I.J. Wireless and Microwave Technologies, **2025, 3, 66-77**
Published Online on June 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2025.03.05

Implementation of Internet of Things Based Data Security Using Hybrid Cryptography

J. S. Prasath
Department of Computer Science and Engineering, Sapthagiri NPS University, Chikkasandra, Bengaluru, 560057, India
E-mail: prasaths@snpsu.edu.in
ORCID iD: https://orcid.org/0000-0002-8718-1494

Received: 26 June, 2024; Revised: 19 August, 2024; Accepted: 04 October, 2024; Published: 08 June, 2025

Abstract: Internet of Things (IoT) is the current trends in tracking the variation of process variables in plant operations. The security threats and security issues continues to rise due to the wide usage of internet. The hybrid cryptography is proposed that involves symmetric AES, asymmetric RSA and hash functions all together enhance the security. The key length of this proposed symmetric AES encryption is 128-bit, RSA public key encryption is 1024-bit and 128-bit message digest is generated from the hash algorithm. It offers low latency in executing the proposed encoding and decoding algorithm. It is developed and verified in real-time environment using embedded system with internet of things. It assures data security and allows only authorized parties to monitor the plant parameters through the wireless networks. It preserves the intruders from gathering and modifying the sensitive plant information. It is suitable for protecting the plant parameters over the wide range of industrial applications.

Index Terms: Encoding, Decoding, Internet, Cryptography, Plant

1. Introduction

Embedded systems with IoT is the current development in wide range of applications. The process parameters can be communicated and gathered through the wireless medium. Data communication through the internet is unsecure and unsafe operations. Attackers easily capture the transmitted information, modify the plant parameters and send it to the destination. This results in loss of original information and damage of industrial devices. The security solutions need to be proposed corresponding to the recent technological developments. Cryptography is a widely used technique in securing the continuous varying process parameters. It converts the process raw data into unreadable cipher text through encryption and this unreadable text is transmitted across internet. At the receiver side, this encrypted data is converted back to plain text through decryption. Cryptography ensures data confidentiality in the internet based data transmission. Hash algorithms can be used to ensure data unaltered during transmission over internet. The wide ranges of cryptography algorithms are available for protecting the continuous varying process data against unauthorized access and modification. A comprehensive analysis is performed with respect to the recent trends, techniques, and concerns in utilizing machine learning for discovering the cyber threat in IoT [1]. The machine learning based intrusion detection system related to IoT security is analyzed. The novel hybrid deep learning mechanism is proposed that synergizes Long Short-Term Memory Auto Encoders and Multilayer Perceptrons in detecting botnets in IoT [2]. It assists the analysis of sequential data and pattern recognition, enabling the model to identify complex botnet action within IoT networks. A comprehensive investigation is performed to analyze the intersection of quantum computing, federated learning, and 6G wireless networks [3]. It is explored to enhance security and privacy within the IoT. The analysis of various machine learning models for IoT security is discussed along with its merits and demerits [4]. The drawback of machine learning models is large computational overhead and risk of privacy leakage. The various performance parameters of cryptographic algorithms to strengthen the security level are block size, key length, rounds of operation and number of digits used for data encoding. The security of plant parameters is achieved through the proposed hybrid cryptography algorithm that includes symmetric and hash functions [5]. The hash algorithm provides authentication of plant operators and assures data integrity. Data Integrity is necessary to assure smooth functioning of industrial operations. It ensures the sensitive process parameters unaltered during communication and monitoring through the internet.

Embedded devices are used in a variety of applications due to cost effective, consuming less energy, and faster speed of operations. The challenging task in an embedded system is to incorporate security mechanisms with the consideration of all aspects from design to implementation. Embedded systems have limited battery powered which

needs additional energy to perform secure operations. Security is a major concern for embedded devices due to the vast usage in variety of fields. Security is often not considered while designing the embedded systems. The security mechanism proposed for embedded systems needs to fulfill the various objectives including confidentiality, integrity, authentication, authorization and data freshness.

