IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

# DESIGN AND IMPLEMENTATION OF SECURITY FRAMEWORK TO ENHANCE INTERNET OF THINGS ENVIRONMENTS USING CRYPTO MODEL

**Gloria Obiageli Obuseh[1], Ikechukwu Innocent Umeh[2], Ikechukwu Udoka Onwuegbuzie[3]**

Nnamdi Azikiwe University, Awka[1,2]

Griffith College Dublin, Dublin, Ireland[3]

**Abstract:** The devices applicable in the Internet Of Things (IoT) have developed to comprise embedded systems and sensors which has the ability to connect, collect, and transmit data over the Internet. Although there exist solutions to secure IoT systems, but the resources to support such solution are insufficient, and considered constrained in terms of secure communication. The aim of the study is to secure the entire path in an IoT environment into two segment, which comprises of securing data through encryption and decryption, using Cryptography and Steganography techniques. The approach introduced in this project makes use of both steganographic and cryptographic techniques. In Cryptography Rivest, Shamir, Adleman (RSA) is used, while in Steganography Image Steganography for hiding the data is applied. Also, the Mutual Authentication process to satisfy all services in Cryptography which include; Access Control, Confidentiality, Integrity, Authentication were employed to maintain the data more security. Having use RSA algorithm for securing the data and again on this we perform Steganography to hide the data in an image, such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

**Keywords:** Design, Internet of Things (IoT), implementation, cryptography, steganography, security, communication, environment.

## I. INTRODUCTION

The Internet of things (IoT) is used to describe a network that connects various physical objects with sensors, to the Internet for information exchange and communication in order to realize intelligent identification, positioning, tracking, monitoring and management of such items (Routh & Pal, 2018). The Internet of Things (IoT) can be defined as a network of globally identifiable physical objects (or things), their integration with the Internet, and their representation in the virtual or digital world. A larger number of devices are connected to the IoT in order to provide innovative and interconnection services.

IoT has changed over time. Early publications relating to IoT focused mainly on IoT usage of secular networks and radio frequency identification (RFID) chipsets for the service. The wide availability and low cost of RFID were significant factors that led to the quick adoption of IoT by many. The cheapness of electronics devices paved more ways for IoT abilities to be included in more devices and improved the functionality of devices with short life expectancies (Rayes & Mohammadi, 2015). The industrial sector witnessed improved developments in radio frequency identification tags, which comprises of an antenna and a memory chip that stores data. The incorporation of the RFIDs into the workflow of devices have been widely applied in numerous areas. For example, RFIDs have been applied in retailing environments to facilitate inventory and package tracking, in the health sector, to monitor patients' health and their medication administration (Monteiro & Silva, 2015). RFID tags are also incorporated in smart passwords, credit cards, and in the identification of badges for accessing secure areas in organizations. The trend of adding RFID tags and readers in "things" not only inspired, but resulted to the term "Internet of Things" (Standford, 2018).

Within the past six years, IoT has received a great deal of attention from both academic researchers and the business community. IoT is now considered one of the most important elements in the technology Industry (Perera et al., 2014). Estimates show that there will be over 50 billion IoT devices by 2030, and generating up to 4.4 zettabytes of data, and that the economic profit or revenue that would be generated by the IoT market to range between $1.6 trillion to $14.4 trillion by 2025.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024
DOI: 10.17148/IJARCCE.2024.13101

Also, projections suggest that IoT shall have impacted positively on nearly every sector, ranging from economy to human life, transportation, healthcare, agriculture, housing, vehicles, schools, markets, and industry by 2025 (Al-Fuqaha et al., 2015).

It is noteworthy that communication in IoT does not only occur between devices, but also between people and their environment. IoT systems require unique identifiers so that people, cars, computers, books, televisions, mobile phones, clothes, groceries, medicines, passports, luggage, and other everyday items can communicate with each other (Soullie, 2014). The Internet of Things has a huge positive impact on citizens, businesses and governments. IoT benefits ranges from aiding governments reduce health care costs and improve quality of life, to reducing their carbon footprint, which is subject to improving access to education in remote and underserved communities, things, and to improve transportation.

## II. SECURITY IN IoT

Security is paramount in IoT is very necessary in application domains with systems, which are critical to personal and community security. For example, systems' passwords need to be secured because weak passwords would avail attackers the opportunity to use some tools to crack any system. In the field of medicine, medical and health monitoring devices must be secure to ensure that the information they monitor, collect or report to is accurate, and that critical equipment remains available and operational unharmed by intruders.

In the security of IoT systems, IPv6 offers interconnection of almost every physical object that is connected to the Internet, availing tremendous possibilities of developing new applications, such as home automation and security management, smart energy monitoring and management, item and shipment tracking, surveillance and military, smart cities, health monitoring, logistics monitoring and management for IoT. The global connectivity and sensitivity of IoT applications, demands for real time security in the deployments IoT (Shahid & Thiemo, 2010).

According (Nicolas & Adam, 2019), Securing an IoT message requires the consideration of the following:

**Confidentiality:** Messages in an IoT environment should be hidden from the intermediate entities to evade content interception while in transit. In other words, End-to-End (E2E) encryption is required to provide the required message secrecy between a message source and a destination. Confidentiality services ensure this through message encryption/decryption.

