Advanced Protection Scheme For Information Monitoring in Internet of Things Environment

Mohamed Gaber (✉ Doctor_moh_2020@yahoo.com)

Egyptian Atomic Energy Authority <https://orcid.org/0000-0001-9238-0204>

Ashraf Khalaf

Minia University Faculty of Engineering

Imbaby Mahmoud

Egyptian Atomic Energy Authority

Mohamed El_Tokhy

Egyptian Atomic Energy Authority

Research Article

Keywords: Secure Monitoring, Steganography, Internet of Thing, Cryptography, AES, RSA, Nuclear Facilities

Posted Date: October 25th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-686564/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Abstract

In the recent years, Internet of Things (IoT) technologies are growing to make great progress for the nuclear energy applications. The protection of their sensitive information has become an important challenge in implementing secure application services. These services should meet the major security attributes including confidentiality, availability, and integrity. This paper introduces a security scheme for the transmitted sensitive information and secure monitoring of the critical radiation levels at the nuclear facilities. It evaluated through integrating the cryptography and steganography techniques with cloud computing services. The cryptography techniques based on Advanced Encryption Standard (AES) and Rivest, Shamir-Adleman (RSA) algorithms. The scheme uses the extracted cryptography keys from authenticated biometric attributes. The proposed scheme provides a low computational time suitable for fast responding in the emergencies. It allows securing access for the encrypted sensitive measurements, files, and images with high data integrity and confidentiality. Furthermore, it hides the confidential sensitive information with great capacity and imperceptibility through the transmitted carrier image. The security performance analysis ensures the robustness of introducing scheme against various attacks through authentication, encryption, and information hiding techniques. It resists the serious attacks, including the man in the middle, noise, and Distributed Denial of Service (DDOS) attacks.

1. Introduction

Internets of Things (IoTs) systems have suffered from many of the hacking attacks. They are the main source of different threats in all of the computerized systems. These threats force the researchers to introduce the efficient security frameworks and techniques. The shared sensitive information influenced by these attacks through undesired actions from the 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 a great serious, especially at the nuclear facilities. It may lead to different sabotage actions through unauthorized access to the sensitive nuclear information. Consequently, the information systems, especially which belong to the nuclear facilities are suffering from serious attacks. One of these more serious attacks is Stuxnet. It has a great effect on the operation of nuclear facility systems especially instrumentation and control systems.

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

The defense in depth technique is depended on using various protection levels to mitigate the 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 the different threats by using the sequential security barriers. Sensitive information assets contain the components that used to store, process, and control the sensitive data. It can be included in the control systems, computer networks, and information systems. The proposed security scheme can target these systems for secure sensitive information transmission. Table 1 illustrates some of the typical systems with sensitive information regard to nuclear facilities and the impacts of missing any of the information security attributes. It investigates the effects of missing any of the confidentiality or availability or integrity on the facility. It contains some of the systems that would find 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 the confidentiality through an unauthorized access to get 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 regard to secure control processes. These applications are highly vulnerable to security attacks through the 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
The typical systems of nuclear facility with sensitive information [7]

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 given to unauthorized persons
Documentation management system	Loss of confidentiality, availability, and integrity of data	Medium Information used to plan more severe attacks.

1.1 Related works

In the recent years, development and evaluation of information security schemes have motivated researchers' interest to implement intelligent secure IoT applications. So, several research papers have been found to study and analyse various IoT security schemes to protect the shared information against the threats. For example, the authors of [1] apply different 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 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 evaluated mathematically and experimentally to verify its ability to hide the 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 radiation monitoring scheme that using geo tagged IoT device 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 concerning authorities. But, they didn't interest in the security issues through applying data protection techniques. The detected measurements didn't secure and the devices didn't follow any authentication procedures. It was noticed in [4] that the authors present high information protection scheme for securing the diagnostic text data in the medical images. They use a combination of Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA) encryption techniques to integrating 2-D Discrete Wavelet Transform (2D-DWT) steganography technique. The scheme uses colour and greyscale images as cover images to hide different text sizes. It starts through encrypting the text data to hide the result in a cover image using a 2D-DWT steganography technique. The evaluation results ensure the scheme 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 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 the emergency situations. They protect the biological monitoring data and inspection reports to secure the medical records with authenticate access. The proposed scheme presents robustness against the replay attack and man in the middle attack 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 case in a nuclear facility. This attack is executed on the reactor to target the radiation monitoring system. It hacks the transmitted data to control in the emergency siren system. So, it ensures the importance of encrypting the transmitted data

and authenticates the assigned messages. They present a check list with assessment for the cyber security items. These items ensure the applying of efficient security techniques for wireless communication in nuclear facilities. It aims to prevent the unauthorized access of monitoring data and the common attacks including Denial of Service (DOS) and brute force attacks. It authenticates the accessing devices to wireless network and provides sufficient data protection.

