

Evaluation of Advanced Information Security Scheme in Internet of Things Environment for Intelligent Monitoring Applications

Mohamed I. Gaber^{*a}, Ashraf A. M. Khalaf^b, Imbaby I. Mahmoud^c, Mohamed S. El_tokhy^a

^A Engineering and Instrumentation Department, NRC, Egyptian Atomic Energy Authority, Egypt.

^b Electric Communications and Electronics Department, Faculty of Engineering, Minia University, Egypt.

^c National Center for Radiation Research and Technology, Egyptian Atomic Energy Authority, Cairo, Egypt.

*Corresponding Author: Mohamed I. Gaber [doctor_moh_2020@yahoo.com]

ARTICLE DATA

ABSTRACT

Article history:

Received 19 Sep 2023

Revised 09 Dec 2022

Accepted 09 Dec 2022

Available online

Keywords:

Secure Monitoring,
Steganography, Internet of
Things, Cryptography, AES,
RSA, Nuclear Facilities

In recent years, the Internet of Things (IoT) technologies have been developed to make great progress for nuclear energy applications. These applications require advanced schemes to secure sensitive information from incremental attacks and sabotage processes. The schemes should meet the major security attributes, including confidentiality, availability, and integrity. This paper introduces an information security scheme for transmitting sensitive information with secure monitoring of the critical radiation levels at nuclear facilities. It is evaluated by integrating the cryptography and steganography techniques with cloud computing services. The cryptography techniques are based on Advanced Encryption Standard (AES) and Rivest, Shamir-Adleman (RSA) algorithms. The scheme uses the extracted cryptography keys from authenticated biometric attributes and is suitable for emergencies through a low computational time. It allows securing access for encrypted sensitive measurements, files, and images with high data integrity and confidentiality.

Furthermore, it hides confidential, sensitive information with great Capacity and imperceptibility through the transmitted carrier images. The security performance analysis ensures the robustness of the introduced scheme against various attacks through authentication, encryption, and information-hiding techniques. Finally, the paper discusses the resistance of the introduced scheme against serious attacks such as the man in the middle, noise, and Distributed Denial of Service (DDOS) attacks.

1. Introduction

Internet of Things (IoT) systems have suffered from many hacking attacks. They are the main source of threats in all computerized systems. These threats force the researchers to introduce efficient security frameworks and techniques. These attacks influence the shared sensitive information through undesired actions from third parties. They can steal or modify the information from unauthorized access. In addition, they hope to destroy any smart system within the applications. The risk of any information leakage is very serious, especially at nuclear facilities. It may lead to different sabotage actions through unauthorized access to sensitive nuclear information.

Consequently, information systems, especially those that belong to nuclear facilities, are suffering from serious attacks. One of these more serious attacks is Stuxnet. It greatly affects the operation of nuclear facility systems, especially instrumentation and control systems.

Internet of Things (IoT) technologies can be efficiently used in nuclear energy applications. These applications may include nuclear power plants, accelerators, and radioactive isotope manufacturing units. Detecting the presence of radiation levels in critical infrastructures or locations through the developed radiation monitoring devices and systems is crucial. The critical infrastructures, including nuclear facilities, seaports, borders, and even hospitals, are equipped with radiation-monitoring systems. They require an efficient information protection scheme for sensitive information and monitoring measurements. Information security uses multiple protection layers to prevent continuous, serious attacks.

The defense-in-depth technique uses various protection levels to mitigate security attacks and threats. If any protection level fails to prevent the attack, the later protection level would be available to activate the mitigation protection algorithms. It ensures the robustness of any information protection system against different threats by using sequential security barriers. Sensitive information assets contain the components that store, process, and control sensitive data. It can be included in control systems, computer networks, and information systems. The proposed security scheme can target these systems for secure sensitive information transmission. Table 1 illustrates some typical systems with sensitive information regarding nuclear facilities and the impacts of missing information security attributes. It investigates the effects of missing confidentiality, availability, or integrity on the facility. It contains some of the systems found at a nuclear facility with the potential impacts of successful attacks. Depending on the objectives of an attack, the attacker may try to exploit the different system vulnerabilities and raise the attack surfaces. Such attacks can lead to loss of confidentiality through unauthorized access to the information and loss of integrity from the interception and change of information, software, and hardware.

Remote monitoring systems depend on the internet to monitor the detected measurements of physical parameters. Implementation of smart applications requires solving serious security challenges regarding secure control processes. These applications are highly vulnerable to security attacks through Internet connections. Therefore, they need an information protection level to secure the sensitive and private information regarding the monitoring environments. The attackers always try to exploit any weak point in the designed application through any of the network vulnerabilities.

TABLE 1: Typical systems of one nuclear facility with sensitive information

System	Impacts on information security	Impacts on the facility
Facility protection system	Loss of integrity and availability	Critical Plant safety compromised
Process control system	Loss of integrity of control data Loss of function availability	High Plant operation compromised
Physical access control system	Loss of availability and integrity of site access systems	High Access is given to unauthorized persons.
Documentation management system	Loss of confidentiality, availability, and integrity of data	Medium Information used to plan More severe attacks.

2. Related Work

In recent years, the development and evaluation of information security schemes have motivated researchers' interest in implementing intelligent, secure IoT applications. So, several research papers have been found to study and analyze various IoT security schemes to protect shared information against threats. For example, the authors of [1] apply common cryptographic algorithms to introduce a comparative analysis using symmetric and asymmetric encryption techniques. These techniques can protect the transmitted data cloud based applications and services. They ensure the advantages of using RSA and AES encryption algorithms over others through the difficulty of getting the generated private key.

In the literature [2], the authors propose three information-hiding techniques. It is based on the deeper layer of image channels with minimum distortion in the Least Significant Bit (LSB). Also, it provides secure communication in critical IoT environments through steganography techniques. The proposed techniques were evaluated mathematically and experimentally to verify their ability to hide secret information from any intrusion. It showed better imperceptibility and Capacity than the other existing techniques, with higher robustness to different attacks.

The authors in [3] introduce a radiation monitoring scheme that uses geo-tagged IoT devices to measure the radiation levels in radiation environments. They use the authenticated cloud server for monitoring the detected values. The scheme can detect the high values and provide alarms with alert messages to the concerned authorities. However, they weren't interested in the security issues of applying data protection techniques. The detected measurements weren't secure, and the devices didn't follow authentication procedures. It was noticed in [4] that the authors present a high information protection scheme for securing diagnostic text data in medical images. They use a combination of Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA) encryption techniques to integrate the 2-D Discrete Wavelet Transform (2D-DWT) steganography technique. The scheme uses color and greyscale images as cover images to hide different text sizes. It starts by encrypting the text data to hide the result in a cover image using a 2D-DWT steganography technique. The evaluation results ensure the scheme's flexibility to hide the medical data into a transmitted cover image with high imperceptibility, Capacity, and minimal deterioration in the received stego-image with high robustness to different attacks.

In [5], the authors proposed an intelligent and secure health monitoring scheme based on cloud computing and cryptography techniques with an IoT environment. It provides authentication monitoring for the elder health data through digital envelope, digital certification, signature, and timestamp mechanisms. These mechanisms provide efficient medical service and suitable actions in emergencies. They protect the biological monitoring data and inspection reports to secure the medical records with authenticated access. The proposed scheme presents robustness against replay attacks and man-in-the-middle attacks with secure data in a cloud environment. As a result, the elders are not worried about their medical records.

The authors in [6] present a study of vulnerability analysis and attack cases in a nuclear facility. This attack is executed on the reactor to target the radiation monitoring system. It hacks the transmitted data to control the emergency siren system. So, it ensures the importance of encrypting the transmitted data and authenticating the assigned messages. They present a checklist with an assessment of the cyber security items. These items ensure efficient security techniques for wireless communication in nuclear facilities. It aims to prevent unauthorized access to monitoring data and common attacks, including Denial of Service (DOS) and brute force attacks. It authenticates the accessing devices to the wireless network and provides sufficient data protection.

In [7], they proposed an encryption-watermarking technique for embedding speech signals into digital images. It encrypts the watermark before embedding it into the cover image through a secure watermarking technique. They use the Arnold Cat Map for encrypting the watermark. The proposed technique introduces a powerful image analysis tool with fast and efficient implementation. Hence, it enhances the quality of a

reconstructed speech signal regarding the acceptable values of SNR and PESQ after watermark extraction and decryption. The obtained results show the robustness of their technique against three types of attacks: JPEG compression, Median, and additive White noise Attacks.

