT devices, services, and communication protocols face multiple security challenges, attacks & threats. Attacks can be categorized concerning the physical level, network level, transport, and application layers. Known and discovered network communication layer [32] [33]. In the network layer, the DOS/DDOS attack invader interferes with two parties' already-established contact by resynchronizing (in an endless cycle) their communication. It disrupts communication and drains network resources. The Contiki Operating System (OS) rate-limiting model shows well-organized recognition of UDP Flood attacks [34]. Software Defined Networking (SDN) initially used detection modules for flooding attacks, but some restrictions make practical testing inappropriate [35]. A severe threat to privacy arises when an intrusive party learns user information and can identify the message ID, timestamps, source, and destination addresses. Visible Light Communication (VLC) presents a viable solution for eliminating eavesdropping on IoT devices using channel correlation and error estimations [36]. In an IoT setting, IDS is used to identify wormhole attacks, while selective forwarding is used as a similar mitigation strategy for grey holes, sinkholes, and black holes [31] [38].

Research on known attacks for IoT devices and proposed solutions show that standard AES encryption algorithms are used to overcome eavesdropping and sniff attacks (with proper integration and confidentiality) [39] [40] with certificate-based EECDH key exchange protocol. Similarly, identify-based authentication protocols can be used to avoid spoofing and cloning attacks. To overcome Interruption, only authorized users are allowed to access selected information. MEC shield (consisting of a central controller and multiple agents located at each node) and heterogeneous IoT systems were also proposed to avoid DDOS attacks [41]. Blockchain cryptography has also been introduced to overcome the key exchange process's complexity and the certificate's requirement.

3.3. IoT Security and Privacy

IoT devices and their applications are often connected to someone's daily experience or industry. Therefore, all of these systems need to handle security and privacy challenges. Along with user authentication, the network layer should have a built-in solution of access control to handle these problems. It is more challenging to safeguard these devices because of the open design of IoT, which creates a more significant number of security concerns. Mobility, connectivity, embedded use, diversity, and size are the IoT characteristics that may cause security and privacy concerns [42]. To implement security, a well-known model for advancing security apparatuses, namely CIA Triad, uses three key areas, i.e., data confidentiality, integrity, and availability, as illustrated in Figure 2.

Figure 2: CIA Triad

Data confidentiality assures the privacy of sensitive data using a variety of procedures so that

disclosure to unauthorized parties is forbidden and that only authorized users can access it. Access control and data encryption are standard technologies used to maintain data secrecy. At the same time, data integrity refers to protecting sensitive information from outsiders during data transport or storage using widely used procedures such as hash algorithms, namely SHA-256. Data availability confirms that certified parties have timely access to their information resources in normal and unusual conditions. DoS attacks on services may deny data availability. Firewalls, IDS, and redundancy techniques are some availability protection strategies. Identity management, authentication, authorization, key exchange and management, trust, and reputation are the five functional bases of IoT security [40]. Figure 3 shows the main focus area for IoT security research. Along with confidentiality, integrity, and availability, it also includes authentication, access control, and non-repudiation. These goals can all be achieved by utilizing cryptographic primitives. One of the biggest hurdles to IoT is the requirement for standards to be developed for devices with limited resources and heterogeneous technology. As a result, these devices introduce multiple vulnerabilities that act as an ideal environment for cyber threats [43]. IoT in our daily lives, particularly in sensitive industrial applications directly connected to a person's life, such as smart homes, makes them min targets that seem enticing for cyberattacks. Even though the bulk of these dangers are not new, their use in a home environment raises second-order issues for residents' physical and mental health [44]. Strong security guarantees will be needed for many IoT applications that process and transmit sensitive data across wireless connections. As a result, standard yet adaptable security procedures for the IoT should be developed and implemented. Standardization makes it possible for security solutions to be adopted widely.