In [8], they proposed an encryption-watermarking technique for embedding speech signals into the digital images. It encrypts the watermark before embedding 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 tool of image analysis 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 including, 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 one is the discussion of the proposed architecture which permits to monitor remotely the radiation levels at the corresponding nuclear facility. It 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 any threat attacks for taking the suitable actions in emergency situations. The second one is the proposed security platform which targets the sensitive data, especially regarding to nuclear facilities. This sensitive data may include compiling sensed data of specific physical parameter 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 attributes. The third one is the discussion of applying the proposed scheme during the emergency situations 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 also can be suitable for other applications that require the monitoring schemes with secure data transmission.

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

2. Security Risks And Mitigation Scenarios

Figure 1 presents the serious security risks and their mitigation scenarios in radiation monitoring system. It illustrates the weakest points with respect to the security risks which may attack many of the IoT

communication layers. The risk of sensitive information leakage and unauthorized access to the system is the most serious one. Thus, a strong information encryption and hiding techniques require to be deployed in the information transmission points. A strong authentication procedure is required in all of the accessing points such as, IoT gateway, smart phone application, and the main system accessing panel. All of 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 ensure the protection of 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.

3. The Proposed Protection Scheme For Information Monitoring

The proposed architecture is divided into three domains as shown in Fig. 2. 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 phone device or tablet which has 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 [9]. It can locate the monitoring areas with Global Positioning System (GPS) to help in the emergency situations. In addition, the connectivity can depend on the wireless networking of Wi-Fi for wide range connection with anti-jamming technique [10].

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 which extracts the cryptography keys from the biometric attributes for using in the proposed information security model. It authenticates the detected biometric attributes regard to the authorized operators through authentication information at the cloud servers. Key generation time and date are stored in the cloud servers and shown at the corresponding cloud dashboard. Secure information transmission routines can be a big challenge to introduce 5 G services and IoT applications [11]. All the parties are connected through an authenticated network with the unique IP addresses. Also, it contains the cryptography and steganography platforms through an implemented Graphical User Interface (GUI). The third domain includes an emergency centre with the IoT application services. Emergency centre will receive the 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 the normal and emergency monitoring situations.

3.1 Biometric security keys extraction

Key Generation Unit (KGU) is responsible for issuing the public and private encryption keys after registers 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 at 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 is depended on the used encryption key in order to make the revelation of it as difficult as possible. As shown in Fig. 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 features attributes. At appendix A, Table 2 shows the samples of extracted features from any detected face and image quality attributes.

The applied Application Programming Interface (API) through 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 [14]. The generated keys are stored on cloud servers and can be used with applied hashing function as the information security platform. Biometrics attribute considered a strong authentication procedure for operators and information transmission authentication mechanisms.

3.2 Applied authentication routine

Authentication function is applied to store the generated keys in hashing form. It replaces the actual generated key with the hashing one for implementing more secure applications. It aims to make the key in difficult recover secure form. Also, the generated biometric keys can be verified through an efficient matching method of the hashing units. The applied cryptography scheme requires a fixed length encryption key. So, hash function is applied to provide output with fixed length of a variable length input. Hashing technique (SHA256) is used to provide a 16 byte output and can apply high performance with AES-256 encryption technique [15] [16]. SHA256 based on Hash-based Message Authentication Code (HMAC). It calculates the message authentication code which specifies the hash function combination with secret cryptographic key for authentication [17].

3.3 Proposed monitoring scheme sequence diagram

The communication parties register themselves at the key generation unit in advance via a secure channel. As shown in Fig. 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 time 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

provides encryption and hiding for the sensitive information which includes the sensing data, files, and images through proposed platform with 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 are exceed the threshold values, it will notify the emergency centre with SMS messages on the registered phone number in an acceptable time. Then, the emergency centre authorities can access the protected information. The fourth step allows sending an acknowledgement to the operator about dispatching the rules and regulations of emergency conditions. But, in the 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 the transmitted sensitive information through not understandable and authenticated transmission [12], [13].