IoT is used to gather and compute the real time information. The major concern of internet based data monitoring is to assure the plant information need be protected from the intruders. The security mechanism should be strong to protect the valuable equipments from accessing of the intruders. The security solutions need to be implemented for perception, network and application layers of the IoT. The security concern in the IoT is reviewed [10]. The methodology needed to secure the resources are identification of authorized parties, giving rights to authorized users to access the resources, and to assure the privacy in monitoring and controlling the plant variables. The existing security solutions are not enough to preserve the valuable devices due to the recent technological development. IoT allows gathering and modifying the plant information through the wireless medium. The industrial and consumer oriented IoT deployment are discussed [11]. The application development for the IoT is the complex operations due to the hybrid coding, various protocols requirement for communicating the information. The security of IoT devices is addressed through the different energy efficient techniques [15]. The energy efficient mechanism can be achieved through the utilization of low power security protocols.

IoT devices having the constraints in handling the security protocols and it is revealing them to feasible intrusions. The security threats continue to increase due to the expansion of IoT devices and networks. The location-based privacy preservation mechanism is proposed that adopts a variable privacy boundary to prevent information secrecy and increase the usage of information and coding in the internet [23]. The energy-efficient security techniques are essential for IoT since it is operated with less power, less bandwidth, and less storage. The energy-saving mechanisms include online or offline security, outsource security, adaptive security, data size compression, low power security protocols that can be applied to IoT security in order to achieve reduced power consumption.

2. Related Works

The embedded systems are broadly utilized in various fields. Embedded systems and wireless communications are the modern technological development in industrial applications. The wireless networks are preferred for industrial process monitoring than wired networks. The wired network requires cable which is difficult to connect between all the process equipment and controllers. The drawback of using cables for process data transmission are high cable cost, cable fault and data loss. The flexibility of cable is also very limited. It is hard to move process equipment and sensors that are connected with cables. When the process needs to be extended with more sensors, additional cables are required for process monitoring.

The use of wireless networks for industrial applications greatly reduces the cable cost and maintenance cost. The industrial process can be easily added with new sensors in wireless networks. The wireless networks will become a central part of future control system. Embedded systems are susceptible to various intrusions which include hardware and software attacks. The physical and side channel attacks are the common hardware attacks on embedded systems. The code and buffer overflow attacks are the software attacks on embedded systems. Data security is a primary concern in the design of embedded based wireless devices. The security mechanism is essential to ensure the privacy and to preserve the plant variables from the intruders. The wide range of security algorithms are exists for protecting the plant parameters. The criteria in choosing the security algorithms depends on data size, key size, energy consumption, execution speed, energy cost and algorithm complexity. The strength of cryptography for embedded devices in terms of energy consumption, data processing speed and energy cost is addressed [30]. The energy utilization of security algorithms are non-linear functions of the length of plaintext. The battery expense is proportionate to the compilation period of cryptography algorithm.

The security threats increase especially when the embedded systems are connected to the networks or internet. The process variables are communicated over the internet that is vulnerable to different attacks. The cryptographic algorithm for securing the embedded systems with wireless networks should be complex and the key size must be large to preserve the process data and resources from the attackers. The attackers eavesdrop the ciphertext and try to obtain the plaintext. Intruders try to hack the process parameters that are sent across the internet. IoT based plant monitoring system should require optimized mechanisms for preserving the equipments in order to use it for complex industrial applications.

The software solutions are not enough to protect the embedded devices and IoT. The process data to be gathered and complexity of security protocols increases in the real-time applications. Embedded systems are designed with electronic components and assembled from different vendors. The security should be ensured while developing the components and integrating with the embedded system. The hardware components of embedded system need to be secured for normal plant operations. The industrial oil and gas operations monitoring and protection is performed using WSNs [31]. The purpose is to decrease the expenses related to commissioning and repair, power demand, and enhance the performance of wireless networks. Industrial process monitoring system can be implemented in a low-cost used for wide range of applications. The progressive trust mechanism is proposed related to routing and data security. The

intelligent behavior attack is used to represent the uneven activeness attack in the content domain. Security attacks in wireless networks take place due to the interruption, interception, modification and fabrication.

