Effective Model for CoAP Inspired Trust Aware Scheme in Internet of Things with AES Algorithm

Hira Beenish[*1], Muhammad Fahad[1], Iftikhar Sami[1]
[1]College of Computing & Information Sciences, Karachi Institute of Economics & Technology, Karachi, Pakistan
***Correspondence:** hira@kiet.edu.pk

Citation | Beenish. H, Fahad. M, Sami. I, "Effective Model for CoAP Inspired Trust Aware Scheme in IoT with AES Algorithm", IJIST, Vol. 5 Issue.4, pp 327-338, Oct 2023.
Received| Sep 04, 2023**; Revised|** Sep 21, 2023**; Accepted|** Sep 23, 2023; **Published|** Oct 02, 2023.

IOT networks have been developed in the realm of technology to make connectivity among the things around us. Networks could only connect computer devices before the Internet of Things (IoT) became a reality. Security is the key issue with these devices. There are significant risks of data loss or hacker assault because these gadgets communicate their data via internet. Challenges from the start have accompanied IoT adoption. In this paper, some of the major difficulties on the way to communicate between gadgets are explored. IoT networks protect user privacy with various types of personal data that are made available for these IoT-based connected devices. To protect IoT-based systems, a trust-aware approach utilizing the CoAP and AES algorithms has been proposed in this paper. The AES method has very robust security, shielding the data and architecture in comparison to others. The utilization of AES coupled with CoAP will enhance the efficacy of the system.

CoAP	Constrained Application Protocol
AES	Advanced Encryption Standard
WAN	Wide Area Network
IoT	Internet of things
M2M	Machine to Machine
M2H	Machine to human
H2H	Human to human
MQTT	Message Queuing Telemetry Transport
LPWAN	low-power wide area network

Keywords: IoT, Security, Security Protocols, AES, Encryption, WAN IoT.

Acknowledgment
NIL

Author's Contribution
Hira Beenish and Muhammad Fahad Methodology. Iftikhar Sami and Hira Beenish Literature. Muhammad Fahad, Iftikhar Sami and Hira Beenish Writing. Muhammad Fahad and Hira Beenish Validation and Investigation.

Conflict of interest
The authors declare no conflict of interest in publishing this manuscript in IJIST.

Project details. NIL

Introduction:

An interconnected network of items with distinct addresses is referred to as the IoT. Several factors put IoT systems at high risk of security. Due to their movement, these devices are very dynamic and constantly change with clearly defined parameters. In terms of platforms, devices, and communication protocols, IoT systems are very heterogeneous. The IoT is a part of the "Digital Environment (DE)" in which every device is connected to the necessities it needs to function. Currently, it is integrated with vehicle's power systems and smart power system IoT-based sensors. DE refers to many sensors that collect data, process it, and then exchange it as needed with different nodes.

DE aims to convert traditional manual control systems to automatic intelligent systems by connecting M2M, M2H, and H2H [1]. The IoT has gained global recognition and significance as the core value for low-managed networks because of the proliferation of devices. The IoT uses remote management to achieve the desired utility for the devices [2]. Different areas in cloud domains were examined to highlight the significance of security in IoT elements [3]. The IoT expands connectivity to items that are not physically in our physical domain. It has become essential in various IoT-connected social contexts, as in Figure 1.

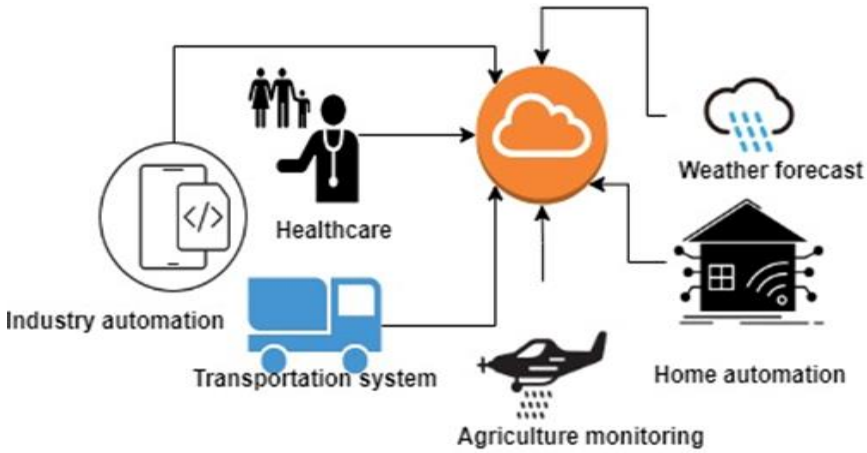

Figure 1. Connectivity of IoT

Thus, even though each environment has different needs like communication, data monitoring, information gathering, and data processing, the IoT has created connectivity everywhere. Due to the large number of objects, it has huge amounts of data to handle these days, all this data is merged with the general communications that are our mobile-based communications [4]. Mobile communication is based on many existing technologies to work efficiently, since the IoT is the block of communication and it is mainly based on wireless communication, which is also based on all cellular generations that are 1G, 2G, 3G, 4G, and most importantly, 5G, as all discussed in [5]. These technologies are based on the fifth generation.