3.4 Information encryption and hiding methodology

Information hiding represents one of the main ways to protect the sensitive information [18] [19]. Therefore, many information steganography techniques applied to hide the data. It may use images, or videos or text. Images with various formats used to hide the information with different capacities [20]. We applied the information hiding technique by using Least Significant Bit (LSB) insertion method. It's based on using RGB color images as carriers for information protection at IoT environment. The technique hides information in the deeper layer of image channels with minimum distortion in LSB to use as indication of data [2]. 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 protected through 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 Fig. 5. Firstly, it is necessary to define the used cover image and the data encryption key. Symmetric key encryption technique (AES) is used to encrypt the compiled files of detecting measurements. Then, the encrypted data is translated into binary. Secondly, 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 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. Although, 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 [32].

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 performance. These techniques provide high execution time with more efficient performance than the traditional techniques [21]. Advanced Encryption

Standard (AES) is used as symmetric key cryptography technique for transmission the sensed measurements and text reports with sensitive information. AES based on principle definitions including substitution-permutation network, combination of both substitution and permutation. AES uses Rijndael cipher which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits [22].

Through the literature analysis, it was noticed 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 through using a longer encryption key. The AES encryption technique is recommended for achieving the major appliance security attributes including integrity and confidentiality [23]. Rivest, Shamir, and Adleman (RSA) algorithm is used as a symmetric key cryptography technique [24] for transmitted 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 suitable environment for data transmission within cloud based applications. The sensitive information is encrypted and stored on the cloud servers. The emergency centre or operator can access the data through authenticated request. RSA algorithm depends on public key known to all the parties and private key for decryption process only. Also, it introduces high security attributes to the encrypted images [25].

4. System Development And Performance Analysis

4.1 Implemented information security platform

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

AES/RSA encryption technique is used to protect the sensitive information of any corresponding facility [26] [27]. Sensed data and other sensitive information can be compiled files for uploading through authenticated terminals. Therefore, our scheme can provide more flexible and accurate monitoring service. The model compiles the hidden monitored measurements into a file. Figure shows the compiled file with the extracted measurements and sensitive information regarding to any nuclear facility. Cover Images can be colour or grey scale images to hidden messages with different sizes.

4.2 Emergency management approach

Detection of an emergency situation considers one of the main goals in any monitoring system for taking the suitable responding actions. As shown in Fig. 8, it 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 way. At the first, the sensed information is collected through the distributed IoT devices and gateways in IoT environment. Then, it forwarded to the operation unit to apply the information security attributes. These attributes guarantee the 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 the critical measurements.

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

After detecting the emergency situations, the authorities need to access the sensitive information of system measurements and their effects on the operation of the suitable emergency responding actions. They have a permission to access the system for getting the sensitive information and reports at any time from different locations. Therefore, they can launch the suitable responding actions which 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 platform can execute the cryptography and steganography operations for all the critical measurements and sensitive information files for secure monitoring. It performed on 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 the 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 to the ordinary plain information. It aims to add extra 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 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) , $\sum_{i=1}^L P(I_i) = 1$ [18]. The entropy would be higher, if the pixel values near to the uniform distribution. For an image approaches uniform distribution, it has 256 gray levels with the same occurrence probability. Hence, the optimal entropy value is eight. Table 2 shows a comparison of the entropies of three tested images as cover and steganography images with many sizes at the different hiding capacities.

5.2 Imperceptibility

Information hiding technique 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 the 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 .

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

$$PSNR = 10 \log_{10} \frac{C_{\max}^2}{MSE} \quad (3)$$

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. $C_{\max}$ refers to the

highest pixel value in the image. Higher PSNR provides better quality of steganography image regarding the cover image. The results of above formulas can use to measure the quality of a steganography process. Simple insertion of the secret message bits into LSB of the used cover image leads to hide the information with undetected changes by the human eyes. The highest PSNR provides the greatest image quality and hiding efficiency. As shown in Table 2, it 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	3.421x10 ⁻⁵
Onion 198 x 135		459.54	7.6052	7.6052	78.3138	9.644x10 ⁻⁵
Cameraman 513 x 513		275.24	7.0101	7.0101	89.9652	6.586x10 ⁻⁵

5.3 Computational time

An execution time of the information security algorithm considers the major evaluation parameter. It has the main role for efficient and secure real time IoT applications. Least 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 image

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

5.4 Key sensitivity

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 Fig. 9. It uses one of the generated keys (K0) to encrypt 'Lena' image with size 220× 220 bits and get a reference cipher image (C0). Then, two modified keys at one bit (K1, K2) are used to decrypt the plain image. It is noticed that only with the correct key (K0) can deduce the correct plain image and the other keys fail to produce it.