**Data Integrity:** No intermediary between a source and a destination should be able to undetectably change secret contents of messages, for example a medical data of a patient stored used an IoT device should not be undetectably modified. Message Integrity Codes (MIC) are mostly used to provide this service.

**Source Integrity or Authentication:** Communicating end points should be able to verify the identities of each other to ensure that they are communicating with the entities who they claim to be. Different authentication schemes exist (Shahid & Gianluca, 2011).

**Availability:** Access to data should always be whenever needed. It is important that services that applications are always available in good working condition. In other words, intrusions and malicious activities must be detectable at any time. Intrusion Detection Systems (IDSs) and firewalls mechanisms are used to ensure availability security services.

**Replay Protection:** A compromised intermediate node can store a data packet and replay it at later stage, the replayed packet can contain a typical sensor reading like, a temperature reading of a patient, or a paid service request. Therefore, multi-faceted security is applied to ensure E2E communication security in IoT environment. Network security in 6LoWPAN networks, and also data-at-rest security should be deployed to protect stored secrets and data.

## III. METHODS OF COMMUNICATION PRIVACY

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. Cryptography is the art of secret writing, which is used to encrypt a plaintext with a key into ciphertext while been transferred between parties on an insecure channel. Using a valid key, a ciphertext can be decrypted to its original plaintext. Without the knowledge of the key, a plaintext remains irretrievable. Cryptography plays an essential role in many factors like confidentiality, privacy, non- repudiation, key exchange, and authentication, which are require for securing a data transmission channel.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024
DOI: 10.17148/IJARCCE.2024.13101

Message insecurity in IoT posse a considerable number of problems. Data loses or modification by unauthorized persons in the process of transmission constitute a greater part of security concerns in IoT. Many Internet users have fallen victim to cybercriminals as a resulting from network security breach, data theft and loses in productivity. Therefore, securing clients data and information is crucial for online safety of IoT messages.

## IV. AIM AND OBJECTIVE OF STUDY

The aim of this study is to design and implement a security framework to enhance an Internet of Things environment. The aim would be achieved by examining the necessary components of a modeling language to elicit the security requirements of an IoT system, how to Secure IoT data using steganography and cryptography and finding and implementing the type of security design needed to be performed in an IoT system to offer baseline security.

## V. RELATED WORKS IN SECURITY OF IoT

Since the inception of IoT, many works have been carried out on IoT data privacy and security. Most of the reviewed works surveyed commercially available and frequently used IoT programming frameworks from major cloud providers, which supported rapid IoT application development, rather than the approaches taken to provide security and privacy at the programming level of IoT security frameworks.

Mislolavskaya and Tolstoy (2019) examined IoT applications in the industry, personal medical devices, Smart Homes, and general IoT Security needs for data safeguard. Mislolavskaya and Tolstoy (2019) concluded that service interruptions and data leakage were the two major security risks to IoT, and listed the potential defenses for different attack categories of smart homes.

Dhanvjay and Patil (2019) surveyed the uses of IoT application in clinical care, health care, remote monitoring and context awareness, and stated that there are no clearly defined architectures for IoT in healthcare, but the study provided the network topology. The study discussed the frameworks for health information service models and Wide Body Area Networks (WBAN) for healthcare applications, and the security and efficient of data delivery for fog-assisted wireless body area networks. In conclusion, Dhanvjay and Patil (2019) stated the necessity of WBAN in IoT for healthcare, and stated that the problems of IoT in healthcare delivery to include; scalability, data privacy, security, and low-powered devices.

Blockchain technology has also been applied to IoT security solution. The taxonomy of security concerns by layers in IoT include the groupings of the protocol stack's layers-low levels. These include; Hardware, Physical and Data Link Layers, intermediate level including the Network and Transport layers. The Application layer-categorize security challenges and potential remedies. Therefore, it is worthy to note that blockchain-based solutions for IoT has its own technical flaws.

Makhdoom and Abolhassan (2019) thorough examined IoT security with respect to the anatomy of Threats to the Internet of Things. The examination encompassed the services and protocols within the semantics, application, MAC/Adaptation, network and physical, and perception levels of the IoT protocol stacks. A survey by Makhdoom and Abolhassan (2019), reviewed the significant malware assaults on IoT devices. The survey also carried out an analysis on the mechanisms of malware attacks from the planning to the execution, hiding and cleanup of such attacks. Makhdoom and Abolhassan (2019) further argued that the current IoT security is insufficient to protect IoT environment against malware attacks, and thus, recommended a framework, which could provide a comprehensive IoT security, with each security mechanism addressing a specific IoT threat.

Assari and Almagwashi (2018) introduced a three-tier architecture comprising of security, privacy, and difficulties facing IoT as a solution to help solve IoT issues. The study emphasized that security and privacy as the most perceived primary obstacles to the future adaption and development of IoT. Minoli (2018) recommended the development of a comprehensive security and privacy framework for IoT to solve IoT's security challenges.

Similarly, Meneghello et al., (2018) explored the specific security techniques employed by the most widely used IoT communication protocols, and highlighted the security dangers in the IoT space. The study also introduced some foundational components of the IoT model and made an assessment on the state of IoT applications.

Frustaci and Fortino (2018) developed a system to evaluate critical security issues on IoT. The system adopted a three layers model comprising of; Application, Transportation and Perception layers.