In contrast, flexibility allows security techniques to be swiftly adjusted to various sensing devices and applications [45]. Most attacks target communication protocols [45], which directly communicate collected device data to storage hardware and processing tools rather than actuators or devices. MitM or DoS attacks are likely to disrupt this transmission. Inadequate communication protocols in an incomplete database can lead to battery-draining devise denial or denial-of-sleep attacks [46]. Moreover, routing protocols are the primary cause of many threats [47]. These attacks include spoofing, changing routing pathways or replaying packets, sinkholes, warm-holes, and other techniques [48]. Nowadays, machine learning merges new solutions for the IoT. Some of the networks used for IoT are as follows.

i) Heterogeneity: Devices use different communication protocols with varying features and capabilities. Uses a variety of hardware resource concepts.

ii) Massive scale deployment: IoT devices on a large scale face challenges: storage capacity, the effectiveness of data communication protocols, and protection from malicious attacks.

iii) Inter-connectivity: IoT devices in smart homes, local or global, cause connectivity of critical infrastructure. Due to computational limitations, IoT devices may need a new breed of optimized cryptographic and other algorithms to deal with security and privacy. At the network, attacks attempt routing to spoof and lunch man in the middle.

iv) Blockchain: This technology can solve scalability, reliability, and privacy issues in IoT.

v) Processing transactions: Records the interaction so it is safe, auditable, transparent, efficient, and interruption-resistant.

vi) Data Tracking: Shared customer information is tracked throughout to give a smooth experience and remain private. By using data storage encryption, every part of information relies on data.

3. PROPOSED SECURITY DESIGN

A robust network layer security mechanism is required during the literature review to ensure maximum protection against cyberattacks. Therefore, security methods should have multiple layers to create optimal management against the attacks. Accordingly, the proposed solution consists of more than one key and an initial personalization procedure to bind the IoT devices with a centrally controlled device/server (CCD/S). In this paper, two layers of cryptographic algorithms are used. Efficient ECDSA-256 is proposed for authentication of IoT devices with signature /verification key pair. In contrast, a separate encryption/decryption key pair is used to share unique keys for data encryption & decryption. These different ECDSA key pairs made the IoT network more robust against attacks and securely transferred the session key for payload encryption.

3.1. Cryptography algorithms and its keys

According to the current cyber security scenario, it is recommended that security solutions should have more than one cryptographic algorithm, i.e., symmetric encryption/decryption algorithm, public key signature and verification algorithm, and key agreement protocols with data integrity methods. For these algorithms, the proposed solution has AES-256 as a systemic key algorithm for actual data encryption & decryption while the ECC-based signature and key agreement protocols, e.g., ECDSA. For Data integrity, SHA-256 is considered a suitable message digest algorithm. Instead of using a single key between IoT devices with CCD/S, key agreement and signature/verification have two separate randomly generated key pairs on both equipment, i.e., device and CCD/S. To recall, private keys of both equipment shouldn't be retrieved from devices. However, both equipment can share their public keys (verification and encryption key of key agreement). A randomly generated real-time key will be used as an AES-256 key for data secrecy.

3.2. Proposed Solution Block Diagram

The block of the proposed solution is shown in Figure 4. It has three modules: Registration, Authentication, and Data transmission. Details of these modules are provided in the following subsections.

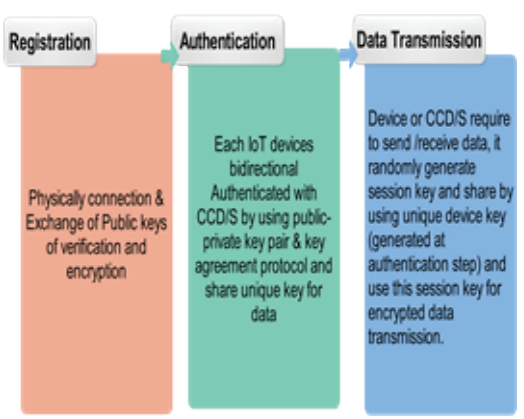

Figure 3: Flow Diagram

- ***Registration***

Each IoT device should be personalized or registered with a centrally controlled device/server (CCD/S) in this step. This step will ensure that no other IoT device can connect with CCD/S. Both devices will share their public keys in this stage via the physical connection of the IoT device with CCD/S. After this step, the IoT device can be placed in its desired location, and it can be remote.

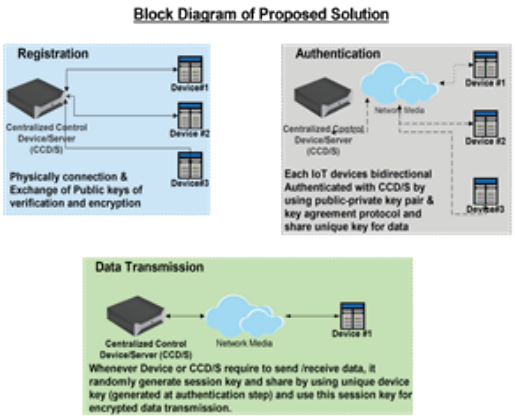

Figure 4: Proposed Solution

- ***Authentication***

CCD/S may have a wrong attempt blockage procedure. It means that the authentication procedure will allow some specific number of authentication attempts; otherwise, the remote IoT device may be blocked by CCD/S. In this step, IoT devices (maybe on the remote end) will authenticate with CCD/S using ECDSA and share a unique key for the rest of the operation.