5.5 Histogram analysis

An effect of the secret message insertion evaluated due to the steganography process by 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 are difficulty detecting the existence of 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

The protective sensitive information destroyed or modified through any intruder interception. So, the proposed scheme evaluated in terms of the resistance against different traditional attacks. These attacks contain Distributed Denial of Service (DDoS) attack, noise attack, and the man in the middle attack. The effectiveness of our proposed scheme noticed through ensuring the main security features and services. These features and services include the confidentiality, integrity, and availability attributes. In addition, the security performance 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 [28], [29]. 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. In our scheme, the hashing function adds random salting bits in the extracted encryption key. 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 act the serious threat on the IoT systems. 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 from 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 authenticated through Bluetooth connectivity with authorized devices in the monitoring area. In addition, the cryptography keys authenticated through biometric recognition attributes in the authorized cloud dashboards. The emergency center receives alert messages through dedicated phone number.

5.6.3 Integrity

The sensed measurements uploaded through Bluetooth connectivity to authenticated mobile device with fixed IMEI [19], [31]. Then, it transmitted through a secure communication tunnel using Virtual Private Network (VPN) which providing authenticated accessing to the network traffic. Using of data encryption and hiding mechanisms allow protecting the sensitive data with the ability of providing backup versions. Therefore, our proposed scheme can detect the third parties behaviors and verify the integrity.

5.6.4 Noise attack analysis

Noise attack is one of the most dangerous attacks which targeting the image encryption techniques. It is performed through adding different noise attacks to the encrypted image prior to decryption. These attacks may include salt and pepper noise, Additive White Gaussian Noise (AWGN), and speckle noise [30]. The immunity against these attacks is conducted through the peak signal to noise ratio and the entropy evaluation metrics. As shown in Table5, it 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 type	Cover image	Steganography image
Analysis
Image Title	Lena	Lena
Analysis
Image Title	Onion	Onion
Analysis

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

5.6.6 Comparison of the proposed scheme against other schemes

The strength of the information protection scheme conducted through a comparative analysis against the other schemes. As shown in Table 6, our proposed scheme introduces higher execution time in terms

of 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 significant decrement at the entropy of decrypted image under the noise attack regarding to 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 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 [19, 21, and 31].

Performance Attributes	Comparison of Different Schemes			
	Reference [19]	Reference [21]	Reference [30]	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 grey scale images	Accurate for grey scale images	Accurate for grey scale images	Accurate for grey and color images
PSNR	44.98	N/A	N/A	78.31
Key Sensitivity	N/A	High for grey scale images	High for grey scale images	High for grey and color images

Table 7 Comparison of performance attributes for the proposed scheme against other schemes in [19, 21, and 31].

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, availability. Any successful attack can damage the security attributes through breaking the cryptography techniques and leakage the sensitive information with less accurate information sharing. Regarding the evaluation security issues, a comparison of the proposed scheme against other schemes is

concluded in Fig. 10. The proposed scheme can provides a great resistance against the different attacks including noise, dictionary, DDOS, and Man in the Middle attacks. But in the other side, the proposed schemes in related references do not provide the solutions to resist the different attacks and it acts as the great weakness point for providing data confidentiality, integrity, and availability. The compared references just consider the man in the middle attack and ignore the others serious attacks.

6. Conclusions

The proposed scheme is aimed to protect the sensitive information and critical measurements for the critical infrastructures including the nuclear facilities. It integrates the 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 images protection. Through performance and security evaluation analysis, it was deduced that the proposed scheme performs very well in terms of algorithms computational time and imperceptibility. Also, it provides high robustness against different attacks to introduce secure monitoring application with high confidentiality and integrity.

References

1. Bhardwaj, A., Subrahmanyam, G., Avasthi, V., & Sastry, H. Security algorithms for cloud computing. 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., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. *Information Security Journal: Global Perspective*, 25, 197–212. DOI: 10.1080/19393555.2016.1206640
3. Muniraj, M., Qureshi, A., Bharathi, N., & India Geo tagged Internet of Things (IoT) device for Radiation Monitoring. International Conference on Advances in Computing, Communications and Informatics, IEEE, (2017). ; 2017, 431–436. DOI:10.1109/ICACCI.2017.8125878.
4. ELhoseny, M., Ramirez-Gonzalez, G., Abu-ELnasr, O., Shawkat, S., Arunkumar, N., & 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., & Wang, K. (2017). An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. *Journal of Sensors*, Hindawi, ; 2017, 1–11. DOI: 10.1155/2017/3734764.
6. Kim, S., Lim, H., Lim, S., Shin, I., & Turkey Study on cyber security assessment for wireless network at nuclear facilities. 6th International Symposium on Digital Forensic and security, IEEE, (2018). DOI:10.1109/ISDFS.2018.8355332.