DOI: 10.17148/IJARCCE.2024.13101

Possible attack methods on each layer were considered, and followed by a consequent method of fixing each layer's attack. According to the study, the perception layer was the most vulnerable for devices with physical accessibility for sensing and monitoring an IoT environment. The study futher recommended the exploration of the differences between a typical IT security requirements and IoT security requirements via a multi-layer and cross-layer security strategy.

Chandra et al., (2018) developed an intruder image capturing system to automate home appliances using small IoT devices like the Raspberry Pi. The system operates by taking a picture of an intruder who breaks into an IoT system, and sending same to an approve email address using the Simple Mail Transfer Protocol (SMTP). The system could defend a family's IoT safety, but did not consider the security of little devices applied in designing IoT systems.

Mohmoud & Yousef (2017) prescribed a three-layer IoT architecture split between Perception, Network and Application layers to achieve IoT security goals of confidentiality, integrity and availability (CIA-triad). The study categorized the issues in IoT into technological and security issues. The security issues included the CIA-triad and end-to-end security, while the technological issues referred to challenges like the heterogeneity of IoT hardware, wireless networking technologies, and scalability requirements.

Benzarti and Tirki (2017) carried out a thorough overview on assaults on IoT networks. The study covered both common and peculiar types of attacks in IoT applications. Benzarti and Tirki (2017) concentrated on the development of IoT applications for smart homes, smart grids, and vehicular ad hoc networks (VANETS), and the associated wireless networking technologies.

The study proffered a taxonomy of assaults on IoT, and categorize the attacks between on different applications, and the associated wireless networks. Finally, the study suggested the design of a more complex plan that would includ cryptography for IoT devices with limited resources since there is no universal defense against all threats.

Neshenko et al.,(2017) concentrated on IoT security flaws, and exposed several IoT vulnerabilities and their attack techniques. The study classified appropriate corrective measures for vulnerabilities attacks.

Sezer (2016) addressed the issues and related influences on IoT elements. The study introduced the vulnerability of embedded systems, various IoT security and privacy threats and challenges caused by basic communication and chip technologies of IoT devices. Sezer (2016) summarized emerging IoT security, technologies, and future trends in IoT security.

Barki & Gharout (2016) developed machine-to machine (M2M) application to be used the primary application categories of automotive, e-health, smart metering, city automation and home automation. The study offered a taxonomy of assaults against M2M, including categories for attacks on data, logical or physical targets.

M2M issues bothered with scalability, heterogeneity, limited resources, and a range of end-to-end communication protocols. Barki & Gharout (2016) suggested that addressing IoT privacy, authentication, and confidentiality were not issues of serious concern.

Doukas et al., (2012) developed a basis for securing the IoT device which did not cover the entire pathway. Security gaps exist between the IoT device and the wireless sensor network gateway (WSN).

From the reviews above, it is evident that security of an IoT environment is sacrosanct and cannot be overemphasized. There is a gap to be filled with respect to the efficiency of security of IoT environments. This study therefore present the design of security framework to enhance an internet of things environment using a crypto model.

## VI. MATERIALS AND METHODS

An Internet of Things environment consists of web-enabled smart devices that use embedded systems such as processors, communication hardware and sensors, which are used to collect, send or act on data gotten from their environments TechTarget (2023).

Therefore, encrypting an Internet of Things (IoT) environment is crucial to guarantee the security and privacy of the messages and data being collected, sent or manipulated. The section below is an outline of the materials and and methods required for encryption of an IoT environment as shown figure 1.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

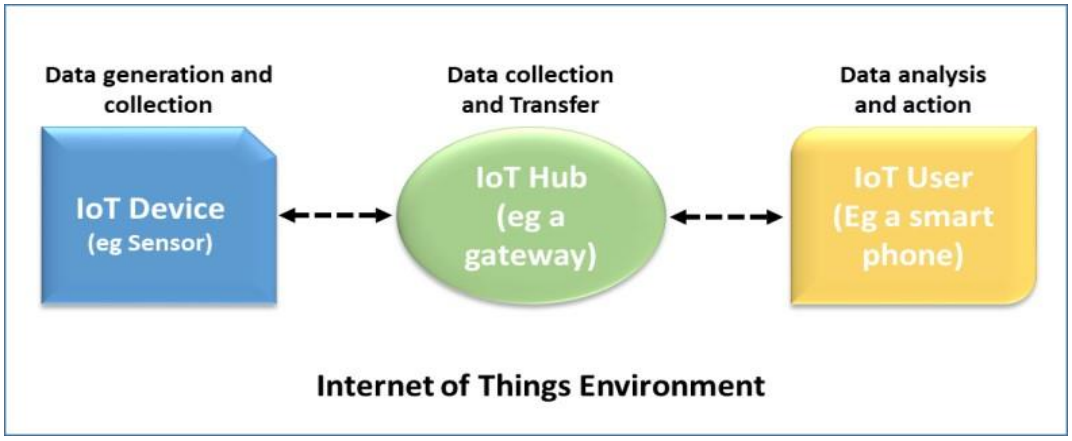


Figure 1. The Internet of Things Environment

Cryptographic Algorithms and Protocols are strong and proven encryption algorithms. Cryptography is a secure key management system that is used to generate, store, rotate, and distribute encryption keys, while derivation functions are used to generate encryption keys from an existing master keys for a higher security provision.

IoT Devices identity and authentication are implemented with strong mechanisms to prevent unauthorized devices from accessing network and stored encrypted data on IoT devices. The mechanism is used to protect sensitive information in network databases even when associated devices are offline.