- ***Data transmission***

After the successful authentication, IoT devices can send and receive data from CCD/S using the AES-256 encryption /decryption algorithm. To make each session unique, the device can randomly generate its session key and share it with CCD/S via the unique key shared in the authentication step and challenged & response method.

4. EVALUATION

The comparative evaluation of the proposed solution is shown in the following subsections.

4.1. Selection of Hardware

Certain IoT Wi-Fi-based devices are on the market for smart solutions, like ESP8266 and ESP32. Both Espressif modules are ideally suited to low-cost IoT applications, but ESP32 is the better of the ESP8266; ESP32 contains all the features of the ESP8266, including a faster CPU core, wifi module, and more GPIOs, with Bluetooth.

i) ESP8266 Processor: The ESP8266 is a custom 32-bit processor clocked at 80MHz. It has 32KB

of instruction space and 80KB of user data. Furthermore, it has 16 GPIO pins for various peripherals such as a serial peripheral interface (SPI), inter-integrated circuit protocol (I2C), universal asynchronous receiver-transmitter (UART), and an analog-to-digital converter (ADC).

ii) ESP32 Processor: The ESP32 is used in different IoT applications, also known as low-cost, low-power systems on chip microcontrollers integrated with wifi and Bluetooth. Data security, authenticity, and integrity are mainly considered to make IoT applications correct, on point, and interception. As per the given, Esp32 is hardware acceleration that helps low-power devices run heavy encryption algorithms faster. Due to faster execution, power consumption will be less, which is better for IoT applications with limited energy.

The ESP32 board is programmed with source code to carry out various project processes. It has on-chip storage for its source code. This block serves as a link between the coder and the user. The operating voltage range of the ESP32 is 2.2V to 3.6V. In normal mode, the ESP32 device supplies 3.3V to the chip. Figure 5 shows the ESP32 pin description.

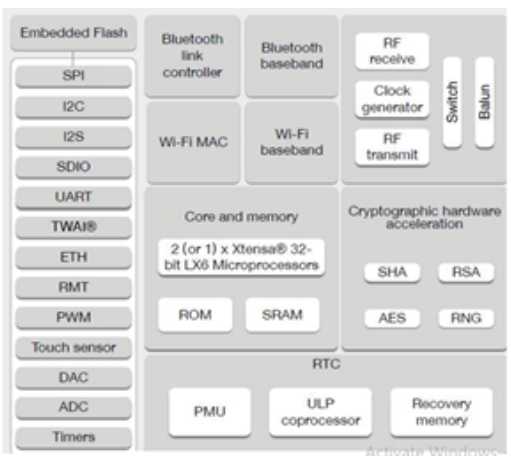

Figure 5: ESP32 SoC

As IoT equipment or sub-equipment doesn't have a large memory area and computational power, selecting cryptographic algorithms requires the full attention of IoT solution designers and providers. There are three cryptographic algorithm categories available which are Lightweight cryptographic algorithms (CLEFIA, AES, RC5), Low-cost cryptographic algorithms (Midori, Trivium, WG-8, Espresso, Lizard, ECC, Ultra-lightweight cryptographic algorithms (QTL, HUMMINGBIRD, Piccolo, Sprout, Fruitv2, KATAN, KATANTAN). However, for proven security, the standard is still AES. At the same time, the SHA-256 is also considered a safe data integrity algorithm. There is comprehensive research on RSA vs. ECC for security strength, memory utilization, and throughput for the key exchange or agreement protocol, as seen in Table 2. We consider ECC to be the most suitable algorithm for our proposed solution.

Table 2: Rsa and ecdsa key size with security level

S.no	Security Level	RSA Key Size	ECDSA Key Size	ESP-IDF Curves
1	80	1024 bits	160-223 bits	Secp192r1, secp192k1
2	112	2048 bits	224-255 bits	Secpr224r1, secp224k1
3	128	3072 bits	256-383 bits	Secp256r1, Secp256k1
4	192	7680 bits	384-511 bits	Secp384r1, Secp384k1
5	256	15360 bits	512+ bits	Secp521r1

To implement our proposed solution, first of all, describe the background and concept of encryption techniques already proposed.