7. IAEA Nuclear Security Series No.17. Computer security at nuclear facilities technical guidance. IAEA Publishing.
8. Talbi, M. (2020). Speech Signal Embedding into Digital Images Using Encryption and Watermarking Techniques. Springer, ; 1–11. DOI:10.1109/ICCEA.2004.1459412.
9. Lee, J., Jeong, K., Kim, J., Im, C., & Portugal The development of remote wireless radiation dose monitoring system. 4th International Conference on Advancements in Nuclear Instrumentation Measurement Methods and their Applications, IEEE, (2016). DOI:10.1109/ANIMMA.2015.7465285.
10. Gaber, M., Mahmoud, I., Seddik, O., & Zekry, A. (2016). Development of Routing protocols in Wireless Sensor Networks for Monitoring Applications. Faculty of Engineering, Ain-Shams University, Master Thesis,
11. Joydev, G. 5G services and IoT challenges. International Journal of Sensors, Wireless Communications and Control(2019). ; 9(4), 417–418, 2019.
12. <https://sightengine.com/>
13. Shah, T., & Venkatesan, S. (2018). Authentication of IoT device and IoT server using secure vaults. 12th IEEE International Conference on Big Data Science and Engineering, IEEE, USA, ; 819–824. DOI: ieeecomputersociety.org
14. Gupta, H., & Varshney, G. A. Security Framework for IOT Devices against Wireless Threats. 2nd International Conference on Telecommunication and Networks (TEL-NET 2017)(2017). DOI:10.1109/TEL-NET.2017.8343548.
15. Sundaram, B., Ramnath, M., Prasanth, M., & Sundaram, J. V. Encryption and hash based security in internet of things. 3rd International Conference on Signal Processing, Communication and Networking, IEEE(2015). DOI: 10.1109/ICSCN.2015.7219926
16. Kalra, S., & Sood, S. (2015). Secure authentication scheme for IoT and cloud servers. *Journal of Pervasive and Mobile Computing, Elsevier*, 24, 210–223. DOI:10.1016/j.pmcj.2015.08.001
17. Rabiah, A., Ramakrishnan, K., Liri, E., & Kar, K. (2018). A lightweight authentication and key exchange protocol for IoT. Workshop on Decentralized IoT Security and Standards, USA, DOI: 10.14722/diss.2018.23004.
18. Devi, M., & Sharma, N. (2014). Improved detection of least significant bit steganography algorithms in color and gray scale images. Proceedings of RAECS UIET, IEEE, Panjab University Chandigarh, DOI:10.1109/RAECS.2014.6799507.
19. Saleh, M., Aly, A., & Omara, F. (2016). Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications*, 7, 390–397. DOI:10.14569/IJACSA.2016.070651
20. Ansari, A., Mohammadi, M., & Parvez, M. (2019). A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security*, 11, 1–11. DOI:10.5815/ijcnis.2019.01.02
21. Usman, M., Ahmed, I., Aslam, M., Khan, S., & Shah, U. (2018). SIT: A lightweight encryption Algorithm for Secure Internet of Things. *International Journal of Advanced Computer Science and Applications*,