The Object-Oriented Analysis and Design (OOAD) software engineering methodology was adopted for the design and development of the proposed security framework because, OOAD focuses on modeling a system by collecting concerned objects, and each encapsulated with its own data and behavior. OOAD would enable the creation of a modular, maintainable, and scalable solution for the required result. In the context of IoT security, objects represent different components of the IoT system such as; devices, gateways, servers, and, users. The actors include administrators, end-users, and external systems, which communicate with the IoT devices. Various cases related to security in the IoT environment are used to secure device onboarding, data transmission encryption, firmware updates, access control, and, more.

Security Requirements are defined to include the level of encryption needed, authentication mechanisms, authorization protocols, and, etc. Security-related objects interact with other objects in the system sequel to how the encryption module interacts with data transmission components, and authentication interaction with user management, etc.

Security design patterns such as the singleton pattern for managing encryption keys were utilized with respect to relevance to security, while observer pattern is used for monitoring security events, or the Strategy pattern for selecting encryption algorithms. The data flow model permit sensitive data through the system to determine where encryption and decryption occurs. The flow involve encryption at the device level, secure communication between devices and gateways, and encrypted storage on servers.

**Cryptography and Steganography**

**Cryptography:** involves the use of algorithms to convert plaintext data into unreadable ciphertext. In the context of IoT, where a diverse range of devices communicate over networks, sensitive data like personal information, health data, and, financial data, are exchanged.

**Steganography:** Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination Kespersky (2023). In an IoT context, steganography can be used to covertly transmit sensitive information between devices or to a central server. Doing so, adds an extra layer of security which make it difficult for attackers to detect the presence of hidden messages. Embedding Algorithms are used to implement steganography. Although different steganography algorithms exist, the Least Significant Bit (LSB) algorithm is the most commonly applied method for implementing steganography. The LSB algorithm performs the embedding operation of message along with the image file where each pixel has a size of 3 bytes.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

Cryptography and steganography play crucial roles in building a web-based system for encrypting Internet of Things (IoT) environments. The combination of both techniques would provide greater assurance of data security, privacy, and integrity in IoT applications, which usually involve a multitude of interconnected devices that collect, transmit, and process sensitive information.

IoT devices transmit data over networks, and thus, making them susceptible to interception and tampering. Cryptography provides mechanisms for securing data during transmission by encrypting data, such that even if intercepted during transmission, the data remains indecipherable without the proper decryption key, thereby maintaining data integrity and preventing unauthorized data access.

Cryptography and steganography do not only protect against unauthorized access, but ensures data integrity. When data is transmitted from an IoT devices to a central server or to other devices in an IoT ecosystem, cryptographic techniques like hashing and digital signatures can be employed to verify that the data were not been altered in transit. Thus guarding against data manipulation or corruption. Different devices IoT environments require different levels of authorization, cryptography therefore, helps to build a robust authentication system through which devices prove their identity by using cryptographic keys. This is way to ensure prevention unauthorized device and data accesses access by illegitimate device or user. Cryptography ensures that data remains encrypted and incomprehensible even when the communication is intercepted without the proper decryption keys.

## THE CRYPTO-STEGNA FRAMEWORK MODEL

The hybrid system combined two different data hiding techniques, which are Cryptography and Steganography to encrypt messages in and IoT environment. Message encryption is followed by a modified LSB technique, which is used to embed the encrypted information in an image. The technique therefore, combines the features of both cryptography and steganography and provides a higher level of security. When cryptography, and steganography combined, a significant robust and secure web-based system of encrypting IoT environments is secured. The CRYPTO-STEGNA IoT security framework is derived from a combination of crypto and steganography technics hybridized to work hand in hand concurrently to secure an IoT environment. The protection of sensitive data, thwarting of unauthorized access, provision of data integrity between IoT devices to a proffer a trustworthy IoT ecosystem can be achieved with the design of the Crypto-Stegna IoT security framework.

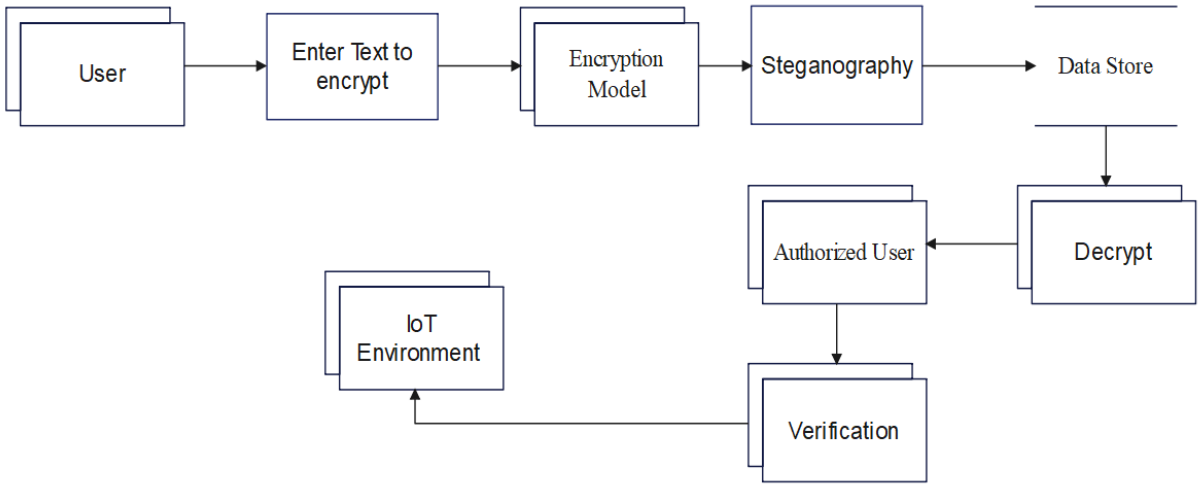


Figure 2. The Dataflow Diagram of the Proposed IoT Security Framework

## THE CRYPTO-STEGNA IoT SECURITY FRAMEWORK

A framework is a conceptual structure or design to guide the build or extension of a structure.