4.2. Advanced Encryption Algorithm (AES)

The Data Encryption Standard (DES) encryption protocol has been exploited and is known to be vulnerable to brute force attacks. As a result, Belgian cryptographers Daemen and Rijmen designed the AES algorithm to replace the DES. It is a cyclic algorithm. It first packs data into fixed-size blocks based on the encryption key size and then performs various operations on each data block with a fixed number of iterations, as shown in Table 2. It has different key sizes, namely 128, 192, and 256 bits, and accordingly performs 10, 12, or 14 operations, as seen in Table 3.

Table 3: Aes key length and number of rounds

Encryption Algorithm	Key Length (bits)	Block Size (bits)	Number of Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

4.3. SHA-2

Secure Hash Algorithm 256 is a set of designed cryptographic hash functions by NIST, published in 2001 round algorithm having single-block and multi-block operations. It is still considered a proven message digest and data integrity algorithm after introducing multiple attacks (high order differential, collision, and Meet-in-the-middle). It can be seen from Tables 4 and 5 that ESP32 outperformed the ESP8266 in all three operations: Set key, Encryption, and Decryption.

Table 4: Aes comparison between esp32 and esp8266

S. no	Operation	Algorithm	ESP32	ESP8266
1	Set Key	AES-128-ECB	0.52us	35.03us
		AES-192-ECB	0.54us	33.69us
		AES-256-ECB	0.572us	44.36us
2	Encryption	AES-128-ECB	0.38us	6.41us
		AES-192-ECB	0.39us	7.69us
		AES-256-ECB	0.41us	8.98us
3	Decryption	AES-128-ECB	0.38us	9.16us
		AES-192-ECB	0.39us	11.05us
		AES-256-ECB	0.41us	12.94us

Table 5
Sha-256 comparison of esp32 and esp8266

S. no	Algorithm	ESP32	ESP826
1	SHA-256 Hashing	0.36us	1.16us
2	SHA-256 Finalizing	23.76us	77.33us
3	SHA-256 HMAC Reset	24.99us	80.32us
4	SHA-256 HMAC Finalize	74.24us	283.73us

4.4. Elliptic Curve Cryptography

There are two options for Elliptic Curve Cryptography (ECC), i.e., Koblitz and random curves. Koblitz curves are characterized by their non-random construction, allowing for especially efficient computation. This differs from the most commonly used elliptic curves, called Random curves with a pseudo-random structure where a specified algorithm chooses the parameters. Secp256K1 and secp256R1 are the most common curves used in the security solution. The ”k” in sepc256k1 stands for Koblitz, and the ”r” in sepc256r1 stands for random. The Secp256k1 is a pure Standard for Efficient Cryptography Group (SECG) curve, while secp256r1 is a so-called National Institute of Standards and Technology (NIST) curve. NIST curves are more widely used and scrutinized than other SECG curves. Both elliptic curves are of the form:

$$y\,2 = x\,3 + ax + b. \qquad (1)$$

Where:
For Koblitz curve: a=0, b=7.
For Random curve:

a= FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC
b= 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B.

The throughput graph of the ECC and RSA implementation is shown in Figure 6. It can be identified from the graph that the throughput of the RSA is better than the RSA.

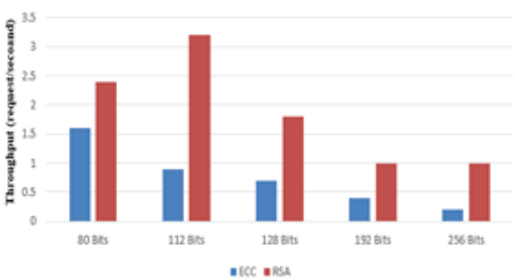

Figure 6: ESP32 ECC/RSA Implementation

5. PROPOSED SOLUTION - PROS AND CONS

The proposed solution has multiple advantages, such as each IoT device physically connecting to load initial security parameters rather than having an online connection. It will avoid the connection of any third-party devices. Only authorized devices will connect to the network using authentication, and a unique session key will ensure data security. The main disadvantage of the proposed solution is that it will have initial personalization processes before the transmission of IoT data to/from CCD/S. Generally, these steps are considered overhead and power consumption compared

to other solutions.