As a result of this survey, the main contributions of this work are three domains (levels). The first is the discussion of the proposed architecture, which permits remote monitoring of the radiation levels at the corresponding nuclear facility. It is based on aggregated sensed data, which are periodically processed and transmitted to cloud servers through security-applied attributes. These attributes aim to protect the sensed data from threat attacks for taking suitable actions in emergencies. The second one is the proposed security platform, which targets sensitive data, especially regarding nuclear facilities. This sensitive data may include compiling sensed data of specific physical parameters or text files and images, as the risk of accessing the sensitive data by unauthorized parties is very high if it is unencrypted and hidden.

Furthermore, these security mechanisms may guarantee the main security challenges, including confidentiality, integrity, and availability. The third is discussing applying the proposed scheme during emergencies and considering the requirements of fast response actions. The scheme consumes little time to execute the security techniques for solving the issues concerning emergency operating conditions in critical infrastructures. In addition, it can also be suitable for other applications that require monitoring schemes with secure data transmission.

The paper is divided as follows. The security risks with their mitigation scenarios are presented in Section 2. Section 3 explains the proposed scheme, including monitoring and information security models with cryptography and steganography techniques for securing the monitoring data. Section 4 presents the information security platform's system development and performance analysis, including the emergency management scenario. Section 5 presents the evaluation results with mitigation approaches for serious security attacks. Finally, section 6 concludes the presented work.

3. Security Risks and Mitigation Scenarios

The information security scenarios are essential through the rapid development of the fourth industrial revolution (Industry 4.0) and artificial intelligence methods [8]. The generated amounts of data meet the demand for careful authentication and encryption techniques. Artificial intelligence (AI) techniques are considered one of the most promising methods for addressing cyber security threats and providing security [9], [10]. Figure 1 presents the serious security risks and their mitigation scenarios in radiation monitoring systems. It illustrates the weakest points concerning the security risks that may attack many IoT communication layers. The risk of sensitive information leakage and unauthorized access to the system is the most serious. Thus, strong information encryption and hiding techniques are required to be deployed in the information transmission points. A strong authentication procedure is required in all access points, such as the IoT gateway, smartphone application, and the main system accessing panel. These mitigation scenarios aim to present a strong robustness against the most serious security attacks.

Also, information security aims to protect the transmitted sensitive data through any information assets such as networks, instrumentation and control systems, and physical access systems. Secure information systems can achieve the main security attributes, including confidentiality, availability, integrity, and authentication. They protect sensitive data and secure keys from any of the different attacks. The proposed

scheme aims to monitor the radiation levels in any environment and upload the information to cloud servers through secure information transmission.

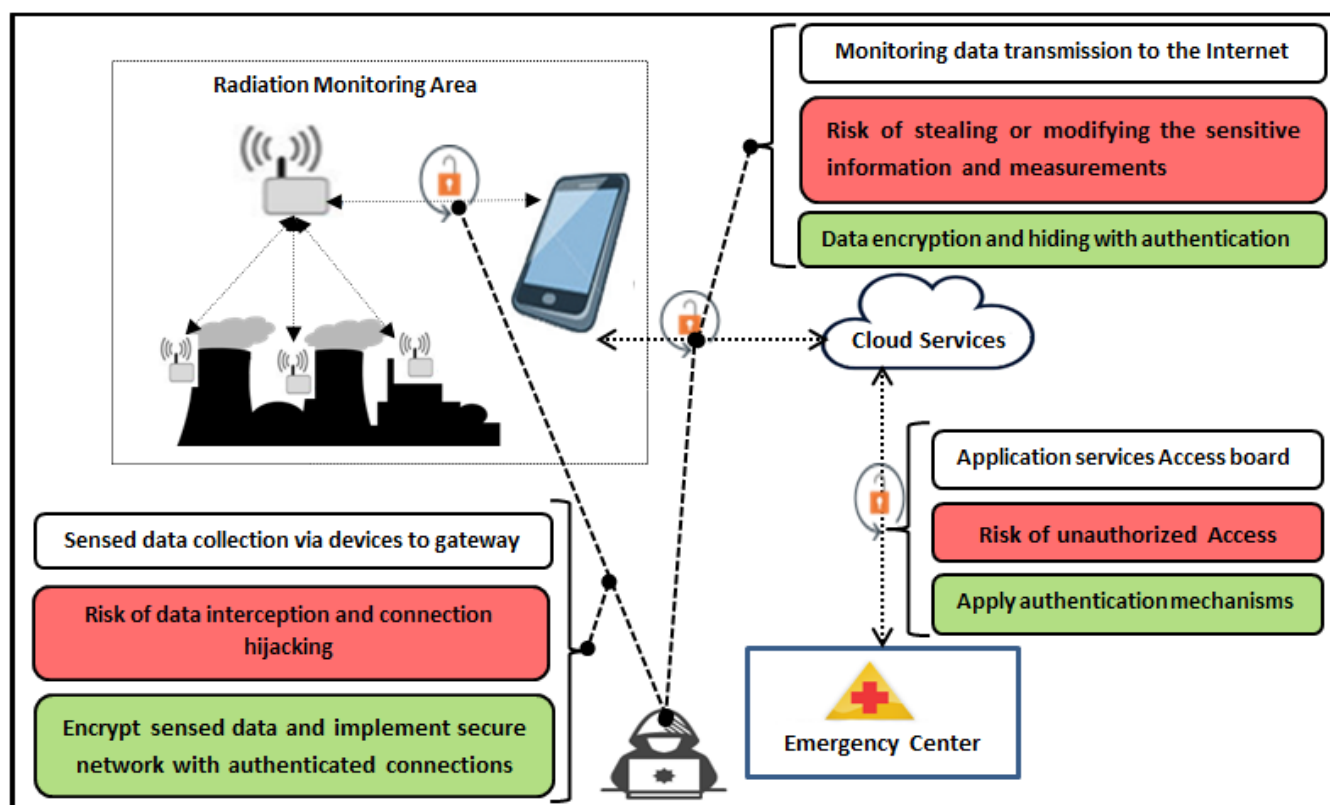


Figure 1 Serious security risks and mitigation approaches for the proposed monitoring architecture.

4. The proposed protection scheme for information monitoring

The proposed architecture is divided into three domains, as shown in Figure 2. The first domain is the sensing and networking domain. It contains a collection of distributed IoT devices for aggregating the sensed measurements at the nuclear facility. The first domain includes a smart mobile device or tablet with a specific International Mobile Equipment Identity (IMEI) with Bluetooth and Wi-Fi connectivity. Internet gateway can provide the connectivity to internet providers. IoT environment is built through the connectivity of sensing devices with Bluetooth beacon and a smart mobile phone device [11]. It can locate the monitoring areas with a Global Positioning System (GPS) to help in emergencies. In addition, the connectivity can depend on the wireless networking of Wi-Fi for wide-range connection with an anti-jamming technique [12].

The second domain is a security domain. It contains a Key Generation Unit (KGU), which launches private and public keys for the cryptography techniques. The key generation unit considers a main confident party that extracts the cryptography keys from the biometric attributes for use in the proposed information security model. It authenticates the detected biometric attributes regarding the authorized operators through authentication information at the cloud servers. Key generation time and date are stored in the cloud servers and shown on the corresponding cloud dashboard. Secure information transmission routines can be a big challenge to introduce 5 G services and IoT applications [13].

All the parties are connected through an authenticated network with unique IP addresses. Also, it contains the cryptography and steganography platforms through an implemented Graphical User Interface (GUI). The third domain includes an emergency center with IoT application services. The emergency center will receive alert SMS messages if the sensed measurements exceed the threshold level. Hence, it launches

the emergency rules. IoT application services authenticate the cloud servers with other parties to get the sensitive measurements and reports for normal and emergency monitoring situations.