The CRYPTO_STEGNA framework is a security design of an encryption system to secure an IoT environment. The aim of the CRYPTO-STEGNA framework combine **AES-RSA algorithms** for message encryption and decryption to provide the security of messages or data in an IoT ecosystem in a record time, using harsh key encryption models. The CRYPTOSTEGNA framework was implemented by applying AES and GMC algorithms alongside the flask framework of python programming language.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

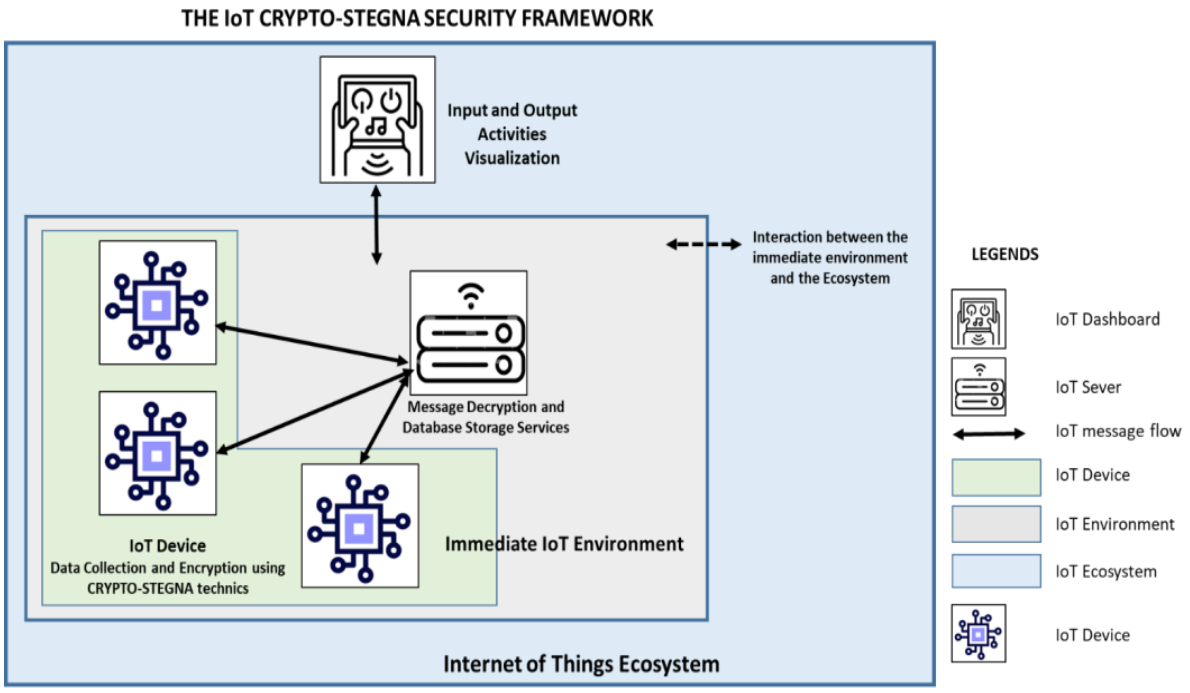


Figure 3. The CRYPTO-STEGNA security framework Systematic model

The Encryption and Decryption of data is done using symmetric or asymmetric encryption keys to secure communication between an IoT device and a central server. The CRYPTO-STEGNA framework design uses a secure key exchange protocol to establish secure connections and exchange keys.

**Data Collection and Processing:**
IoT devices collect data from sensors or other sources, process the collected data to extract relevant information.

**Message Encryption on IoT Device**
IoT devices such as sensors, smart phones, and etc. collects and processes data, which is followed by data encryption to established encryption key. The AES (advanced Encryption Standard) encryption and the GCM (Galosi/ Counter Mode) block cipher mode symmetric key cryptography algorithms are implemented on the IoT hardware devices to achieve a secure data confidentiality and integrity operation.

**Message Decryption**
The central server receives encrypted data from IoT devices, and decrypt the data using the corresponding decryption key. The verification of data integrity is done by checking message authentication codes (MACs) if required.

**The Data Storage and Database:**
A secured database in the data storage system receives, decrypt and stores data within the IoT ecosystem. Proper database security practices, such as access control and encryption algorithms are implemented to protect the data at rest.

**Data Visualization:**
Data visualization is done via the web-based dashboard interface through which users' access and visualization of the IoT data. Data visualization libraries such as D3.js, Chart.js are used to generate graphs, charts, and other visual representations.