3. Literature Review

Industrial process information transmitted across wireless networks should be protected since it is vulnerable to various attacks. The challenging task is to implement the security mechanisms in real-time applications. The challenges in protecting the information and ensuring the identity during transmission through IoT are reviewed that are corresponding to the secrecy, faith, identity and rights control [24]. In this review work, the requirement for IoT is addressed which is to develop the optimal security mechanisms for embedded networks.

The security frameworks are necessary to preserve the sensor networks from the variety of attacks. IoT layered architecture security, management of data transmission and networks are discussed [25]. The existing concern in protecting the IoT devices is discussed. These challenges are resource limitations, implementing the multi-layer security framework, interoperability of security protocols, vulnerability of single point failure, hardware vulnerability of IoT architecture, scalable and trust management. The protocols used for protecting the data transmission security in the IoT are analysed [20]. The research challenges include designing key management mechanisms to assist security of top most layers, security against packet fragmentation attacks, routing security, identification of threat models, security against internal attacks, and effective key management.

The complexity of implementing the security are analysed correspond to the properties of the IoT devices and the add-on characteristics of the IoT [26]. In this work, they addressed the required security solutions to attain a high level security in IoT, including low powered security algorithms and protocols design, mechanisms to preserve the physical systems, and various approaches to manage and set up the security settings of IoT devices. Smart card based user authentication mechanism is proposed with efficient password protection [16]. This review work also addressed the existing target devices are incapable for usage in low powered protocols. The hybrid security algorithm is proposed for data security in waste-water treatment plant [8]. The waste-water content is preserved through the encryption and hash algorithm. This work addressed the security protocols are essential for data communication across internet. The security issues, and various attacks on IoT are addressed [12]. The unique structure can be used for securing the applications that utilizes the IoT. The security problems of the distributed formulation of the IoT are addressed [21]. The distributed mechanism raises the difficulty of different methodologies operated for security. Hardware security mechanism is proposed along with the hybrid cryptography algorithm to ensure secure communication and accessing of plant information across internet [6]. The symmetric and public key algorithms generates large key size. Hardware key is required to access the security code, to perform encoding and decoding of process data.

The architecture is proposed using embedded devices for ensuring data protection and secrecy in various levels of processors. Security must be given top priority and to take steps towards implementing in real-time applications. A fault space transformation based measure is proposed for analysing the variable failure on symmetric AES algorithm [13]. The research issue is the complexity in achieving equivalent insertion of fault in the existence of fault space transformation.The modified AES security algorithm is proposed for data security [18]. The total rounds of operation in AES algorithm is increased to 16 that provides higher level of security. The computational time increases due to this increased number of rounds in performing encryption and will become complex for the intruder to break the system. The security algorithm is proposed that is based on Elliptic Curve Cryptography (ECC) and homomorphic encryption to protect the information communicated across wireless networks [19]. The public and private keys are produced from this elliptic curve for secure data transmission across wireless sensor networks. It enhances the operations performed by the network in terms of lifespan, expenses related to transmission, and power requirements. The modern cryptography is proposed that utilizes symmetric and public key to enhance the level of security [27]. In this work, data encryption is achieved through the utilization of elliptic curve and symmetric Advanced Encryption Standard (AES) algorithms. Authentication is achieved through the utilization of XOR-DUAL RSA encoding and integrity is achieved through the utilization of Message Digest-5 (MD5) algorithm. It offers higher efficiency with respect to the execution period, the length of the encrypted data, and the power requirement in Wireless Sensor Networks.

4. Security Requirements of Wireless Networks

The methodologies need to be proposed for securing the sensitive process information and protecting the plant equipments from unauthorized access and attacks. Intruders can access or modify the sensitive process data communicated over internet. The process and control variables should not be accessed and modified by the intruders during transmission across wireless networks. The security mechanism is developed that decrease the hazard corresponds to secure non-cyclic real-time operations compiling on servers [22]. The performance of security mechanism is analysed in terms of latency and energy.