The proposed home automation security is based on IoT protection, concerning the regular layered building [9]. The security risks of an IoT are then examined for equipment, and approach to its parts [10]. The author portrays the safe calculations to be implemented for the safety of IoT customers. The ways of detecting and correcting primarily mobile intruders are described as effective answers for safety in the IoT. Various protection and security issues, and their realistic countermeasures for cloud-based IoT systems have been discussed in [11] which look at important IoT protections, inconveniences, affirmation, approval and wellness, as well as the need for lightweight cryptographic techniques, malware, and programming susceptibilities. The IoT era making an undertaking encoded secure structure, with consistency requires execution to decode. However, to deal with

unmanageable utilization of data, the security policies portray the scrambling and unscrambling data techniques. The security viewpoint focuses on three layers related to the administration, correspondence, and application. So, the OWASP depicts the top ten susceptibilities for the IoT infrastructure. These suspicious and shaky incorporate interfaces which are a part of the gadgets of IoT engineering.

Protocols like CoAP, MQTT, WPA, MD5, Hash, etc. have been introduced to make communication secure and reliable. CoAP is the most widely used protocol in IoT applications due to advantages such as its developer friendliness and lightweight design in terms of energy use and communication mobility, portability, and having a sufficient number of techniques to enhance data security and integrity. The security of data processing protocols, particularly the CoAP protocol, is an essential problem since there are no reliable standards for safe systems.

Aside from its utilization, the IoT serves human connectivity needs. IoT has become a part of various applications of daily use including medical procedures in physician's facilities, distinguishing climate conditions and biochips which are now serving the network's particular needs [6] [7]. The future of IoT is significant because it has made its place in the market due to its usage [8]. To address safety issues within the IoT paradigm, much effort has been made recently. An element of these methodologies targets security problems at a particular layer. An ongoing assessment classifies security issues regarding utility, engineering, correspondence, and records.

Objectives:

This paper consists of security challenges that have been faced by IoT networks and security protocols with a new proposed framework. We used the AES algorithm in wireless sensors for secure communication to examine its reliability and competitiveness.

Security Attacks on IoT architecture:

IoT-based security architecture can be categorized into three types

- Systems
- Applications
- Network devices

All the above-mentioned types deal with the overall security challenges and it requires security frameworks, application-related security issues, and communication among devices respectively. In Figure 2, we have discussed multiple AES attacks that are led in the direction of solutions with their possible destructions. An IoT network must have the following capabilities to provide a secure platform to its users as discussed in [3].

Able to Recover:

IoT devices have lower-cost chipsets and hardware, resulting in a higher failure risk. Fault management is difficult, especially if these gadgets are dispersed across a vast region in physical and difficult-to-reach locations. This problem can be solved via fault tolerance, which attempts to make it able to operate in a way from occurring in the first place, or through failure recovery approaches, which aim to recover from issues.

Access Control:

The system administrator can control the access of users. Each user should have their ID and password to access only the relevant portion of the system or database or the user can access or manage the same multiple gadgets that are connected to the same IoT system.

IoT Architecture:

The perception layer, network layer, and application layer are the three levels that incorporate the IoT structure. Many applications employ network support technologies as the processing layer (for example network processing, computing technology, middleware technology). The basic architecture of IoT consists of 3 layers [4] as under

- Application Layer
- Network Layer
- Perception Layer

The first layer of architecture is known as the object layer which contains sensors and actuators to collect and communicate information with surroundings. This layer digitizes the information and passes it to other layers through a secure channel [12]. The second Network layer is used for establishing connections among devices, servers, and smart things. It is also used for the transmission and processing of sensor data to their access points [8]. The perception layer is closest to the user and is also known as the abstraction layer. It transfers the data generated by the object layer through various available technologies like RFID, 3G, Wi-Fi Bluetooth, etc. It is also responsible for processing the received data and making a decision based on the protocols which are a part of their systems, or their connectivity with the system and actuators. It is responsible for providing customer services according to its system requirements [4].