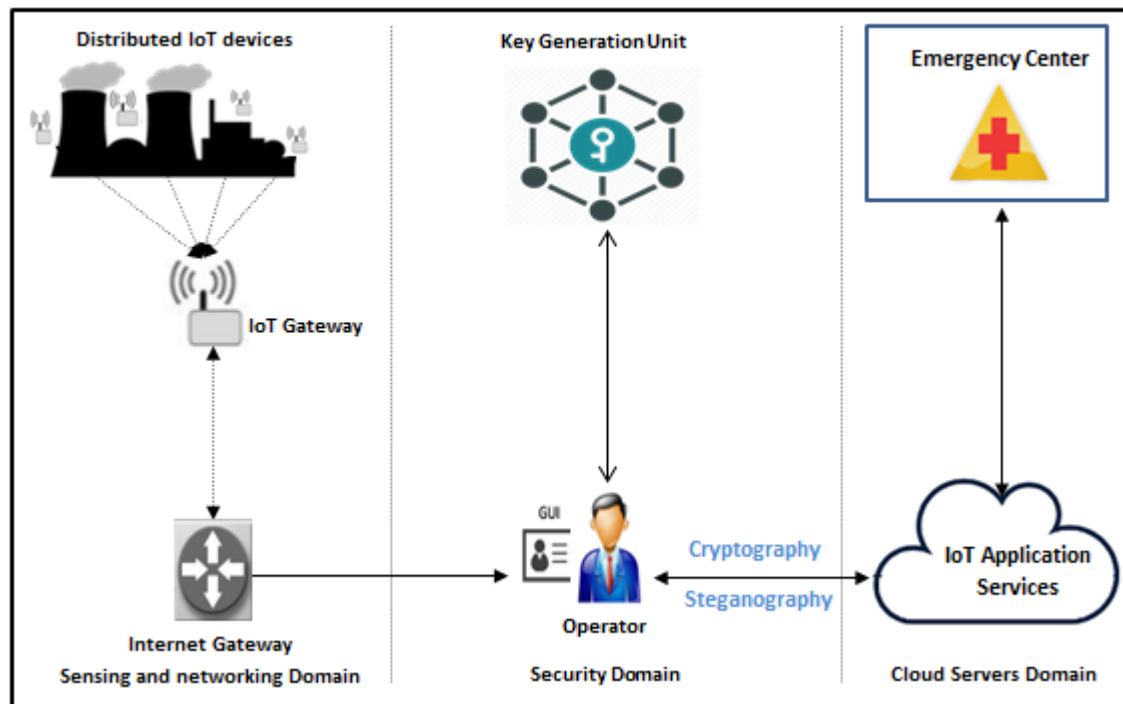


Figure 2 Proposed scheme architecture for secure remote monitoring system

4.1 Biometric Security Keys Extraction

The Key Generation Unit (KGU) is responsible for issuing the public and private encryption keys after registering the assigned parties. It distributes the extracted encryption keys for the cryptography and steganography techniques. The security information may include authorization identity information launching public and private keys. The authentication of operators is performed by adding two parameters to all of their API requests. These parameters are API credentials with API_User and API_Secret, as shown in Table 1, appendix A. Both parameters are strings and provided in the cloud account information. The strength of information security techniques depends on the encryption key to make the revelation of it as difficult as possible. As shown in Figure 3, it illustrates the extraction process of encryption keys from biometric attributes. It uses the captured images from a high-resolution camera to get the specific attributes regarding included image faces and quality. The programming script uses the authentication information of API credentials to authenticate the extracted feature attributes. Appendix A, Table 2 shows the samples of extracted features from any detected face and image quality attributes [14].

The applied Application Programming Interface (API) through a cloud server is flexible, fast, accurate, and scalable to get authenticated attributes for key extraction. It provides easy integration with consistent moderation decisions through a simple programming script. Also, it guarantees high privacy with authenticated biometric attributes far from any third parties [16].

The generated keys are stored on cloud servers and can be used as an information security platform with an applied hashing function. Biometrics attribute is a strong authentication procedure for operators and information transmission authentication mechanisms.

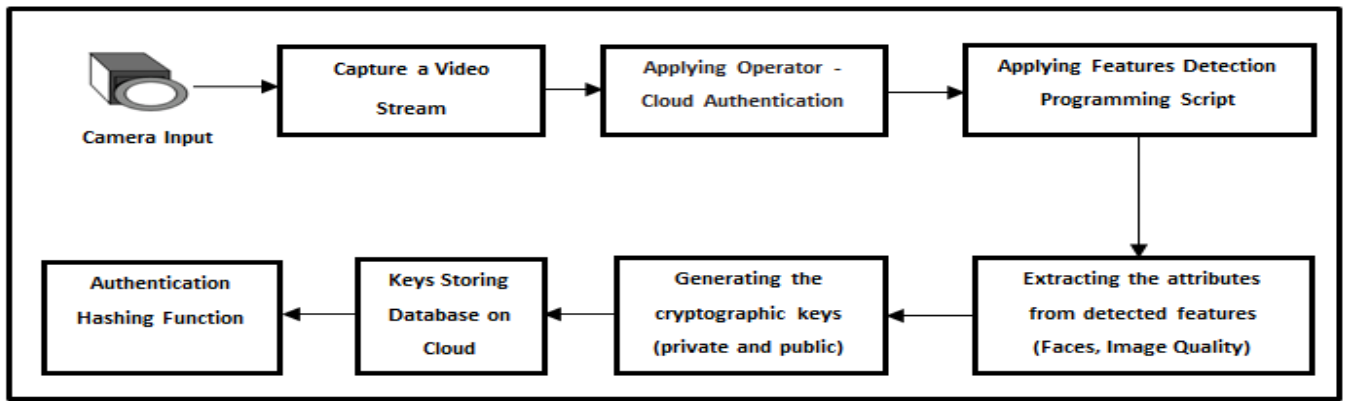


Figure 3 Block diagram of key generation unit

4.2 Applied authentication routine

An authentication function is applied to store the generated keys in hashing form. It replaces the generated key with the hashing one to implement more secure applications. It aims to make the key to difficult recovery secure form. Also, the generated biometric keys can be verified by efficiently matching the hashing units. The applied cryptography scheme requires a fixed-length encryption key. So, the hash function is applied to provide output with a fixed length of a variable length input. The hashing technique (SHA256) is used to provide a 16-byte output and can apply high performance with the AES-256 encryption technique [17] [18]. SHA256 is based on a Hash-based Message Authentication Code (HMAC). It calculates the message authentication code, which specifies the hash function combination with a secret cryptographic key for authentication [19].

4.3 Proposed Monitoring Scheme Sequence Diagram

The communication parties register themselves at the key generation unit in advance via a secure channel. As shown in Figure 4, the secure monitoring scheme is executed in steps. Firstly, the gateway unit gets the sensed measurements from the embedded sensors of distributed IoT devices in different periods. The nuclear facility may include the radiation sensing nodes at the required monitoring areas with a gateway node for sensing information aggregation. Thus, the smart mobile device aggregates the collected data through the dedicated Bluetooth or Wi-Fi connectivity units. In the second step, the operator gets the authenticated extracted biometric keys for the cryptography and steganography algorithms. It encrypts and hides sensitive information, including sensing data, files, and images, through the proposed platform with a flexible Graphical User Interface (GUI).

In the Third step, the application services allow comparing the sensed data with stored threshold values in the system database. Once the detected measurements exceed the threshold values, it will notify the emergency center with SMS messages on the registered phone number at an acceptable time. Then, the emergency center authorities can access the protected information. The fourth step allows sending an acknowledgment to the operator about dispatching the rules and regulations of emergency conditions. However, in normal operation conditions with acceptable sensed values, the detected values are stored in the cloud servers for historian purposes. The monitoring application services aim to secure sensitive information, especially for industrial plants [15].