4.1 Data confidentiality

Data confidentiality is a technique that assures the process messages and data must not be eavesdropped to the intruders. The security mechanisms on low powered devices are monitored which usually originate in internet [17]. The

process data can be kept confidential by converting it into unreadable format by encryption. The cipher text is obtained from the encryption which is communicated across wireless medium. The decoding process takes place at the destination to obtain the unreadable text back into readable plain text. The key length of 2048-bit is produced from the proposed public key encoding and integrity is achieved through the proposed 512-bit hash function [7]. Authentication of plant information across internet is achieved through this security algorithm. The modified symmetric encryption with two keys operated that is utilized to produce cipher text file for guaranteed communication [28]. The compilation time required for asymmetric algorithm is high that results in computing delay of internet operations.

4.2 Data integrity

It ensures plant parameters must not be altered at the time of communication. The technique proposed for tracking the code integrity for application oriented processors is proposed [32]. It can be used to identify the code integrity over a vast range.

4.3 Authentication

Authentication is the process of determining and verifying the individuals in the communication medium. Individuals should have their own user name and password to utilize the resources. It allows the industries to secure the networks by permitting only genuine users to give rights to utilize the resources include equipments, files, communication medium, servers and other network-based services. Authentication mechanism is proposed with an end-to-end dual encoded information architecture [9]. It operates without utilization of external digital certificates, provides powerful confidentiality and it does not require authentication of third parties.

4.4 Availability

Availability is a security mechanism that ensures the networks, devices, information and data should be available to authorized users at any time.

4.5 Access Control

Access control mechanism is a technique that allows accessing of resources and modifies the information only by the authorized users. The main concern in utilizing the technique for access control to wireless networks is proposed [14]. The protocols for IoT are not applicable for low powered networks. The access control mechanism is needed for accessing the resources of wireless networks.

5. Proposed Heterogeneous Cryptography Algorithm

This compound cryptography algorithm is proposed which is based on public key, symmetric key and hash algorithms that strengthens the security of sensitive plant information. The key length of 1024-bit is produced using RSA public key cryptography. The symmetric AES encryption of 128-bit key length is proposed that encodes the process data and produces the output in unreadable format. The MD5 hash function is proposed to produce the hash data that assures plant information unaltered across IoT. The computations of this security mechanism is high speed, offers low latency and safety for industrial devices and plant operators.

Generation of Security Key

Encryption

- Generation of two prime values, a and b
- Calculate

$$y = a * b \tag{1}$$

$$\emptyset = (a-1)(b-1) \tag{2}$$

- Select ‘r’ data, $1 < r < \emptyset$, with

$$\gcd(r, \emptyset) = 1 \tag{3}$$

- Calculate the private key s, $1 < s < \emptyset$, with

$$r*s = 1 \bmod \emptyset \tag{4}$$

- The key open to everyone is (y, r) and the key is accessed only by authorized user is (y, s)
- Keep each data s, a, b and φ secret
- Generation of encoded data,

$$e = d^r \bmod y \tag{5}$$

y – Modulus, r – Public key, s- Private key
e - Encoded data, d – Original numerical data

- Generation of symmetric key through symmetric encryption
- Generation of hash value

Data Decryption

- Generation of decoded data,

$$d = e^s \bmod y \tag{6}$$

- Symmetric decryption is performed
- Plain text is monitored over internet

The generation of security key involves encryption and decryption. Encryption is the process of reading the plain text as input and converts it into equivalent cipher text. In the above encryption algorithm, equation (5) is used to find the cipher text for the input numerical data. The public key denoted by 'r' is required to convert the input data into cipher text. Encryption algorithm is utilized to ensure data confidentiality across internet. The MD5 (Message Digest) hash algorithm is integrated with the encryption in order to generate hash value. The hash algorithm ensures that the data cannot be modified by the attackers during transmission over internet. Decryption is the process of converting the cipher text back to plain text. Equation (6) is used to find the original data from the cipher text. The private key denoted by 's' is required to convert the cipher text into plain text.

6. Flowchart of Proposed Heterogeneous Cryptography Algorithm

The flowchart of this proposed cryptography algorithm is shown in figure 1 and figure 2.