IoT Convention and Benchmark:

The IoT structure is based on a layered layout with fundamental conventions. It contains the guidelines and conventions for low-rate wireless personal area network devices for individuals (LR-WPANs). For LR-WPANs, the IEEE provides many standards that are a part of 802.15. This standard is mostly used as low-level layers, including the physical layer and the MAC layer. The physical layer decides whether to conduct correspondence over distant channels with unique repeat patterns and realities. The MAC layer warranty is associated with the frameworks, which are concerned with channels and they can get rid of jitters that cause the synchronization. Due to packet length, which is the MTU used by the IEEE 802.15 for existing communication of MTU with the old versions of IPs is now converted for security to IPV6. Every instrument in IoT is distinct because it is associated with different organized addresses, but they are in the same contact with remote connections. The Routing Protocol for Low-Power and Loss Networks (RPL) is employed to assist LoWPAN things so they can adequately aid in routing. The RPL calculates the normal backing errors that are purpose-to-point activity and additionally the correspondence between multi-focuses and single points. Due to payload, the appliances structured in IoT merge User Datagram Protocol (UDP) for fast connections, as it does not rely on acknowledgment, making it viewed as more powerful and less cumbersome than other protocols [1]. The LPWAN is an extended form of communication for "things" in IoT. Instead of a traditional WAN, which needs the additional capability to figure out data with unknown destinations, the LPWAN utilizes the WAN protocol for communication among different security protocols and devices, while supporting various data rates for communication in a network when it reaches its higher connected scales. The weightless protocol utilizes three distinctive standards for communication in LPWAN, namely uni-directional, bi-directional, and low-control modes. To ensure the classification of information as it passes through many device hops, an appropriate encryption tool is needed. The information stored on a device is vulnerable to data breaches by exploiting terminals present in an IoT due to a diverse mix of administrations, devices, and systems. Attacks on IoT devices have the potential to alter data, which might reduce the accuracy of the information.

Table 1. Encryption techniques used in IoT-based Literature.

References	RSA	MD5	HASH	AES	TBSA
[1]	✓	✓	×	×	✓
[13]	×	×	×	✓	×
[12]	✓	×	×	×	×

[14]	✓	×	✓	✓	✓
[15]	✓	✓	✓	✓	×
[16]	×	✓	×	×	×
[17]	×	✓	✓	✓	✓
[18]	✓	✓	✓	✓	✓
[19]	×	×	×	×	✓
[20]	✓	✓	×	✓	×

The above table elaborates on the encryption techniques that are used in referenced papers, to enhance the IoT techniques from a security perspective. A lot of work has been done for encryption techniques that are working on IoT.

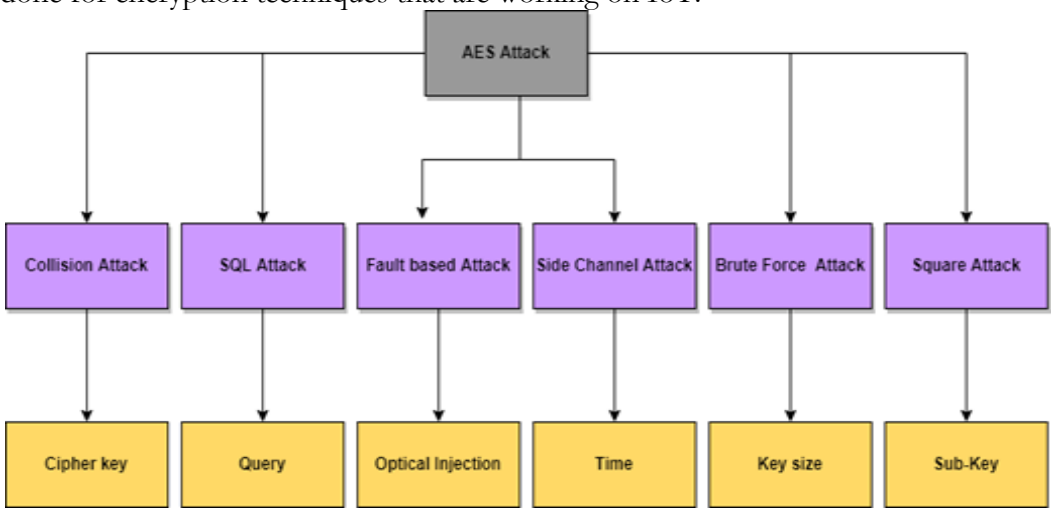

Figure 2. AES attack attributes.