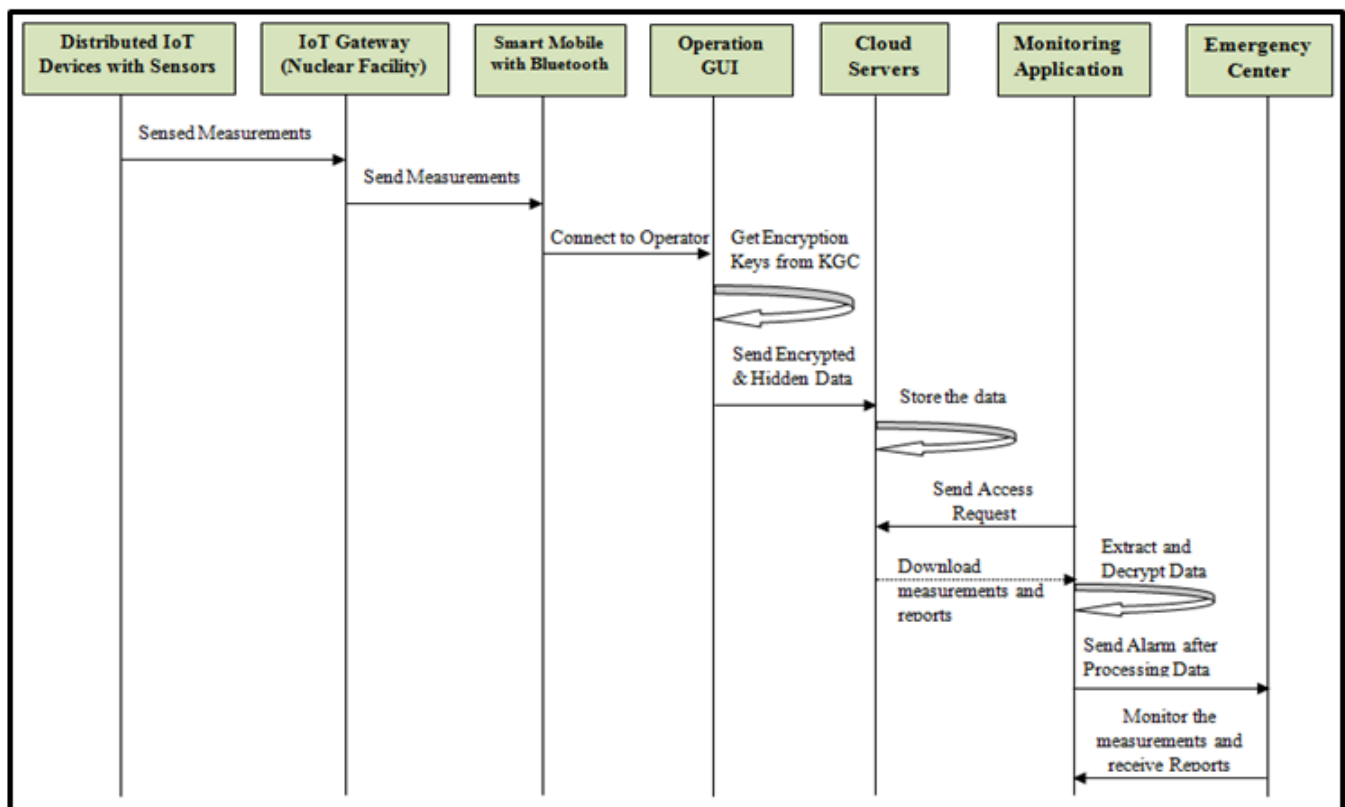


Figure 4 Secure monitoring scheme sequence diagram

4.4 Information Encryption and Hiding Methodology

Information hiding represents one of the main ways to protect sensitive information [20] [21]. Therefore, many information steganography techniques are applied to hide the data. It may use images, videos, or text. Images with various formats are used to hide the information with different capacities [22]. We applied the information hiding technique using the Least Significant Bit (LSB) insertion method. It's based on using RGB color images as carriers for information protection in an IoT environment. The technique hides information in the deeper layer of image channels with minimum distortion in LSB to indicate data [2]. The information encryption technique would protect the sensed measurements before applying the hiding process. Symmetric key encryption algorithm used for information encryption through Advanced Encryption Standard (AES) algorithm. In addition, the reports and images with sensitive information are protected using Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA) algorithms.

The applied steganography technique for encrypting and hiding the data is shown in Figure 5. Firstly, defining the used cover image and the data encryption key is necessary. Symmetric key encryption technique (AES) encrypts the compiled data of detecting measurements. Then, the encrypted data is translated into binary. Secondly, the LSB of each pixel in the cover image is computed and exchanged with each bit of the secret message one by one. Then, the steganography image is launched with encrypted hidden data. For extracting the hidden data, the technique determines the LSB of each pixel in the steganography image to convert each eight bits into character. Then, the generated key is used to decrypt the secret message for deducing the plain measurements. However, the Least Significant Bit (LSB) modification is a very weak approach for digital watermarking. It can introduce a watermarked image without appreciable distortion and enhance the calculated PSNR and MSE values [34].

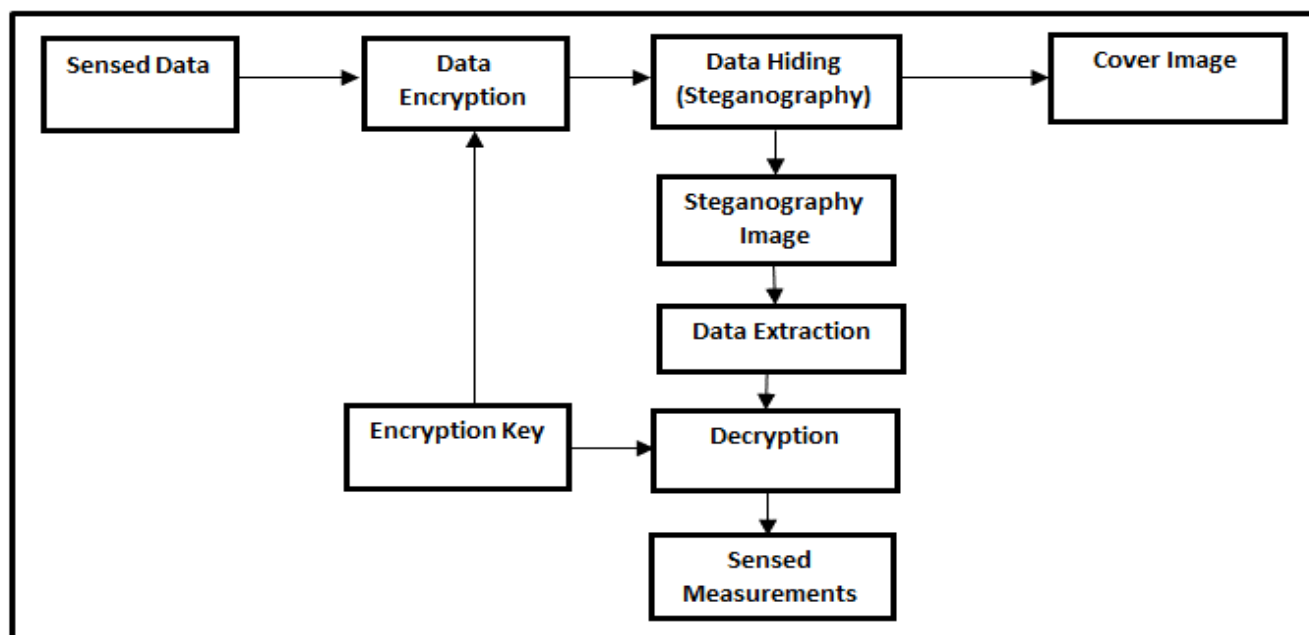


Figure 5 Process diagram of the information encryption and steganography

IoT applications and services require different techniques to secure the shared information. IoT environment may use various resources with limited supplied energy and processing. It needs special information security techniques to enhance the system's performance. These techniques provide high execution time with more efficient performance than the traditional techniques [23]. Advanced Encryption Standard (AES) is a symmetric key cryptography technique for transmitting sensed measurements and text reports with sensitive information. AES is based on principle definitions including substitution-permutation network, combining both substitution and permutation. AES uses the Rijndael cipher, which has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits [24]. The literature analysis showed that the AES algorithm performs the best in terms of encryption performance, flexibility, security, and memory usage. It is deduced that AES eliminates the execution processing time by using a longer encryption key. The AES encryption technique is recommended to achieve major appliance security attributes, including integrity and confidentiality [25]. Rivest, Shamir, and Adleman's (RSA) algorithm is used as a symmetric key cryptography technique [26] for transmitting images with sensitive information. It aims to provide extensive secure attributes for the encrypted transmitted images. RSA uses the extracted biometric attributes as public and private encryption keys. It provides a suitable environment for data transmission within cloud-based applications. The sensitive information is encrypted and stored on the cloud servers. The emergency center or operator can access the data through an authenticated request. RSA algorithm depends on a public key known to all the parties and a private key for the decryption process only. Also, it introduces high-security attributes to the encrypted images. Many heterogeneous devices deployed in the IoT environment make it difficult to detect IoT attacks using traditional rule-based security solutions [27].

5. System Development and Analysis

5.1. Implemented Information Security Platform

Figure 6 shows the information security platform for sensitive information encryption and hiding. It simulates the performance of secure monitoring and transmission of sensed measurements, text reports, and images through encryption and hiding techniques. The platform involves selecting a cryptography key, steganography cover image, and information hiding or extracting options. It determines the execution time for applying the security techniques and sending information to cloud servers.