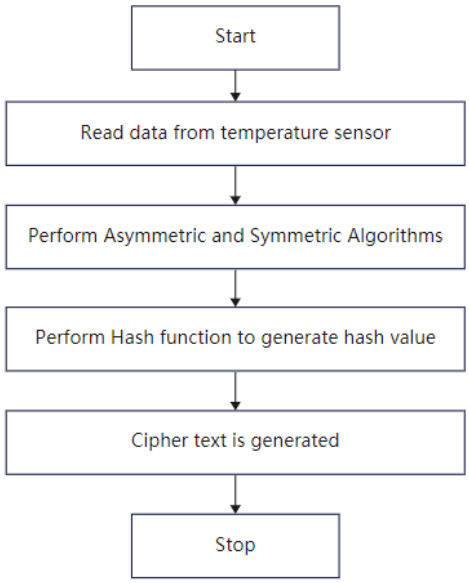

Fig. 1. Flowchart of proposed Encryption algorithm

This proposed cryptography is formulated and verified experimentally using hardware. Embedded system reads the temperature data from the plant and encodes it to produce unreadable text. The symmetric AES encoding is performed that converts the numerical process data into unreadable data. This proposed symmetric algorithm provides data confidentiality and hash function ensures data integrity. The cipher text generated at the transmitter and the plain text produced at the receiver can be monitored only by the authorized users at the web page.

The privacy and authentication mechanisms are addressed through the dual techniques encryption [29]. The dual encoding mechanisms are utilized that is related to block encryption and the other is AES encoding. It strengthens the safety level and identifies the authorized users across wireless medium. Symmetric AES and asymmetric RSA both together increase the level of data security and provide effective key management.

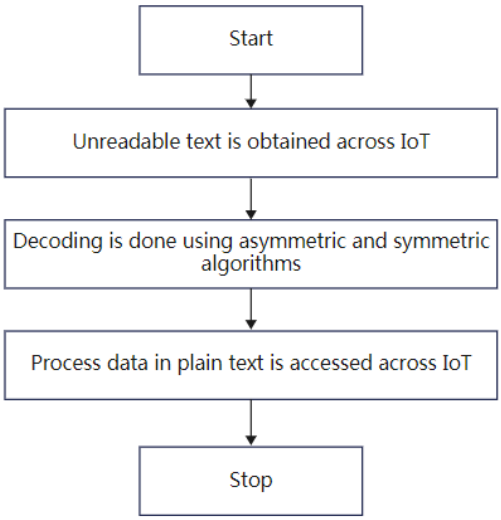

Fig. 2. Flowchart of Proposed Decryption algorithm

This proposed work involves symmetric key, public key and hash functions to strengthen the security of plant sensitive information. Figure 3 shows the proposed encryption and decryption of plant parameter with embedded system through internet. The public key encryption is used to produce the unreadable text and its output is taken for AES encoding to produce unreadable data. The hash function produces the hash value in order to ensure process data unaltered during transmission across internet. The numerical plain text is obtained by the process of decoding the cipher text at the destination. The cipher text and the numerical process variable to be accessed through the IoT.

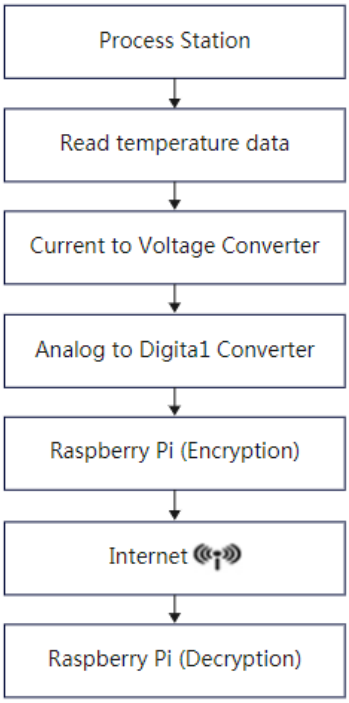

Fig. 3. Flow diagram of Encoding and Decoding of Plant Parameter with Embedded System through Internet

7. Results and Discussion

This hybrid security mechanism is written in python and it is implemented in embedded system. It accesses the temperature value and encodes it to get the encrypted data. The hash function is utilized to provide data integrity across internet. It accesses the plant information in unreadable text through wireless medium. The hardware setup of embedded system with IoT is shown in the figure 4.