Open Issues and Challenges:

When considering the development of robust defensive measures against cybersecurity hazards, it is important to acknowledge the unique characteristics and constraints of the IoT. Disregarding these privacy and security considerations will yield adverse consequences across several aspects of our lives, including the residential dwellings we inhabit, the automobiles we utilize for commuting, and even our well-being.

For the association of every individual issue, the grouping of security vulnerabilities for IoT is done alongside. Embedded sensors are produced on a variety of heterogeneous devices that are connected by a network in an IoT implementation. These IoT devices are individually recognizable and are typically characterized by low power consumption, little memory, and constrained computational power. Such gateways are set up to link IoT devices to the outside world so that IoT users can access data and services remotely. Radio interference significantly affects performance and might affect transceiver communication. The gadgets used by the IoT should use the management key points. If there is any weak point in the network area or any huge overhead securing sending or receiving, it may expose the network layer to a huge number of dangerous things.

IoT resolves the usefulness of scale node authentication. In addition, mobile intelligent terminals will also play a significant role in the IoT perception layer. Thus, its security cannot be disregarded. To ensure the classification of information as it passes through many device bounces, an appropriate encryption tool is needed. The information stored on a device is defenseless against data protection by exchanging off terminals that are present in an IoT due to a diverse mix of administrations, devices, and systems. The IoT devices are susceptible to attacks, which might reduce the accuracy of the information by modifying data.

Low-level security:

The top security layer is connected to issues in the physical and DTLS layers connected to the hardware. The IoT has been used in every aspect of the quickest-developing technology trends in recent years. However, increasing security prevention creates several potential connectors to refrain from victimization on IoT devices. It is mentioned for IoT design engineers who want to safely implement these devices.

Challenges:

IoT has been facing many challenges as the size of the network increases. One of the biggest concerns in IoT networks is data handling, fault tolerance, energy efficiency, reliable communication protocols, and security [2].

Data Security:

Data transmission is only allowed on authentic devices. Different mechanisms are available to test the authenticity of devices [3]. Since each smart device is anticipated to be fed by several sensors, each of which produces vast amounts of data over time, not only a huge number of smart objects but a huge amount of data will also be generated by each device. It is therefore crucial to develop an effective defense that can secure these data streams.

Data Privacy:

Data privacy is an important part of any system. So, any irrelevant person or any other client cannot access or share the data of any client [3]. IoT privacy protection is essential since there is a huge amount of information about a person's life by listening to the sensed data that their wearable technology and smart home gadgets transmit. It is necessary to create new processes that will make it more difficult for future fog devices to locate smart items. Furthermore, by collecting and analyzing the wireless signals that are transmitted between the sensing items, it is now able to detect the presence of humans and track their position, their lip movement, and their heartbeats.

Lack of Common Standards:

There are many IoT-providing industries and each has its standards. There is a need to establish some standard protocols. Several IoT common standards were developed to assist in the analysis of the value and services that we can use for IoT solutions to connect various devices to the internet. The IoT is being pushed by several groups, including the European Telecommunications Standards Institute (ETSI), the World Wide Web Consortium, EPC-Global, and the Institute of Electrical and Electronics Engineers (IEEE) (W3C), as in [13].

IoT Design Challenge:

A conventional IoT setup includes a variety of devices with embedded sensors that are connected via a network. IoT devices are extremely well-defined and typically have low power, memory, and handling capacity. Doors are delivered to connect IoT devices outside of the home to manually arrange information and services for IoT consumers. As discussed in [16], some issues are related to data and privilege protection. Since the security of IoT is a very important aspect, Also, some brute force attacks and SQL injection operations can be performed on IoT systems, e.g., smart lock systems, home automation systems, etc.

Novelty Statement:

To overcome all the above-mentioned issues, a proposed scheme is presented to provide a favorable solution. Encryption techniques are used e.g. AES and CoAP to secure the data before sending it to the cloud and to make smart gadgets compatible, an architecture is proposed that is connected with semantic web technologies like AES, allowing communication between the CoAP and AES protocols, which are used for semantic reasoning, to provide interoperability across communicating messages in the IoT.