Figure 6 Information Cryptography and Steganography Security Platform

AES/RSA encryption technique is used to protect the sensitive information of any corresponding facility [28]. Sensed data and other sensitive information can be compiled files for uploading through authenticated terminals. Therefore, our scheme can provide a more flexible and accurate monitoring service. The model compiles the hidden monitored measurements into a file. Figure 7 shows the compiled file with the extracted measurements and sensitive information about any nuclear facility. Cover Images can be color or grey-scale images to hide messages with different sizes.

```

test (1).txt - Notepad
File Edit Format View Help
Sensed Radiation Level in Area A (CPM)= 580.52 CPM
Sensed Radiation Level in Area B (CPM)= 860.71 CPM
Sensed Radiation Level in Area C (CPM)= 350.66 CPM
Sensed Radiation Level in Area D (CPM)= 730.79 CPM
Dose Rate (µSv/h)= 0.29 µSv/h
Feedback of Protection System = True
Feedback of Cooling System = True
  
```

Figure 7 Example of hidden and extracted measurements through the steganography process

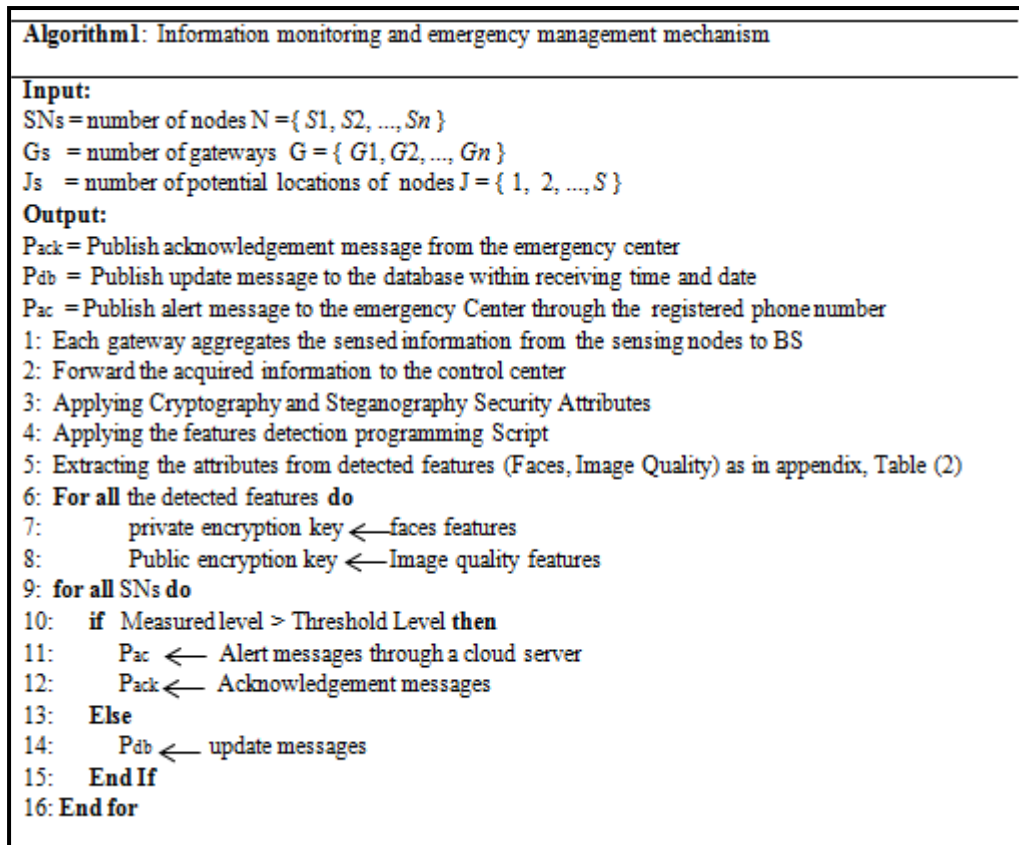


Figure 8 Information monitoring and emergency management mechanism

5.2 Emergency Management Approach

Detection of an emergency is one of the main goals in any monitoring system for responding appropriately [29]. Figure 8 shows the steps of our scheme to detect and monitor the radiation levels within a secure data transmission routine. The flowchart explains the steps of our scheme to detect the sensed radiation levels and send the sensitive information through a secure transmission. At first, the sensed information is collected through the IoT environment's distributed IoT devices and gateways. Then, it is forwarded to the operation unit to apply the information security attributes. These attributes guarantee secure transmission through cryptography and steganography techniques for information encryption and hiding. These techniques are involved in the proposed information security platform. The platform gives a great and simple method to encrypt with hide for critical measurements.

In addition, it can encrypt files and images for sensitive information protection. If the sensed radiation level has exceeded the threshold level, the cloud servers could alert the emergency center with alarm messages on the resisted phone number for monitoring. Hence, the authorities of an emergency center can send the acknowledgments of receiving the alerts to access the monitoring reports and take responding actions. All the received data is stored in the system database for historian's purposes with the receiving date and time. It can be used to monitor the critical measurements at the infrastructures, especially the nuclear facilities. In normal situations, the detected values are below the threshold level. However, in emergencies, the detected values are above the threshold level, and the monitoring system must be very sensitive to any increment that may disturb the operation routine.

After detecting the emergencies, the authorities need to access the sensitive information of system measurements and their effects on the operation of suitable emergency responding actions. They can access the system to get sensitive information and reports at any time from different locations. Therefore, they can launch suitable response actions that prevent any progressive danger regarding the system protection scenarios. All the steps aim to monitor the critical measurements especially regarding the radiation levels at any monitoring area of a nuclear facility from the different radiation sources.

5. Performance Evaluation and Test Results

Security platforms can execute cryptography and steganography operations for all the critical measurements and sensitive information files for secure monitoring. It was performed on an Intel core i3-2370M CPU@2.40 GHz processor using Python programming language tools and open-source libraries. MATLAB is used to evaluate the performance of implementing algorithms through evaluation metrics, including information entropy, imperceptibility, and algorithm execution time. Also, the robustness of our scheme against common attacks is evaluated through security performance analysis.

Information Security platform depends on the following environments:

- Programming language environment: Python
- Software: 64-bit Microsoft Windows 7 Operating system
- Hardware: Laptop with Intel core i3-3230M CPU @ 2.66GHz, 4GB memory, HD Webcam with a resolution of 1366x768 pixels.
- Cloud Environment: Hosted web application server on Infrastructure as a Service (IaaS) systems

5.1. Information Entropy

The security algorithms provide more data than ordinary plain information. It aims to add difficult conditions for the third parties to get the original information. Adding more data can introduce better security performance with higher entropy. Information entropy $E(I)$ refers to the added security information for an image as shown as follows:

$$E(I) = -\sum_{i=1}^L P(I_i) \log_2 P(I_i) \quad (1)$$

Where L refers to the number of grey levels, I_i is the pixel value in the image, and $P(I_i)$ is the occurrence probability of (I_i) , $\sum_{i=1}^L P(I_i) = 1$ [20]. The entropy would be higher if the pixel values were near the uniform distribution. An image that approaches uniform distribution has 256 gray levels with the same occurrence probability. Hence, the optimal entropy value is eight. Table 2 compares the entropies of three tested images as cover and steganography images with many sizes at different hiding capacities.

5.2. Imperceptibility




Information hiding techniques can be evaluated through metrics, including Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), etc. These metrics evaluate the difference between cover and steganography images. The greatest quality can provide higher robustness against attacks through extra imperceptibility with higher hiding accuracy. MSE and PSNR are defined as shown in equations (2) and (3) [2]. The cover image is C , and the steganography image is S with dimensions M and N .

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (S_{ij} - C_{ij})^2 \quad (2)$$

$$PSNR = 10 \log_{10} \frac{C_{\max}^2}{MSE}$$

Where C_{ij} and S_{ij} represent the cover and steganography images pixel values at row i^{th} and column j^{th} position. M and N are the number of rows and columns in the images, respectively. Refers to the highest pixel value in the image. Higher PSNR provides better quality of steganography image regarding the cover image. The results of the above formulas can be used to measure the quality of a steganography process. Simple insertion of the secret message bits into the LSB of the used cover image leads to hiding the information with undetected changes by the human eyes. The highest PSNR provides the greatest image quality and hiding efficiency. Table 2 shows the imperceptibility and entropy for three tested images with different sizes and insertion capacity in bytes. The results deduce the accuracy of information hiding with the highest PSNR and lowest distortion (MSE) with high data capacity.