Figure 5 shows the embedded system with IoT at the transmitter side. Embedded system is used to read the process temperature data and performs encryption. Encryption is the process of converting the input temperature value in

original plain text into encrypted form. This cipher text is transmitted through the inbuilt Wi-Fi in the embedded system that enables communication of plant temperature data across internet.

Figure 6 indicates the monitoring of plant parameter in real-time. The security algorithm is developed using python to access and display the temperature value. It allows accessing and monitoring of plant data in online mode.

Fig. 4. Hardware setup of Embedded based Wireless Secured Transmission of Process data

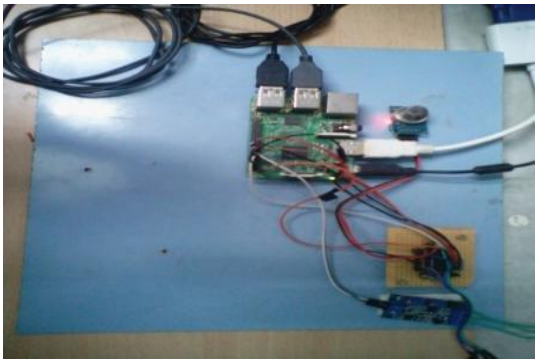

Fig. 5. Embedded System with IoT for transmission of Process Data

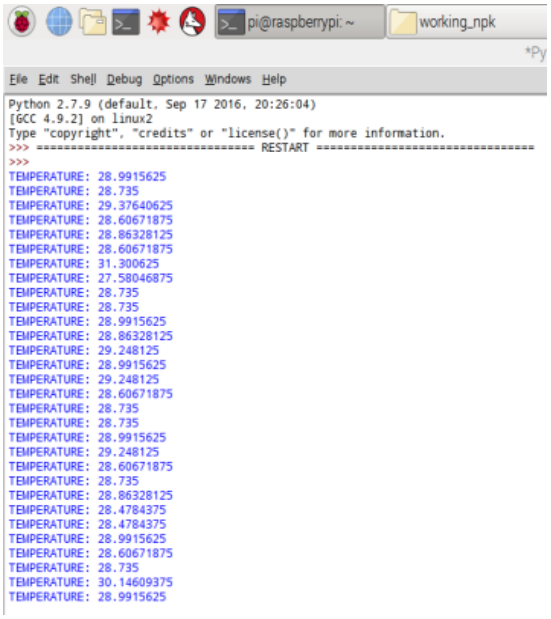

Fig. 6. Monitoring of temperature process variable using Embedded System

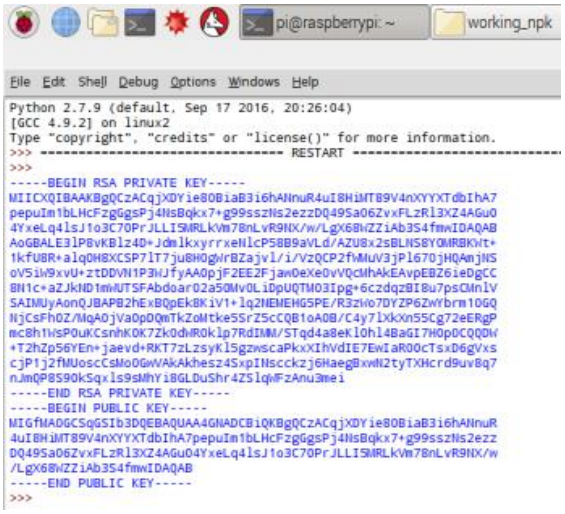

Fig. 7. Dual Key Generation from Asymmetric RSA Algorithm

Figure 7 shows the generation of key from the symmetric and asymmetric algorithms. It produces key length of 1024-bit that enhances the security. The asymmetric algorithm is utilized for encoding the plant parameters to generate the unreadable text and the private key is used for decoding the unreadable data to generate the plant parameters in plain text. Figure 8 shows the temperature process data in unreadable cipher text accessed across the IoT. This unreadable ciphertext is transmitted across internet. It assures data confidentiality and hash function assures process variables should not be modified by the intruders. Figure 9 shows the embedded system with internet based plant information reception. The cipher text is received and it is decoded to obtain the plant data in numerical values. Figure 10 shows the readable plain text acquired through the process of decoding performed at the receiver. The latency of this proposed cryptography algorithm is very low and it is of the order of 0.027 milli-seconds.