Material and Methods:

CoAP is an HTTP-compatible, compact Internet Application Protocol. The GET, PUT, POST, and DELETE methods are used to access it in microcontrollers, social networks, and automation. REST is based on a client-server architecture that is stateless and applies to both clients and servers for web services. The proposed scheme gets the data from the edge node and implements the AES algorithm on the data, and after that encrypted data wraps into CoAP and is transferred to the cloud. Now it is not easy for an attacker to steal data or perform SQL injection in the system. Since there are 10, 12, and 14 rounds in the AES algorithm and every step is coherent with the next step, and then it converts data to CoAP message format, CoAP will hide the encrypted data and create another layer of data packets. By implementing AES and CoAP, IoT systems will be more secure and efficient, as shown in Figure 3. There are other methods that we call access control systems [16]. However, it can't provide sophisticated and better results due to the limited resources of IoT devices. To fulfill data confidentiality, the data encryption technique used in this paper is AES with CoAP to secure our system.

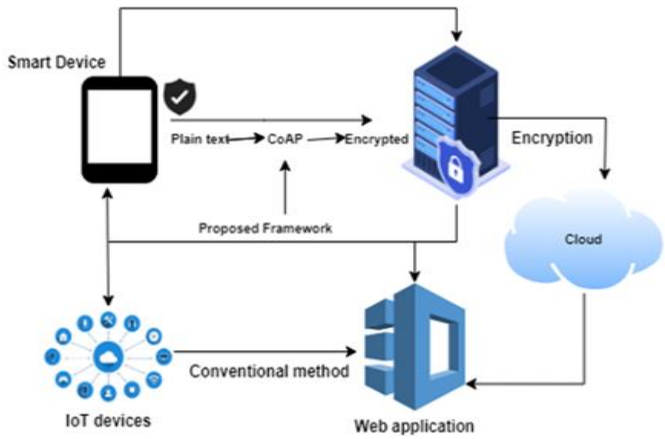

Figure 3. Proposed Framework of AES

CoAP is currently one of the most well-liked approaches to IoT communication since it offers a great degree of adaptability and is widely used. Its adaptability and interoperability in terms of Internet of Things communication is the primary benefit it offers. The CoAP protocol achieved the quickest time-to-completion, which we believe is due to the reliable exponential back-off mechanism. This technique is helpful in settings when there is a lot of messaging going on. When using the CoAP as an adjunct to the traditional technique, as shown in Figure 3, and combining all of the phases of the AES, it was noticed that the inclusion of CoAP required a greater amount of data bits than the traditional approach alone did. This was the case even though the inclusion of both approaches resulted in the same level of security. As a result, the secure CoAP protocol, in its specified form, displays a reduction in the amount of power that is consumed in proportion to the rise in the number of bits, as the graph in Figure 5 illustrates.

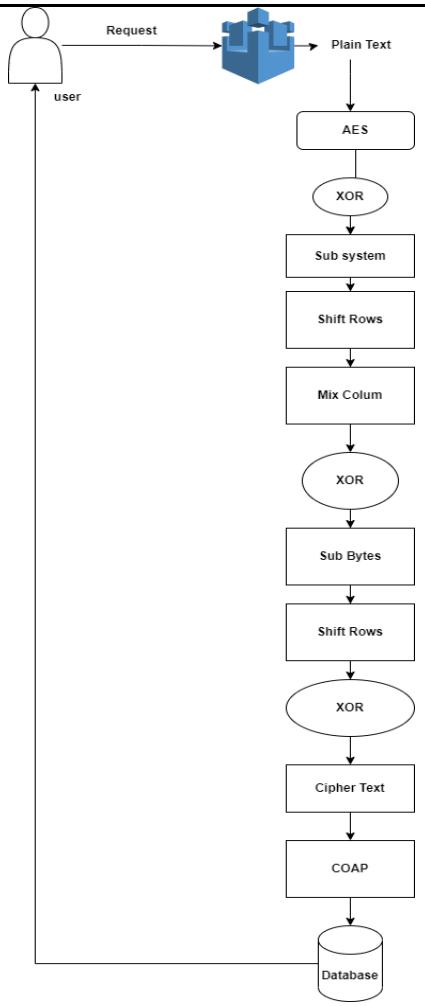

Figure 4. Flow chart of Proposed Model.

Workflow of Model for AES algorithm:

AES is a block cipher, and it comes in three versions: AES128, AES192, and AES256. Each version, numeric part represents the key length used in that specific version. In this paper, we propose AES128 with a key length of 128 bits and a 128-bit block size, and a total of 10 rounds are required for the encryption and decryption processes. AES takes input in a 128-bit block size and encrypts the data as per the flow of Figure 4. The encrypted data will be considered a payload for the CoAP protocol, and then the network layer of the edge devices will send the encrypted payload to the server. The server receives the payload from the CoAP protocol and decrypts it before submitting it to the database for permanent storage. As AES uses a 128-bit key length for encryption, an interception attack on the network is countered. The 128-bit key length provides sufficiently large key space, where Brute Force attacks seem ineffective and cryptanalysis is not possible as AES is more secure against this attack with the integration of CoAP.