**The Dashboard:**
An IoT dashboard the user interface within an IoT ecosystem or platform, through which a user can monitor and interact with the connected devices in the forms of graphs, charts, images, and other UI elements.

**Program Module Specifications:**
The program specification module of the system is divided into two as follows:

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024
DOI: 10.17148/IJARCCE.2024.13101

**The Encryption Module:**
The Encryption Module is responsible for encrypting sensitive data before transmission, thereby ensuring data confidentiality and security. The encryption module is embedded in an IoT device using

**Input Requirements and Outputs of the Encryption Module:** The inputs requirements of the encryption module are Plain text data (string), while the output is an encrypted data string.

**Functions:** The function of the encryption module is to generate encryption keys as string outputs even when no inputs are made.

**Decryption Key Generation:**
**The Generate_key()**: is used to generate a symmetric encryption key for crypto plaintext.

Input: No inputs are required to generate an encryption key (string) as Output

**The Encrypt_data (data, key)**: Encrypts the input data using the generated encryption key.

The input here refers to the data, which is to be encrypted (string), Encryption key is the generated string by the Generate_key.

The Output is the resultant Encrypted data string.

**The Crypto Decryption Module:**
**Crypto Description:** Decryption is the conversion of an encrypted data back to its original form by the decryption module. Generally, decryption is the reversal of encryption. The Decryption Module exists in the storage system, and is responsible for decrypting the received encrypted data back into its original form as sent from a receiver to a destination (user). The decryption is done using an RSA asymmetric standard algorithm to generate a decryption_key (string).

**Specifications:** Input specification requirements of the decryption module are; the encrypted data (string) and the encryption keys (string) to produce a decrypted data (string) as output.

**Functions:**

**Decrypt_data(encrypted_data, key)**: Decrypts an encrypted data using the resultant encryption key generated by the encryption module.

Input: Encrypted data (string), Encryption key (string)
Output: Decrypted data (string)

**The CRYPTO-STEGNA Algorithm**

**Crypto Encryption module**
1. **Input:**
a. IoT data to be secured (**iot_data**)
b. Encryption key (**encryption_key**)

2. **Encryption process:**
encrypted_data = encrypt(iot_data, encryption_key)

3. **Output:**
a. Encrypted IoT data (**encrypted_data**) **Steganography module:**

1. **Input:**
a. Encrypted IoT data (**encrypted_data**)
b. Carrier medium (e.g., an image) for steganography (**carrier_medium**)

2. **Steganography process** steganogram = hide_data(carrier_medium, encrypted_data) The **hide_data** function embeds the encrypted IoT data within the carrier medium using steganography techniques.

3. **Output:**
a. Steganogram (**steganogram**) **Decryption:**

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

1. **Input:**
a. Steganogram (**steganogram**)
b. Decryption key (**decryption_key**)

2. **Steganography Extraction Algorithm:**
extracted_data = extract_data(steganogram)

3. **Decryption Algorithm:**
decrypted_data = decrypt(extracted_data, decryption_key)

The **decrypt** function uses the decryption key to decrypt the extracted data, revealing the original encrypted IoT data.

4. **Output:**

a. Decrypted IoT data ( **decrypted_data** )

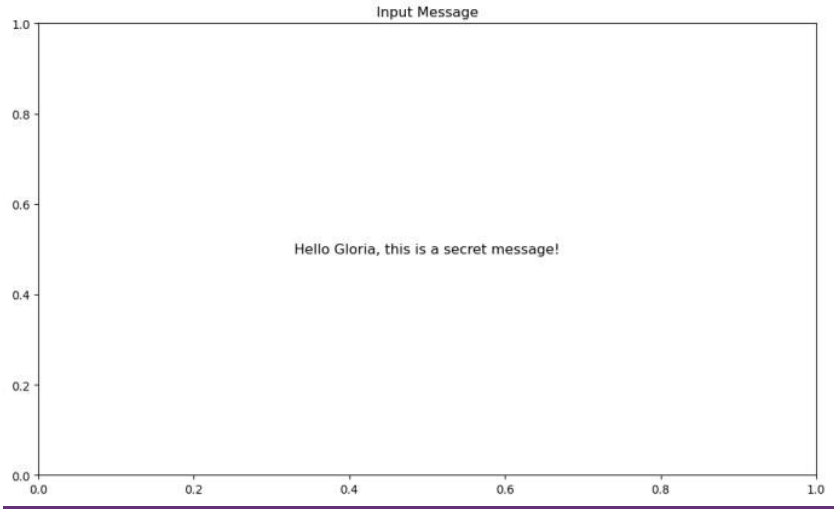


Figure 4: Message to be encrypted

## VII. RESULTS AND DISCUSSIONS

Testing to visualize the time taken for the hybrid model to encrypt and decrypt text files were carried out using various text (string) inputs. The visualization results were present in the forms of bar charts and a line plots.