Fig. 8. Temperature process parameter in Cipher text monitored through IoT

Fig. 9. Embedded System with IoT for plant parameter reception

Fig. 10. Receiver section of monitoring of Temperature Parameters in Plain Text

Figure 11 shows the original plain text gathered through the IoT. The correct file name is to be entered in the web page to monitor the temperature value across IoT.

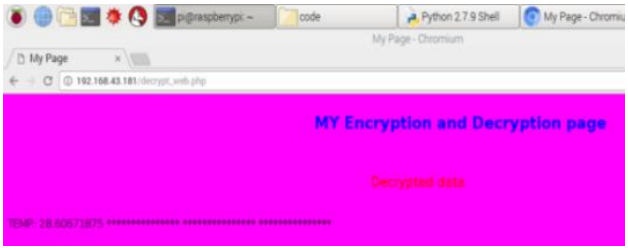

Fig. 11. Temperature process parameter accessed through the IoT at the receiver

Cryptography is the technique of converting the input raw data into unreadable cipher text. It involves symmetric and asymmetric algortihms to generate cipher text from the plain text. Hash algorithms are used to ensure data unaltered during transmission over internet. These security algorithms can be programmed using Python language. Raspberry Pi contains inbuilt ARM processor and Wi-Fi that enables programming in python and transmits the unreadable cipher text across internet. The various industrial process parameters are detected through sensors, and transmit the output signal to the embedded ARM processor. Python code can be implemented in the Raspberry Pi operating system. This python code reads the process data from the sensors and generates cipher text. The decryption is performed at the receiver to convert the cipher text back into original plain text. The encrypted unreadable text and decrypted text can be monitored through the internet by providing the correct IP address of the Raspberry Pi board.

Table 1 shows the comparison between standard and proposed cryptographic algorithms. The standard cryptographic algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), triple DES, RC2, RC5, and Blowfish algorithms. This proposed hybrid algorithm combines the features of Asymmetric, Symmetric, and hash functions and it is implemented in high speed embedded ARM cortex processor. The speed of encryption of this proposed hybrid algorithm is very high of 0.0006079 ms (milli-seconds) as compared to standard cryptographic algorithms and it achieves high level of security.

This proposed work enables only the genuine users to gather and modify the plant messages through IoT. This hybrid cryptography mechanism ensures secrecy and validation of process parameters and hash function assures process data unaltered during transmission through wireless medium. It is implemented and experimental verification is done using hardware and accessing the process variables across internet. It consumes very less compilation time and it strengthens the level of security. The advantage of this hybrid cryptography is the usage of cost-effective embedded devices, cryptography at various level, communication of plant data through wireless networks and accessing of plant information over internet. It is suitable for secure communication and accessing of enterprise plant data over internet.

Table 1. Comparison between Standard and Proposed Cryptographic Algorithms

Algorithm	Key size	Block size	Rounds	EncryptionSpeed	Security Level
AES	128, 192, 256 bits	128 bits	10, 12, 14	128 bits - 0.0468 ms 192 bits - 0.0476 ms 256 bit - 0.0498 ms Fast	Considerably Secure
DES	56-bits	64 bits	16	92 ms Very Slow	Inadequate Security
3 DES	112-bits	64 bits	48	176 ms Very Slow	Adequate Security
RC2	8-128 bits	64 bits	18	7.19 msFast	Vulnerable
RC5	2040 bits	128 bits	255	0.90 msFast	Considerably Secure
Blowfish	32-448 bits	64 bits	16	7.03 ms Fast	Vulnerable
Proposed Algorithm(RSA, AES and MD5)	1024-bit, 128-bit, and 128-bit	86 bytes, 16 bytes, and 512-bit	10 for AES, 4 for MD5	0.0006079 ms Very Fast	Highly Secure

This proposed hybrid cryptography includes Asymmetric, Symmetric, and Hash algorithms that increase the level of security. The large key size of 1024-bit is generated using asymmetric algorithm that strengthens the security. This proposed symmetric and asymmetric algorithm assures data confidentiality and authentication of process parameters. Hash algorithm ensures that the process data cannot be modified by the attackers. This proposed hybrid cryptography is implemented using embedded processor with high speed of 1.2 GHz clock frequency and monitoring of process data through internet.