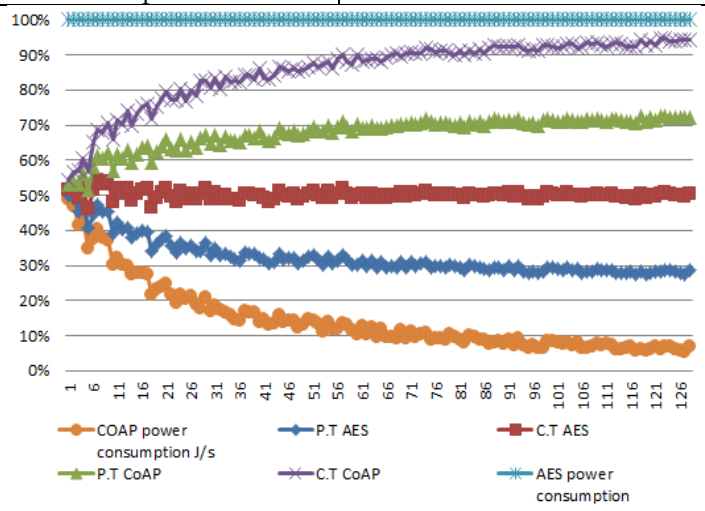

Figure 5.AES and CoAP power consumption of bits

If C.T. AES lines will change to a higher percentage then the power consumption will increase of the AES-based devices. The X-axis represents the power consumption of protocols and The axis represents the bit utilization percentage, 1-126 is the range of power consumptions of AES and COAP protocol

Discussions:

IoT devices have constrained processing capabilities, memory, and storage space, so they must run on a minimal amount of electricity. Due to the complexity of the encryption and decryption procedures, security methods need strong encryption methods that are suited for devices with limited resources. These approaches are required for data transmission that is both speedy and secure. As a result, limited devices, such as actuators and sensors, require algorithms that are not resource-intensive but still provide enough security. Hash functions and the AES need to be used to protect the communication that takes place between these devices and guarantee their integrity and confidentiality. The deployment of the CoAP protocol in IoT networks introduces additional issues, as a result of the high number of false warnings that are produced by this protocol.

The provision of real-time authentication presents a problem, as does the extension of the range of assaults detected, as well as the consideration of the influence of the performance of IoT devices in terms of overhead, energy consumption, and accuracy. The new era of Industry 4.0 and industrial IoT calls for the development of an innovative intrusion detection approach to ensure the safety of all linked systems and services. More work needs to be done to build prevention methods for specific attacks that could be launched against the environment of an IIoT system, such as a smart grid, transportation, or smart industrial. Creating a security protocol for the smart grid application that uses less computing and is optimized for devices with limited resources.

These devices are vulnerable and are unable to defend themselves against attacks. For Internet of Things security, product researchers need to rethink how they develop technologies, secure code, and hardware in areas such as physical security, network security, application security, and compliance. In this work, we focus on a significant side of the Internet of Things that is related to Internet protocols. Even though research on these protocols has been conducted and published, there is still a need for more in-depth research to complete studies and analyses on a variety of topics, most notably security, and potential remedies. One of the most important protocols that is considered to be an application layer protocol is called CoAP. The comparison was carried out by contrasting the approaches taken, the goals of the studies, and the findings presented in each paper. Hosts that are enabled with the CoAP protocol will play a crucial role in the Internet of Things (IoT). In addition, installations of CoAP-enabled devices in the real world necessitate the use of security solutions. We evaluate and investigate the main IoT security vulnerabilities. We briefly discuss the frameworks recommended in the literature for using IoT with many security characteristics.

The study also distinguishes between the various subsequent algorithms used in the field of IoT security and discusses the techniques used to improve IoT security. Finally, a framework for securing IoT-based systems, such as smart homes, smart lock systems, etc., has been proposed. The capability of CoAP to deal with multicast is communication and one of its most notable characteristics. This capability enables an Initiator to send requests to numerous Responders at the same time. The lack of success of this work lies in the fact that we did not take into account the multicast functionality. The proposed model encrypts the end user data after the encryption techniques of AES, as shown in Figure 4, this encapsulates the AES-encrypted data with CoAP.