TABLE 2: The imperceptibility and information entropy metrics for different hiding data capacity and image sizes

Image	Size	Hiding Capacity (bytes)	Entropy		PSNR	MSE
			Cover Image	Steganography image		
Lena 220 x 220		336.56	7.7371	7.7371	82.798	3.421×10^{-5}
Onion 198 x 135		459.54	7.6052	7.6052	78.313 8	9.644×10^{-5}
Cameroon 513 x 513		275.24	7.0101	7.0101	89.965 2	6.586×10^{-5}

5.3. Computational Time

The execution time of the information security algorithm is considered the major evaluation parameter. It has the main role for efficient and secure real time IoT applications. The last execution time provides high performance for secure and smart applications. As shown in Table 3, it illustrates the execution times for cryptography and steganography algorithms with different image sizes.

TABLE 3: The execution time for cryptography and steganography techniques with different sizes of Lena

5.4. Key Sensitivity

Image Sizes (Lena Image)	Data Encryption and Hiding Time	Data Encryption and Extraction Time	Image Encryption Time	Image Decryption Time
220 x 220	0.09s	0.09s	5.66s	5.66s
370 x 370	0.12s	0.12s	12.73s	12.73s
513 x 513	0.59s	0.59s	24.3s	24.3s

The cryptography technique must detect any change in the ordinary encryption key. So, the encryption algorithm shall be very sensitive to each simple change even if one bit of the true key. As shown in Figure 9. It uses one of the generated keys (K_0) to encrypt the 'Lena' image with size 220×220 bits and get a reference cipher image (C_0). Then, two modified keys at one bit (K_1 , K_2) are used to decrypt the plain image. It is noticed that only the correct key (K_0) can deduce the correct plain image, and the other keys fail to produce it.

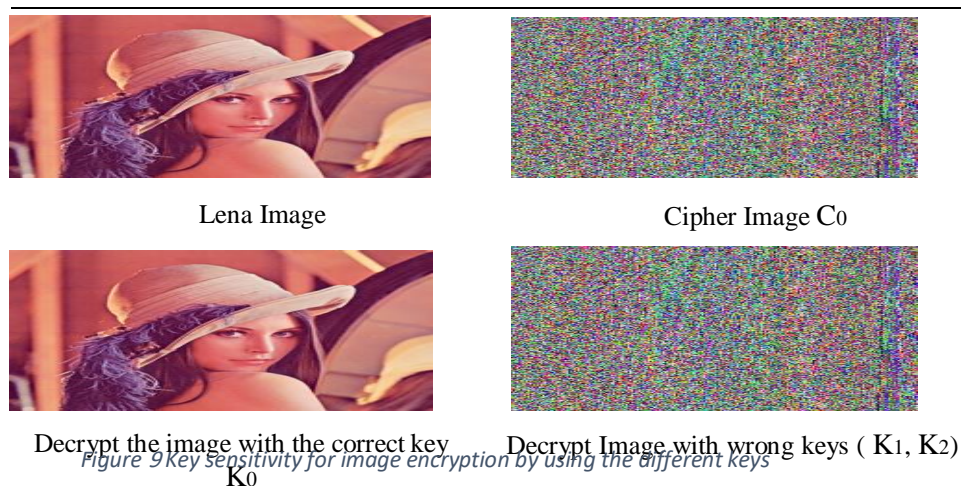


Figure 9 Key sensitivity for image encryption by using the different keys

5.5.

Analysis

Histogram

An effect of the secret message insertion was evaluated due to the steganography process using the histogram analysis. This analysis can detect the randomness of image pixels after hiding the corresponding sensitive information. The deduced histogram analysis illustrates the effect of secret message insertion on the image pixels. As shown in Table 4, it can evaluate the difference between the cover and steganography images in terms of the histogram analysis. The intruders have difficulty detecting hiding information through the same histogram analysis for the cover and steganography images. It is an indication of achieving the desired security. Therefore, the proposed scheme introduces high robustness through this analysis against such attacks.

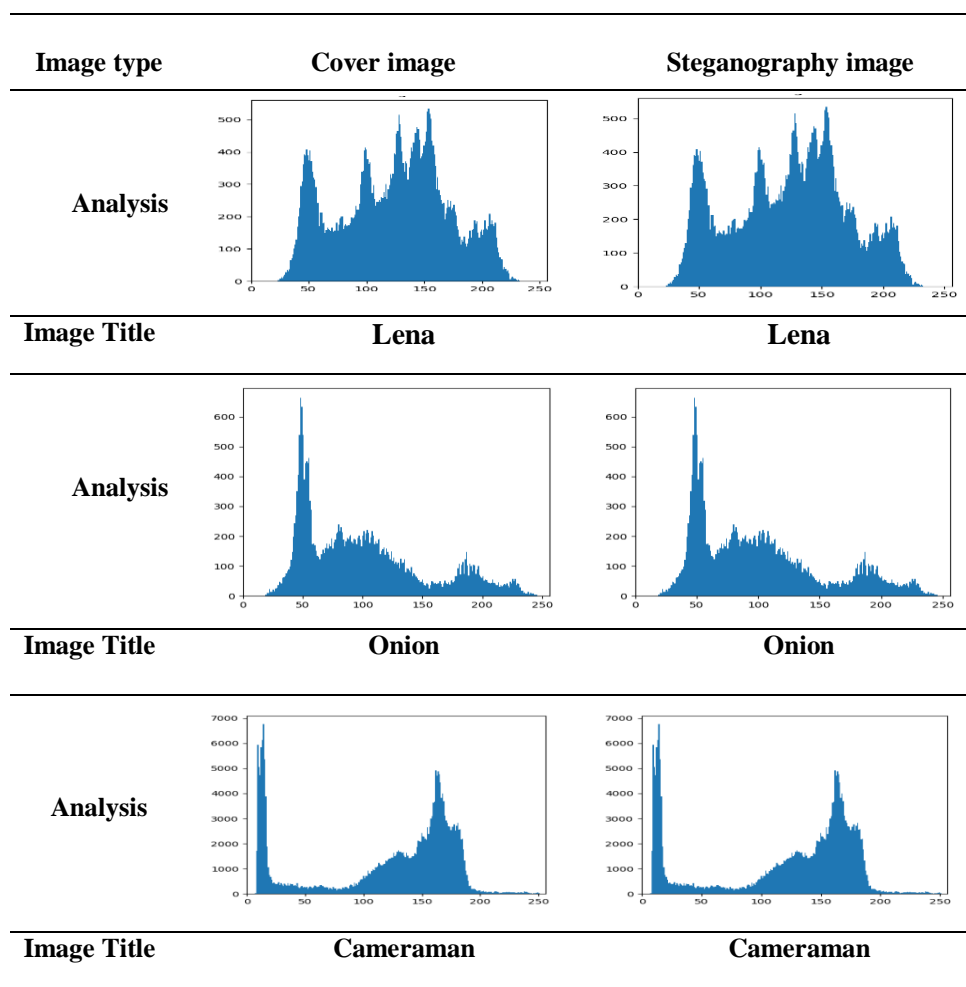
5.6. Security Performance Analysis

Protective, sensitive information can be destroyed or modified through any intruder interception. The intrusion detection systems mitigate known and unknown attacks using secure and efficient data collection [30]. The proposed scheme was evaluated regarding the resistance against different traditional attacks. These attacks include Distributed Denial of Service (DDoS), noise, and the man-in-the-middle attack. The effectiveness of our proposed scheme is noticed by ensuring the main security features and services. These features and services include confidentiality, integrity, and availability attributes. In addition, the security performance was evaluated through the histogram analysis and key sensitivity metric.

5.6.1. Man in the Middle Attack

It acts as the most serious cryptanalysis attack [31]. It aims to interpret the encryption technique for obtaining the encryption key from the encrypted text. The attacker tries to catch the transmitted information between the sender and receiver. The hashing function adds random salting bits in the extracted encryption key in our scheme. These random bits authenticate the exchanged messages between the different domains. The man-in-the-middle attack cannot deduce the generated encryption key. Therefore, it can't catch the exchanged messages after the hashing procedure.

TABLE 4: Histogram Analysis for cover and steganography images



5.6.2. Distributed Denial of Service (DDoS) Attack

Distributed Denial of Service (DDoS) attacks seriously threaten the IoT systems [33]. It is targeting the availability of communication networks by flooding a huge number of fake requests. These requests interrupt the communication between IoT devices and their communication servers. In our proposed scheme, it is mandatory to authenticate every party in the architecture before accessing the system. Therefore, the scheme cannot suffer DDoS attacks through the applied authentication procedure. The cloud server verifies the connected mobile phone with the registered International Mobile Equipment Identity (IMEI). The sensed data is authenticated through Bluetooth connectivity with authorized devices in the monitoring area. In addition, the cryptography keys are authenticated through biometric recognition attributes in the authorized cloud dashboards. The emergency center receives alert messages through a dedicated phone number.