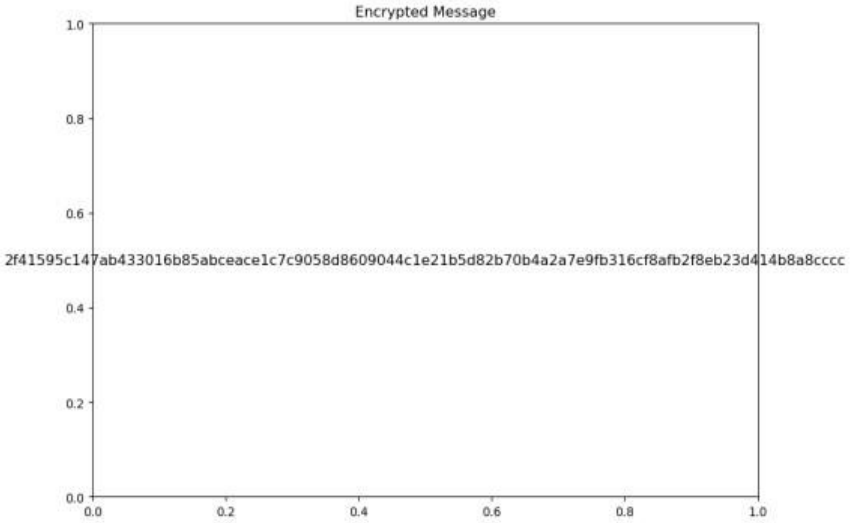


Figure 5: Encrypted message

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

| Input Text (String) | Byte Size (Bytes) | Encryption Time (Sec) | Decryption Time (Sec) | Outpur Text (String) |
|---|---|---|---|---|
| Hello, Gloria | 15 | 0.0000 | 0.00010 | Hello, Gloria |
| "How are you doing | 18 | 0.0000 | 0.0010 | "How are you doing |
| welcome to Unizik Msc | 19 | 0.0000 | 0.00010 | welcome to Unizik Msc |

Table 1. Evaluation of Hybrid CRYPTO-STEGNA MODEL

The test result in the table showed that the CRYPTO-STEGNA framework when applied in an IoT environment could encrypt 17.33 bytes of string data (messages) sent between IoT devices in 0 seconds, and decrypt same data in average time of 0.0010 seconds. The test imply that

**Performance Evaluation**

The system performance evaluation of encryption, decryption time on each of input text was carried out using the sample data shown in the table 1 above. The figure 4 presents the bar chart of the performance evaluation of the CRYPTO-STEGNA IoT security framework model.

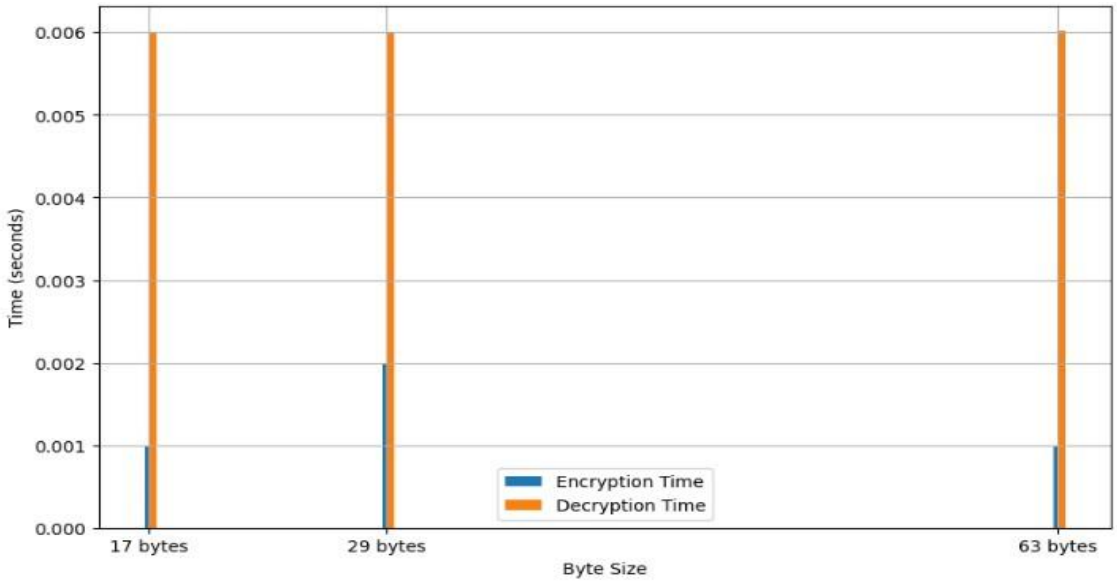


Figure 4. The CRYPTO-STENGA Framework Evaluation Performance

**Documentation**

Flask is a template for building simple webpages. The Flask documentation provides comprehensive guidance on implementing encryption within an Internet of Things (IoT) environment using the Crypto model. The model seamlessly integrates cryptographic functionalities into Flask applications, ensuring data security and privacy in IoT systems. By leveraging the Crypto model's suite of encryption algorithms, key management techniques, and secure communication protocols, developers can effectively safeguard sensitive information transmitted between IoT devices and backend servers. The documentation offers step-by-step instructions, code samples, and best practices to enable Flask-based IoT applications to establish secure end-to-end communication, protect against data breaches, and mitigate potential security threats, thereby fostering trust and reliability in IoT deployments.

Encrypting IoT (Internet of Things) environments is crucial for ensuring data security and maintaining the privacy of users. Here are four application areas where encrypting IoT environments is essential:

1. **Data Privacy and Confidentiality:** Prevents unauthorized access to data by malicious actors or unauthorized parties, protecting users from identity theft, fraud, and other privacy breaches.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024
DOI: 10.17148/IJARCCE.2024.13101

2. **Device Authentication and Access Control:** Encryption can be used to establish a secure and authenticated connection between IoT devices and networks, preventing unauthorized devices from gaining access.