There have been different implementations of CoAP depending upon the market's interest in IoT technologies that have significantly expanded as a result. By integrating AES with CoAP, the sensitive data transmitted over the CoAP protocol can be securely encrypted, ensuring confidentiality and data integrity. This integration allows for secure communication between devices and servers, protecting the transmitted data from unauthorized access and enhancing the overall security architecture of CoAP-based systems.

This is because there is a high probability that CoAP will affect the future of all applications. IoT Systems for access control methods can also be used for this implementation, and real-world systems and 3D simulations will both be used in future work. The research reported in this article is to secure the IoT and CoAP-based systems using AES.

Data security and data privacy are the most important challenges of the research that need to be focused and implemented. The proposed model makes end-user data temper-free and secure by applying the AES algorithm for encryption. Man-in-the-middle (MITM) and modification attacks are addressed in this solution therefore, sensor data besides end-user data can safely be transferred. The AES standard makes it much more difficult to perform cryptanalysis therefore online modification is also not possible unless the master key is not compromised. The generation of the key is also very complex procedure therefore, the interceptor is not in a position to generate the valid master key. The strong avalanche effect of the AES algorithm makes it a prime choice for securing data. This study makes an impact on the proposed framework of various Internet of Things (IoT) communication solutions by first presenting a comparison table that contrasts the properties of various IoT protocol implementations. The majority of protocols already allow both TCP and UDP traffic, except UDP.

The support for UDP is particularly relevant in future IoT environments because the devices that will be there will become more mobile. The CoAP protocol is designed or simplicity and operates over the UDP in IoT. This is used in Internet data transfer and is employed with restricted nodes and restricted networks in the Internet of Things. Because of this, communication protocols need to be developed in a way that takes into account the varied topologies that may be present. Other important facets of the Internet of Things, such as the discovery of data and devices, are still defined manually. The purpose of the majority of the many solutions that have been created is to offer support between devices and the edge in terms of providing end-to-end coverage for secure communication. To summarize, from a design standpoint, AES and CoAP are the solutions that seem to provide the most flexible design, integrated by design a set of characteristics that are significant when thinking about the possible evolution of IoT environments. Both of these solutions are integrated by design to provide a set of features that are relevant when thinking about the potential evolution of IoT environments. In comparison to the other alternatives, it offers superior support in terms of communication within the plant, and as a result, it is the communication standard that is universally accepted in settings involving industrial automation.

The new technology of the Internet of Things enables physical network connectivity and the processing capability of sensors and control systems, making it possible for these systems to generate, exchange, and consume data with minimal involvement from humans. This survey has revealed a variety of security dangers at different layers of the Internet of Things (IoT), as well as security concerns and solutions about the overall environment of the Internet of Things (IoT). It has addressed the concerns of the security of the application layer, as well as the network layer, the middleware layer, and the communication protocols. In addition to this, it has presented an in-depth review of existing Internet of Things solutions that are based on a variety of security techniques, such as cryptography and IDSs.

The current state of IoT security has been reviewed, along with some of the potential future research avenues that may be taken to increase IoT security levels. The results of this poll are going to be compiled into a plan for improving the safety of industrial uses of the Internet of Things. Because of it being that CoAP is a new protocol, it is not yet widely studied in many different fields. It is currently being used in a variety of applications, which has led to an increase in the number of application-specific upgrades being carried out. A significant amount of investigation was conducted to improve CoAP in terms of security,

end-to-end authentication, streaming services, and so on**.** The proposed framework uses a single request to retrieve data. This helps in requesting messages by minimizing the amount of channel accesses that are required. As a result of this, the throughput performance can potentially be improved.

Conclusion:

IoT devices are susceptible and aren't able to protect themselves. We evaluate and investigate the main IoT security vulnerabilities. We briefly discuss the frameworks recommended in the literature for using IoT with many security characteristics. The study also distinguishes between the various subsequent algorithms used in the field of IoT security and discusses the techniques used to improve IoT security. Finally, a framework for securing IoT-based systems, such as smart homes, smart lock systems, etc., has been proposed. The proposed model encrypts the end user data using the AES technique, as shown in Figure 4, by encapsulating the encrypted data with CoAP. IoT Systems for access control can also be used for this implementation, and real-world systems and 3D simulations will both use it in the future.

References:

[1] E. Akanksha, "Efficient framework to secure communication in IoT using novel finite field encryption," Adv. Intell. Syst. Comput., vol. 860, pp. 1–11, 2019, doi: 10.1007/978-3-030-00184-1_1/COVER.