5.6.3. Integrity

The sensed measurements were uploaded to an authenticated mobile device with fixed IMEI through Bluetooth. Then, it is transmitted through a secure communication tunnel using a Virtual Private Network (VPN), providing authenticated access to the network traffic. Using data encryption and hiding mechanisms allows the protection of sensitive data with the ability to provide backup versions. Therefore, our proposed scheme can detect the third party's behaviors and verify the integrity.

5.6.4. Noise Attack Analysis

A noise attack is one of the most dangerous attacks targeting image encryption techniques. It is performed by adding different noise attacks to the encrypted image before decryption. These attacks may include salt and pepper noise, Additive White Gaussian Noise (AWGN), and speckle noise [32]. The immunity against these attacks is conducted through the peak signal-to-noise ratio and the entropy evaluation metrics. Table 5 shows the effect of salt and pepper noise on the image encryption evaluation.

TABLE 5: Statistical evaluations for different sizes images and their decrypted ones under salt and pepper noise

Image	Size	Noise Attack	Entropy		PSNR
			Plain Image	Decrypted under Noise Attack	
Lena	370 x 370	Salt and Pepper	7.7445	6.953	39.955
Onion	198 x 135		7.6052	6.891	38.212
Cameraman	513 x 513		7.0101	6.616	42.845

5.6.5. Confidentiality

Information encryption and hiding techniques are used in our proposed information security platform. The AES encryption technique encrypts the measurement values for the sensed measurements protection before hiding them in the steganography image. In addition, it applied for protection the files with sensitive information. For sensitive image protection, the RSA technique is applied. All the resources and encryption keys have followed the specified authentication procedure. So, the data confidentiality attribute is achieved.

5.6.6. Comparison of the Proposed Scheme against Other Schemes

The strength of the information protection scheme was conducted through a comparative analysis against the other schemes. As shown in Table 6, our proposed scheme introduces higher execution time regarding the cryptography and steganography techniques. It provides great hiding accuracy through identical histogram analysis for the carrier and steganography images. In addition, it enhances the key sensitivity and PSNR through the encryption and hiding scenarios. However, it suffers from a significant decrement in the entropy of decrypted images under the noise attack regarding the other schemes. According to related evaluation models, our proposed scheme introduces the greatest imperceptibility attributes (higher PSNR, least MSE). As shown in Table 7, the proposed scheme has higher PSNR with the least MSE values but the others comparing schemes introduce little PSNR values with higher MSE.

TABLE 6: Comparison of performance attributes for the proposed scheme against other schemes in [21, 23, and 35].

Performance Attributes	Comparison of Different Schemes			
	Reference [21]	Reference [23]	Reference [35]	Proposed Scheme
Entropy	N/A	7.9	7.9	7.73
Computational Time for Encryption and Hiding	4.29s	N/A	N/A	0.59s
Computational Time for Image Encryption	50.43s	N/A	5.4s	24.3s
Histogram	Accurate for greyscale images	Accurate for greyscale images	Accurate for greyscale images	Accurate for grey and color images
PSNR	44.98	N/A	N/A	78.31
Key Sensitivity	N/A	High for greyscale images	High for grey scale images	High for grey and color images

TABLE 7: Comparison of imperceptibility attributes for the proposed scheme against other schemes [2, 4]

Evaluation Models	PSNR	MSE
Reference Scheme [2]	57.02	0.1288
Reference Scheme [4]	65.3	0.075
Proposed Scheme	89.9652	6.586×10^{-5}

The security issues are used to measure the robustness of the proposed security scheme against the different attacks. They can affect the information protection attributes, including confidentiality, privacy, integrity, and availability. Any successful attack can damage the security attributes by breaking the cryptography techniques and leakage sensitive information with less accurate information sharing. Regarding the evaluation security issues, a comparison of the proposed scheme against other schemes is concluded in Figure 10. The proposed scheme can provide great resistance against different attacks, including noise, dictionary, DDOS, and Man in the Middle attacks.

Conversely, the proposed schemes in related references do not provide the solutions to resist the different attacks. It is a great weakness for data confidentiality, integrity, and availability. The compared references consider the man-in-the-middle attack and ignore the other serious attacks.

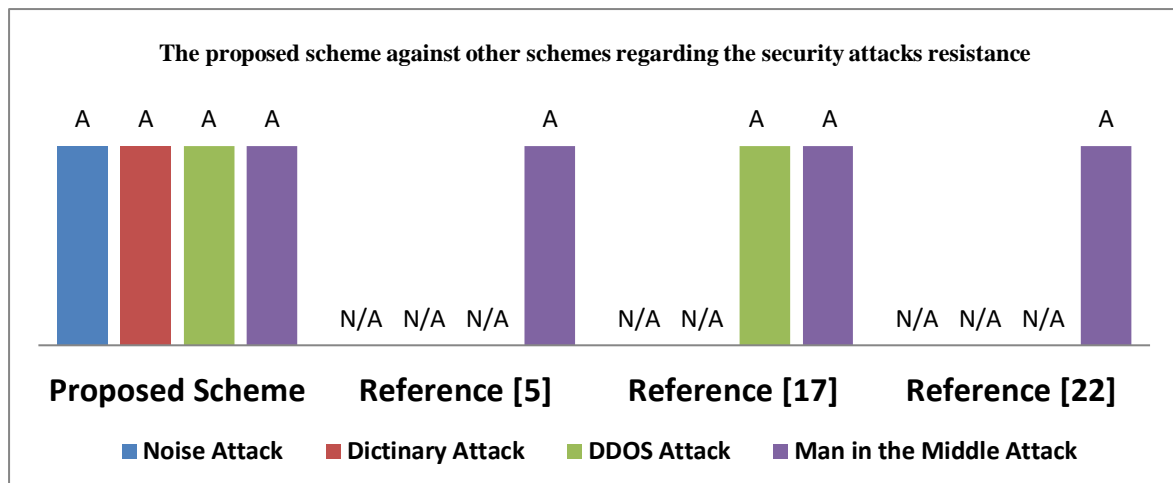


Figure 10 Comparison of security issues for the proposed scheme against other related schemes in [5, 17, and 22].

6. Conclusions

The proposed scheme aims to protect sensitive information and critical measurements for critical infrastructures, including nuclear facilities. It integrates information encryption and hiding techniques, including biometrics key extraction, cryptography, steganography, authentication, and cloud computing. The proposed security platform presents secure information transmission through symmetric and asymmetric encryption techniques with information hiding. It used extracted biometric keys for AES encryption of the sensed measurements and sensitive reports. RSA encryption algorithm is used for sensitive image protection. It was deduced through performance and security evaluation analysis that the proposed scheme performs very well regarding the algorithm's computational time and imperceptibility. Also, it provides high robustness against different attacks to introduce secure monitoring applications with high confidentiality and integrity.

References

- [1] Bhardwaj A., Subrahmanyam G., Avasthi V., and Sastry H.: Security algorithms for cloud computing. In: International Conference on Computational Modelling and Security, Elsevier, India, 2016(85), 535-542. DOI:10.1016/j.procs.2016.05.215.
- [2] Bairagi K., Khondoker R., and Islam R.: An efficient steganographic approach for protecting communication in critical infrastructures of the Internet of Things (IoT). Information Security Journal: Global Perspective, 2016(25), 197–212. DOI: 10.1080/19393555.2016.1206640.
- [3] Muniraj M., Qureshi A., and Bharathi N.: Geo-tagged Internet of Things (IoT) device for Radiation Monitoring. In: International Conference on Advances in Computing, Communications and Informatics, IEEE, India, 2017(2017), 431-436. DOI:10.1109/ICACCI.2017.8125878.
- [4] ELhoseny M., Ramirez-Gonzalez G., Abu-ELnasr O., Shawkat S., Arunkumar N., and Farouk A.: Secure medical data transmission model for IoT-based healthcare systems. Proc IEEE, 2018(6), 20596 – 20608, 2018.DOI: 10.1109/ACCESS.2018.2817615.
- [5] Hu J., Chen C., Fan C., and Wang K.: An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. Journal of Sensors, Hindawi, 2017(2017), 1–11. DOI: 10.1155/2017/3734764.
- [6] Kim S., Lim H., Lim S., and Shin I.: Study on cyber security assessment for wireless network at nuclear facilities. In: 6th International Symposium on Digital Forensic and Security, IEEE, Turkey, 2018. DOI:10.1109/ISDFS.2018.8355332.
- [7] Talbi M.: Speech Signal Embedding into Digital Images Using Encryption and Watermarking Techniques. Springer, 2020, 1–11. DOI:10.1109/ICCEA.2004.1459412.