6. CONCLUSION and FUTURE WORK

This research concludes that ECC is a better alternative to RSA for IoT deployments at any layer because it consumes less energy and has better throughput. AES256 and SHA256 are considered proven security for data encryption algorithms and message integrity. So the chosen algorithm suite is ECDHE-ECDSA-AES256-CBC-SHA256, where ECDHE (Elliptic-curve Diffie–Hellman Ephemeral) is for key agreement, and ECDSA (Elliptic-curve Digital Signature algorithm) is for certificate exchange. The analysis of hardware selection in ESP boards showed that ESP32 is better than the ESP8266 because of its dual-core processor with DMIPS/Dual 160MHz speed. Moreover, network-based IoT devices have become very useful due to their small size and low power, and most solution providers are transforming their services using them. Security of these network devices also becomes essential. The proposed solution will provide data security at every layer; in the future, real-world implementation tests of the proposed solution on various IoT devices and platforms will be carried out to validate its effectiveness in diverse environments.

REFERENCES

[1] "State of IoT 2023: Number of connected IoT devices growing 1616.7 billion globally — iot-analytics.com," https://iot-analytics.com/numberconnected-iot-devices/, [Accessed 12-08-2023].

[2] P. Karuppusamy, "A sensor based iot monitoring system for electrical devices using blynk framework," *Journal of Electronics and Informatics*, vol. 2, no. 3, pp. 182–187, 2020.

[3] "Iot In our daily life - Bing — bing.com," https://www.bing.com/search?q=Iot+In+our+daily+life, [Accessed 12-08-2023].

[4] C. Kolias et al., "Securely making" things" right," *Computer*, vol. 48, no. 9, pp. 84–88, 2015.

[5] A. Zanella et al., "Internet of things for smart cities," *IEEE Internet of Things journal,* vol. 1, no. 1, pp. 22–32, 2014.

[6] I. Khajenasiri et al., "A review on internet of things solutions for intelligent energy control in buildings for smart city applications," *Energy Procedia*, 111, pp. 770–779, 2017.

[7] S. Kumar, et al., "Internet of things is a revolutionary approach for future technology enhancement: a review," *Journal of Big data*, 6(1), pp. 1–21, 2019.

[8] A. H. Alavi et al., "Internet of thingsenabled smart cities: State-of-the-art and future trends," *Measurement,* 129, pp. 589–606, 2018.

[9] A. Assiri and H. Almagwashi, "Iot security and privacy issues," *in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). IEEE*, pp. 1–5, 2018.

[10] L. Atzori et al., "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer networks,* 56(16), pp. 3594–3608, 2012.

[11] N. Poursafar et al., "Long-range wireless technologies for iot applications: A review," in *2017 Eleventh International Conference on Sensing Technology (ICST). IEEE*, pp. 1–6, 2017.

[12] M. Chen et al., "On the computation offloading at ad hoc cloudlet: architecture and service modes," *IEEE Communications Magazine,* 53(6), pp. 18–24, 2015.

[13] S. K. Datta et al., "Integrating ¨ connected vehicles in internet of things ecosystems: Challenges and solutions," in *2016 IEEE 17th international symposium on a world of wireless, mobile and multimedia networks (WoWMoM). IEEE,* pp. 1–6, 2016.

[14] M. K. Yogi et al., "Mist computing: Principles, trends and future direction," *arXiv preprint arXiv*:1709.06927, 2017.

[15] S. Ketu and P. K. Mishra, "Cloud, fog and mist computing in iot: an indication of emerging opportunities," I*ETE Technical Review,* 39(3), pp. 713–724, 2022.

[16] M. S. Oudah and A. T. Maolood,"Lightweight Authentication Model for IoT

Environments Based on Enhanced Elliptic Curve Digital Signature and Shamir Secret Share," *International Journal of Intelligent Engineering & Systems* 15(5), 2022.

[17] M. A. Shaaban, "Efficient ECC-based authentication scheme for FOG-BASED IoT environment," in *International Journal of Computer Networks & Communications (IJCNC),* 15(4), July 2023.

[18] J. Clark, F. Ali, "Analysis of ECDSA's Computational Impact on IoT Network Performance," in *ACMSE 2023: Proceedings of the 2023 ACM Southeast Conference,* pp. 196-200, April 2023.

[19] H. A. N. Songshen and X. U. Kaiyong, "Hash-Based Signature for Flexibility Authentication of IoT Devices," in *Wuhan University Journal of natural science*, 27, 2022.

[20] J. J. Puthiyidam and S. Joseph, "Enhanced authentication security for IoT client nodes through T-ECDSA integrated into MQTT broker," in *Journal of Supercomputing*, (Pub Date:01-December-2023).