[2] K. Zhao and L. Ge, "A survey on the IoT security," Proc. - 9th Int. Conf. Comput. Intell. Secure. CIS 2013, pp. 663–667, 2013, doi: 10.1109/CIS.2013.145.

[3] M. Dabbagh and A. Rayes, "IoT Security and Privacy," Internet Things from Hype to Real. Road to Digit. Second Ed., pp. 211–238, Jan. 2018, doi: 10.1007/978-3-319-99516-8_8/COVER.

[4] M. Abdur, S. Habib, M. Ali, and S. Ullah, "Security Issues in the IoT (IoT): A Comprehensive Study," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 6, 2017, doi: 10.14569/IJACSA.2017.080650.

[5] H. Beenish and M. Fahad, "5G a review on existing technologies," 2019 2nd Int. Conf. Comput. Math. Eng. Technol. iCoMET 2019, Mar. 2019, doi 10.1109/ICOMET.2019.8673407.

[6] P. Sethi and S. R. Sarangi, "IoT: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, 2017, doi: 10.1155/2017/9324035.

[7] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "Security&privacy issues and challenges in NoSQL databases," Comput. Networks, vol. 206, p. 108828, Apr. 2022, doi: 10.1016/J.COMNET.2022.108828.

[8] S. Deshmukh and S. S. Sonavane, "Security protocols for IoT: A survey," 2017 Int. Conf. Nextgen Electron. Technol. Silicon to Software, ICNETS2 2017, pp. 71–74, Oct. 2017, doi: 10.1109/ICNETS2.2017.8067900.

[9] S. Pirbhulal et al., "A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network," Sensors 2017, Vol. 17, Page 69, vol. 17, no. 1, p. 69, Dec. 2016, doi: 10.3390/S17010069.

[10] S. GÖRMÜŞ, H. AYDIN, and G. ULUTAŞ, "Security for the IoT: a survey of existing mechanisms, protocols and open research issues," J. Fac. Eng. Archit. GAZI Univ., vol. 33, no. 4, pp. 1247–1272, Dec. 2018, doi: 10.17341/GAZIMMFD.416406.

[11] K. Chen et al., "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," J. Hardw. Syst. Secur. 2018 22, vol. 2, no. 2, pp. 97–110, May 2018, doi: 10.1007/S41635-017-0029-7.

[12] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad, "A review of data security and cryptographic techniques in IoT based devices," ACM Int. Conf.

Proceeding Ser., Jun. 2018, doi: 10.1145/3231053.3231100.

[13] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in IoT," Neural Comput. Appl., vol. 32, no. 15, pp. 10979–10993, Aug. 2020, doi: 10.1007/S00521-018-3801-X/METRICS.

[14] S. Sasirekha, S. Swamynathan, and S. Suganya, "An ECC-based algorithm to handle secure communication between heterogeneous IoT devices," Lect. Notes Electr. Eng., vol. 443, pp. 351–362, 2018, doi: 10.1007/978-981-10-4765-7_37/COVER.

[15] J. J. Barriga A and S. G. Yoo, "Security over smart home automation systems: A survey," Smart Innov. Syst. Technol., vol. 94, pp. 87–96, 2018, doi: 10.1007/978-3-319-78605-6_7/COVER.

[16] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Futur. Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/J.FUTURE.2016.11.031.

[17] D. Halabi, S. Hamdan, and S. Almajali, "Enhance the security in smart home applications based on IOT-CoAP protocol," 6th Int. Conf. Digit. Information, Networking, Wirel. Commun. DINWC 2018, pp. 81–85, May 2018, doi: 10.1109/DINWC.2018.8357000.

[18] D. e. S. Agha, F. H. Khan, R. Shams, H. H. Rizvi, and F. Qazi, "A Secure Crypto Base Authentication and Communication Suite in Wireless Body Area Network (WBAN) for IoT Applications," Wirel. Pers. Commun., vol. 103, no. 4, pp. 2877–2890, Dec. 2018, doi: 10.1007/S11277-018-5968-Y/METRICS.

[19] B. Yilmaz and S. Özdemir, "Performance comparison of cryptographic algorithms in IoT," 26th IEEE Signal Process. Commun. Appl. Conf. SIU 2018, pp. 1–4, Jul. 2018, doi: 10.1109/SIU.2018.8404524.

[20] I. Sultan, B. J. Mir, and M. Tariq Banday, "Analysis and optimization of advanced encryption standard for the IoT," 2020 7th Int. Conf. Signal Process. Integr. Networks, SPIN 2020, pp. 571–575, Feb. 2020, doi: 10.1109/SPIN48934.2020.9071380.