- [8] Xu Z., Liu W., Huang J., Yang C., Lu J., and Tan H.: Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey. *Security and Communication Networks Journal*, Hindawi, 2020 (2020), 1-13. doi.org/10.1155/2020/8872586
- [9] Abdullahi M., Baashar Y., Alhussian H., Alwadain A., Aziz N., Capretz L. F., and Abdulkadir S.: Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics Journal*, MDPI, 11(198), 1-27, 2022.
- [10] Kotenko I., Izrailov K., and Buinevich M.: Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches. *Sensors Journal*, MDPI, 22(1335), 2022.
- [11] Lee J., Jeong K., Kim J., and Im C.: The development of remote wireless radiation dose monitoring system. In: 4th International Conference on Advancements in Nuclear Instrumentation Measurement Methods and their Applications, IEEE, Portugal, 2016. DOI:10.1109/ANIMMA.2015.7465285.
- [12] Gaber M., Mahmoud I., Seddik O., and Zekry A.: Development of Routing protocols in Wireless Sensor Networks for Monitoring Applications. Faculty of Engineering, Ain-Shams University, Master Thesis, 2016.
- [13] Hajjaji Y., Boulila W., Farah I., Romdhani I., and Hussain A.: Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review*, 39, 1-17, 2021. <https://doi.org/10.1016/j.cosrev.2020.100318>
- [14] <https://sightengine.com>, accessed in Jan, 2020
- [15] Jhanjhi N., Humayun M., and Almuayqil S.: Cyber Security and Privacy Issues in Industrial Internet of Things. *Computer Systems Science & Engineering Journal*, Tech Science Press, 1-20, 2021. DOI:10.32604/csse.2021.015206
- [16] Gupta H. and Varshney G.: A Security Framework for IOT Devices against Wireless Threats. In: 2nd International Conference on Telecommunication and Networks (TEL-NET 2017), 2017. DOI:10.1109/TEL-NET.2017.8343548.
- [17] Mousavi S., Ghafari A., Besharat S., and Afshari H.: Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. *Journal of Ambient Intelligence and Humanized Computing*, 2021(12), 2033–2051, 2021. <https://doi.org/10.1007/s12652-020-02303-5>
- [18] Savitha V., Karthikeyan N., Karthik S., and Sabitha R.: A distributed key authentication and OKM-ANFIS scheme based breast cancer prediction system in the IoT environment. *Journal of Ambient Intelligence and Humanized Computing*, 2021(12), 1757–1769, 2021. <https://doi.org/10.1007/s12652-020-02249-8>
- [19] Rabiah A., Ramakrishnan K., Liri E., and Kar K.: A lightweight authentication and key exchange protocol for IoT. In: Workshop on Decentralized IoT Security and Standards, USA, 2018. DOI: 10.14722/diss.2018.23004.
- [20] Devi M. and Sharma N.: Improved detection of least significant bit steganography algorithms in color and gray scale images. *Proceedings of RAECS UIET*, IEEE, Panjab University Chandigarh, 2014. DOI:10.1109/RAECS.2014.6799507.
- [21] Saleh M., Aly A., and Omara F.: Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications*, 2016(7), 390-397. DOI:10.14569/IJACSA.2016.070651.
- [22] Ansari A., Mohammadi M., and Parvez M.: A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security*, 2019(11), 1-11. DOI:10.5815/ijcnis.2019.01.02.
- [23] Usman M., Ahmed I., Aslam M., Khan S., and Shah U.: SIT: A lightweight encryption Algorithm for Secure Internet of Things. *International Journal of Advanced Computer Science and Applications*, 2018(8), 1–10. Doi:10.14569/IJACSA.2017.080151.
- [24] Duraisamy S., Krishnasamy P., Jacaob J., and Duraisamy J.: Enhancement of Security and QoS in Wireless Medical Sensor Networks *Journal of Computer Science and Engineering*, 14(2), 66-75, 2020. <http://dx.doi.org/10.5626/JCSE.2020.14.2.66>
- [25] Hussain R. and Abdullah I.: Review of different encryption and decryption Techniques used for security and privacy of IoT in different applications. In: 6th International Conference on Smart Energy Grid Engineering, IEEE Access, Canada, 2018, 293 – 297. DOI:10.1109/SEGE.2018.8499430.
- [26] Kalra S. and Sood S.: Secure authentication scheme for IoT and cloud servers. *Journal of Pervasive and Mobile Computing*, Elsevier, 2015(24), 210-223.
- [27] Kim J., Shim M., Hong S., Shin Y. and Choi E.: Intelligent Detection of IoT Botnets Using Machine Learning and Deep Learning, *Applied Sciences*, MDPI, 10 (7009), 1-22, 2020. Doi:10.3390/app10197009 2020
- [28] Qiu L., Liu Z., Pereira G., and Seo H.: Implementing RSA for sensor nodes in smart cities. *Personal and Ubiquitous Computing Journal*, Springer, 2017(21), 807–813, 2017. DOI: 10.1007/s00779-017-1044-y.

- [29] Ullo S. and Sinha G.: Advances in Smart Environment Monitoring Systems Using IoT and Sensors. Sensors Journal, MDPI, 20(3113), 1-18, 2020. doi:10.3390/s20113113
- [30] Sadikin F., Deursen T., and Kumar S.: A Hybrid Zigbee IoT intrusion detection system using secure and efficient data collection, Internet of Things Journal, 2020(12), 1-18, 2020. <https://doi.org/10.1016/j.iot.2020.100306>
- [31] Wang C., Shen J., Liu Q., Ren Y., and Li T.: A novel security Scheme based on instant encrypted transmission for Internet of Things. Journal of Security and Communication Networks, Hindawi, 2018. DOI:10.1155/2018/3680851.
- [32] Jiao S. and Liu R.: A survey on physical authentication methods for smart objects in IoT ecosystem. Internet of Things Journal, 2019(6). DOI: 10.3390/s19051141.
- [33] Kponyo J., Agyemang J., Klogo G., and Boateng J.: Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices, Internet of Things Journal, 12, 2020. <https://doi.org/10.1016/j.iot.2020.100319>
- [34] Sharma P. and Rajni: Analysis of Image Watermarking Using Least Significant Bit Algorithm. International Journal of Information Sciences and Techniques, 2012(2), 95-101, 2012. DOI:10.5121/ijist.2012.1409.
- [35] Loukhaoukha K., Chouinard J., and Berdai A.: A secure image encryption algorithm based on Rubik's cube principle. Journal of Electrical and Computer Engineering, Hindawi, 2012(2012), 1–13. DOI:10.1155/2012/173931.

Appendix A:

TABLE 1: Authentication attributes of key extraction in cloud servers

API_Credentials	Values
API_User	157003700
API_Secret	OOP9yLhALy9VynNqtwDA

TABLE 2: Extracted biometric cryptography keys

Detected Face Features	Detected Image Quality Features
ID = Med_4A8JhVetJSCU3qxUsM8ZT	ID = Med_4A8S7eQBtiPjrn04cu1g
Request ID = Req_4A8JzxIcMtlhprwtY60F8	Request ID = Req_4A8SngZ57S3RvOdwkksxf
X1= 0.2438	Brightness = 0.663
Y1= 0.4146	Contrast = 0.581
Left_eye"x"= 0.5266	Sharpness = 0.965
Left_eye "y"= 0.6354	Colors "r" = 164
Right_eye "x"= 0.3688	Colors "b" = 173
Right_eye "y"= 0.6375	Colors "hex"= #a49ead
Right_mouth"x"= 0.3891	Colors "g" = 158
Right_mouth "y"= 0.8729	Colors "r" = 170
Left_mouth "x"= 0.5141	Colors "b" = 181
Left_mouth "y"= 0.8729	Colors "hex"= #0a0ab5
Nose_tip "x"= 0.4656	Colors "g" = 163
Nose_tip "y"= 0.7542	Colors "r" = 155
Timestamp = 1548763023.321	Timestamp = 1548763591.6594
"Status" = Success	"Status" = Success