3. **Secure Communication Networks:** IoT devices often communicate over various networks, including Wi-Fi, cellular, and Bluetooth. Encrypting these communications prevents eavesdropping and man-in-the-middle attacks.

4. **Industrial IoT (IIoT) and Critical Infrastructure Protection:** In industrial settings, where IoT devices monitor and control critical infrastructure (e.g., power plants, factories, transportation systems), encrypting data and communications is vital.

## VIII. CONCLUSION

A web-based system for encrypting IoT environments using Python and the Flask framework could improve device security and privacy by integrating a Crypto model and Steganography techniques. This initiative addresses growing concerns about data breaches and unauthorized access in IoT deployments. A strong Crypto model encrypts sensitive data sent between IoT devices and the web application, making it unreadable to unauthorized parties. This cryptographic layer protects against eavesdropping and data tampering, enhancing system integrity. By hiding encrypted data in innocent-looking digital media, Steganography strengthens the security infrastructure and prevents attackers from discovering it. As IoT grows, security vulnerabilities increase, requiring proactive measures to protect sensitive data and user privacy. This integrated approach addresses these issues and enables future IoT ecosystem security advances. However, security requires ongoing updates and maintenance to adapt to changing threats. Crypto model and Steganography in a Python and Flask-based web system provide a holistic solution for IoT security. This approach aligns with the growing focus on cybersecurity and shows how interdisciplinary approaches can solve complex technological problems. Prioritizing security measures can enable widespread adoption of IoT technologies with confidence in their resilience to emerging threats.

## REFERENCES

[1]. Al-Fuqaha, Guizani, Mohammadi, Aledhari and Ayyash (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4):2347–2376.
[2]. Assari and Almagwashi (2018) A multidisciplinary systematic literature review on frailty: Overview of the methodology used by the Canadian Initiative on Frailty and Aging. BMC Med. Res. Methodol. 2018, 9, 68–72.
[3]. Barki and Gharout (2016) Enabling end-to-end coapbased communications for the web of things. Journal of Network and Computer Applications, 59:230–236
[4]. Chandra et al., (2018). Requirements engineering and management for software development projects. Springer Science & Business Media.
[5]. Dhanvjay and Patil (2019). S.O. Integration of Network science approaches and Data Science tools in the Internet of Things based Technologies. In Proceedings of the 2019 IEEE Region 1 Symposium (TENSYMP), Jeju, Korea, 23–25 August 2019; pp. 1–6. https://doi.org/10.1109/tensymp52854.2021.9550992.
[6]. Doukas et al., (2012). Secure design patterns. Technical report, CARNEGIE MELLONUNIVPITTSBURGH PA SOFTWARE ENGINEERING INST
[7]. Durga et al., (2022) H. Cyber security Issues in Internet of Things and Countermeasures. In Proceedingsofthe2018IEEE International Conference on Industrial Internet (ICII), Bellevue, WA, USA, 21–23 October 2022; pp. 195–201.
[8]. Kaspersky (2023). What Is Steganography & How Does It Work? https:// www. kaspersky.com. Retrieved on October, 30th 2023.
[9]. Makhdoom and Abolhassan (2019). A critical analysis on the security concerns of internet of things (IoT). Int. J. Comput. Appl. 2019, 111, 1–6.
[10]. Mislolavskaya and Tolstoy (2019). Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. Futur. Gener. Comput. Syst. 2019, 82, 274–289. https://doi.org/10.1016/j.future.2017.12.009.
[11]. Monteiro and Silva (2016) "ASIC-oriented comparative review o f hardware security algorithms for internet of things applications", Microelectronics (ICM), 28th International Conference on. IEEE
[12]. Morin, Harrand and Fleurey (2017). Model-based software engineering to tame the iot jungle. IEEE Software, 34:30–36. SIG (2017). Common vulnerability scoring system sig.
[13]. Rayes and Mohammadi (2015) "Security and privacy in Internet o f things: methods, architectures, and solutions", Security and Communication Networks 9.15: 2641-2642.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13101

[14]. Routh and Pal, (2018) "ZeroCrossing Analysis o f Levy Walks and a DDoS Dataset for Real-Time Feature Extraction: Composite and Applied Signal Analysis for Strengthening the Internetof-Things Against DDoS Attacks," International Journal of Software Science and Computational Intelligence (IJSSCI) 8.4, 1-28.

[15]. Shahid and Thiemo (2010) “Real time intrusion detection in internet o f things, Ad-Hoc networks", 11(8), 2661-2674.

[16]. Sezer, (2016). Cache Freshness in Named Data Networking for the Internet of Things. Comput. J. 2018, 61, 1496–1511. https://doi.org/10.1093/comjnl/bxy005.

[17]. Standford, (2018) "Protection of ECC computations against side-channel attacks fo r lightweight implementations", Verification and Security Workshop (IVSW), IEEE International. IEEE

[18]. Soullie, (2014) “Construction and strategies in IoT security system, Green computing and communication (GreenCom) ", IEEE and Internet of things, IEEE international conference on and IEEE cyber physical and social computing, pp. 1129-1132, 20-23 August 2014.

[19]. Perera et al., (2014) "Taxonomies for Reasoning About Cyberphysical Attacks in IoT-based Manufacturing Systems", International Journal of Interactive Multimedia & Artificial Intelligence 4.3