[21] R. Román and R. Arjona, "A lightweight remote attestation using PUFs and hash-based Signatures for low-end IoT devices," in *Future Generation Computer Systems,* 148, pp. 425-435, November 2023.

[22] J. Granjal et al., "Security in the integration of low-power wireless sensor networks with the internet: A survey," *Ad Hoc Networks*, 24, pp. 264–287, 2015.

[23] M. Frustaci et al., "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of things journal*, 5(4), pp. 2483–2495, 2017.

[24] S.Chakrabarty and D. W. Engels, "Black networks for bluetooth low energy," in *2016 IEEE International Conference on Consumer Electronics (ICCE). IEEE,* pp. 11–14, 2016,.

[25] A. H. Adnan et al, "A comparative study of wlan security protocols: Wpa, wpa2," in 2015 International Conference on Advances in Electrical Engineering (ICAEE). IEEE, pp. 165–169, 2015.

[26] G. Hatzivasilis et al., "A review of lightweight block ciphers," *Journal of cryptographic Engineering*, 8, pp. 141–184, 2018.

[27] T. Shirai et al., "The 128- bit blockcipher clefia," in *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg*, *March 26-28, 2007, Revised Selected Papers 14. Springer*, pp. 181–195, 2007.

[28] T. Winter et al, "Rpl: Ipv6 routing protocol for low-power and lossy networks," Tech. Rep., 2012.

[29] S. Blake-Wilson et al., "Elliptic curve cryptography (ecc) cipher suites for transport layer security (tls)," T*ech. Rep.,* 2006.

[30] E. Rescorla, "The transport layer security (tls) protocol version 1.3," Tech. Rep., 2018.
[31] D. McGrew and D. Bailey, "Aes-ccm cipher suites for transport layer security (tls)," *Tech. Rep.,* 2012.

[32] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the internet of things (iot): A security taxonomy for iot," 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). IEEE*, pp. 163– 168, 2018.

[33] H. Ning et al., "Cyber-physical-social based security architecture for future internet of things," Advances in Internet of Things, 2(1), pp. 1, 2012.

[34] M. Malik, M. Dutta et al., "Contiki-based mitigation of udp flooding attacks in the internet of things," in *2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE*, pp. 1296–1300, 2017.

[35] A. Wani and S. Revathi, "Analyzing threats of iot networks using sdn based intrusion detection system (sdiot-ids)," in S*mart and Innovative Trends in Next Generation Computing Technologies: Third International Conference, NGCT 2017, Dehradun, India, October 30-31, 2017, Revised Selected Papers, Part II 3. Spring-*

er, pp. 536–542, 2018.

[36] X. Liu et al., "Seclight: A new and practical vlc eavesdropping-resilient framework for iot devices," *IEEE Access*, 7, pp. 109–19124, 2019.

[37] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in internet of things," *International Journal of Computer Applications,* 121(9), 2015.

[38] S. Raza et al., "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks,* 11(8), pp. 2661– 2674, 2013.

[39] M. A. Razzaq et al., "Security issues in the internet of things (iot): A comprehensive study," *International Journal of Advanced Computer Science and Applications*, 8(6), 2017.

[40] S. N. Firdous et al., "Modelling and evaluation of malicious attacks against the iot mqtt protocol," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE*, pp. 748–755, 2017.

[41] W. Zhou et al., "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of things Journal*, 6(2), pp. 1606–1616, 2018.

[42] A. Iqbal et al., "Internet of things (iot): On-going security challenges and risks," *International Journal of Computer Science and Information Security,* 14(11), p. 671, 2016.

[43] M. Frustaci et al., "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of things journal,* 5(4), pp. 2483–2495, 2017.

[44] M. Frustaci et al., "Evaluating critical security issues of the iot world: Present and future challenges," IEEE Internet of things journal, 5(4), pp. 2483–2495, 2017.

[45] X. Chen et al., "Sensor network security: A survey," *IEEE Communications surveys & tutorials,* 11(2), pp. 52–73, 2009.

[46] "IoT devices installed base worldwide 2015-2025 — Statista — statista.com," https://www.statista.com/statistics/471264/iot-number-of-connecteddevices-worldwide, (Accessed 12-08-2023).

[47] S. Madakam et al., "Internet of things (iot): A literature review," *Journal of Computer and Communications*, 3(5), p. 164, 2015.

[48] J. Shahid et al., "Cellular automata trust-based energy drainage attack detection and prevention in wireless sensor networks," *Computer Communications*, 191, pp. 360–367, 2022.