- 8, 1–10. Doi:10.14569/IJACSA.2017.080151
22. Martin, K., Lu, H., Bui, F., Plataniotis, K., & Hatzinakos, D. (2009). A biometric encryption system for the self-exclusion scenario of face recognition. *Systems Journal, IEEE Access*, (3), 440–450. DOI:10.1109/JSYST.2009.2034944
23. Hussain, R., & Abdullah, I. (2018). Review of different encryption and decryption Techniques used for security and privacy of IoT in different applications. 6th International Conference on Smart Energy Grid Engineering, IEEE Access, Canada, ; 293–297. DOI:10.1109/SEGE.2018.8499430.
24. Kalra, S., & Sood, S. (2015). Secure authentication scheme for IoT and cloud servers. *Journal of Pervasive and Mobile Computing, Elsevier*, 24, 210–223
25. Leong, K., Chze, P., Wee, A., Sim, E., May, K., Networks, I. E. E. E., & Access Multi-factors security key generation mechanism for IoT. 9th International Conference on Ubiquitous and Future, Italy(2017). DOI: 10.1109/ICUFN.2017.7993953.
26. Wei, W., Jun, Z., & Access, I. E. E. E. Image encryption algorithm Based on the key extracted from iris characteristics. 14th International Symposium on Computational Intelligence and Informatics, Hungary(2014). DOI: 10.1109/CINTI.2013.6705185.
27. Qiu, L., Liu, Z., Pereira, G., & Seo, H. (2017). Implementing RSA for sensor nodes in smart cities. *Personal and Ubiquitous Computing Journal, Springer*, ; 21, 807–813, 2017. DOI: 10.1007/s00779-017-1044-y.
28. Sridhar, S., & Smys, S. (2017). Intelligent security framework for IoT devices cryptography based End-To-End security Architecture. International Conference on Inventive Systems and Control, IEEE Access, DOI: 10.1109/ICISC.2017.8068718.
29. Wang, C., Shen, J., Liu, Q., Ren, Y., & 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.
30. Jiao, S., & Liu, R. (2019). A survey on physical authentication methods for smart objects in IoT ecosystem. *Internet of Things Journal*. 6, DOI: 10.3390/s19051141
31. Loukhaoukha, K., Chouinard, J., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering, Hindawi*, ; 2012, 1–13. DOI:10.1155/2012/173931.
32. Sharma, P., & Rajni (2012). Analysis of Image Watermarking Using Least Significant Bit Algorithm. *International Journal of Information Sciences and Techniques*, ; 2, 95–101, 2012. DOI:10.5121/ijist.2012.1409.

Figures

Figure 1

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

Figure 2

Proposed scheme architecture for secure remote monitoring system

Figure 3

Block diagram of key generation unit

Figure 4

Secure monitoring scheme sequence diagram

Figure 5

Process diagram of the information encryption and steganography

The interface is titled "Information Encryption and Steganography Platform". It is divided into two main sections: a left sidebar with blue headers and a main right area with a purple background.

Left Sidebar:

- Image Options:** Contains a "Select Image" button with a folder icon.
- Encryption:** Contains a "Generated Key:" label and a large text input field.
- Critical Measurements:** Contains a large text input field.
- Stego Options:** Contains two buttons: "Hide" with a closed eye icon and "Show" with an open eye icon.
- Image or File Encryption Options:** Contains a "Password" label and a text input field, and two buttons: "Encryption" and "Decryption".

Main Area (Informations and Progress):

- Image Info :** Contains two input fields: "Name :" and "Path :".
- Process Info :** Contains an "Operation :" label, an "Output :" input field with a "Browse" button, and a "Start" button.
- Image or File Encryption :** Contains an "Operation:" label, a "Path:" input field with a "Browse" button, and a "Start" button.

Figure 6

Information cryptography and steganography security platform

Figure 7

Example of hidden and extracted measurements through the steganography process

Algorithm1: Information monitoring and emergency management mechanism

Input:

SNs = number of nodes $N = \{ S1, S2, ..., Sn \}$

Gs = number of gateways $G = \{ G1, G2, ..., Gn \}$

Js = number of potential locations of nodes $J = \{ 1, 2, ..., S \}$

Output:

Pack = Publish acknowledgement message from the emergency center

Pdb = Publish update message to the database within receiving time and date

Pac = Publish alert message to the emergency Center through the registered phone number

1: Each gateway aggregates the sensed information from the sensing nodes to BS

2: Forward the acquired information to the control center

3: Applying Cryptography and Steganography Security Attributes

4: Applying the features detection programming Script

5: Extracting the attributes from detected features (Faces, Image Quality) as in appendix, Table (2)

6: **For all** the detected features **do**

7: private encryption key $\leftarrow$ faces features

8: Public encryption key $\leftarrow$ Image quality features

9: **for all** SNs **do**

10: **if** Measured level > Threshold Level **then**

11: Pac $\leftarrow$ Alert messages through a cloud server

12: Pack $\leftarrow$ Acknowledgement messages

13: **Else**

14: Pdb $\leftarrow$ update messages

15: **End If**

16: **End for**

Figure 8

Figure 9

Key sensitivity for image encryption with by using the different keys

Figure 10

Comparison of security issues for the proposed scheme against other related schemes in [5, 15 and 20].

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [AppendixA.docx](#)