The energy efficiency can be attained by incorporating low energy security protocols. New models of energy storage and usage can increase the life of batteries or even remove their use entirely. This can be achieved by using energy harvesting to power the device when energy is available and returning to using a battery when the stored harvesting energy is exhausted.

8. Conclusion

The security algorithms are necessary to preserve the valuable industrial equipment against variety of attacks. Due to the wide usage of IoT in variety of applications, information can be easily hacked and altered by the attackers. This leads to abnormal functioning of plant operations and results in failure of process devices. The security mechanisms are essential to protect the sensitive process data and plant information against unauthorized access and modification. The hybrid cryptography is proposed that produces key length of 1024-bit using public key RSA algorithm and 128-bit key length using AES encoding that ensures secrecy and authentication of process parameters. The benefit of this proposed algorithm is it has the capability to perform encoding at different levels and the hash function assures unalteration of process data by the intruders. This security algorithm offers low latency in compilation of encoding and decoding. The implementation cost is very low due to the usage of embedded system and it is suitable for wide variety of applications. The security framework is essential and need to be proposed for IoT based applications.

References

[1] Fatima Alwahedi, Alyazia Aldhaheri, Mohamed Amine Ferrag, Ammar Battah, Norbert Tihanyi, “Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models,” Internet of Things and Cyber-Physical Systems, Vol. 4, pp. 167-185, 2024

[2] Shamshair Ali, Rubina Ghazal, Nauman Qadeer, Oumaima Saidani, Fatimah Alhayan, Anum Masood, Rabia Saleem, Muhammad Attique Khan, Deepak Gupta, “A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks,” Alexandria Engineering Journal, Vol. 103, pp. 88-97, 2024.

[3] Danish Javeed, Muhammad Shahid Saeed, Ijaz Ahmad, Muhammad Adil, Prabhat Kumar, A.K.M. Najmul Islam, “Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions,” Future Generation Computer Systems, Vol. 160, pp. 577-597, 2024.

[4] Vinay Gugueoth, Sunitha Safavat, Sachin Shetty, “Security of Internet of Things (IoT) using federated learning and deep learning Recent advancements, issues and prospects,” ICT Express, Vol. 9, No. 5, pp. 941-960, 2023.

[5] J.S.Prasath, U. Ramachandraiah, S. Prabhuraj, G.Muthukumaran, “Internet of Things based Hybrid Cryptography for Process Data Security,” Journal of Mathematical and Computational Science, Vol. 10, no.6, pp. 2208-2232, 2020.

[6] J.S.Prasath, U.Ramachandraiah, G.Muthukumaran, “Modified Hardware Security Algorithms for Process Industries using Internet of Things,” Journal of Applied Security Research, pp. 1-14, 2020.

[7] J.S.Prasath, U.Ramachandraiah, “Modified Asymmetric and Hash Algorithms for Internet Enabled Industrial Automation,” Test Engineering and Management Journal, Vol. 83, pp. 7431-7444, 2020.

[8] J.S. Prasath, S. Jayakumar, K. Karthikeyan, "Real-Time Implementation for Secure monitoring of Waste-Water Treatment Plants using Internet of Things," International Journal of Innovative Technology and Exploring Engineering., Vol. 9, no. 1, pp. 2997-3002, 2019.
[9] Aniruddha Bhattacharjya, Xiaofeng Zhong, Jing Wang, "An End-to-End User Two-way Authenticated Double Encrypted Messaging Scheme based on Hybrid RSA for the future Internet architectures," International Journal of Information and Computer Security, Vol. 10, No. 1, pp. 63-79, 2018.
[10] Mauro Conti, Ali Dehghantanha, Katrin Franke, Steve Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, Vol. 78, pp. 544-546, 2018.
[11] Mahmoud Ammar, Giovanni Russello, BrunoCrispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, Vol. 38, pp. 8-27, 2018.
[12] Arbia Riahisfar, Enrico Natalizio, Yacine Challa, Zied Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, Vol. 4, pp. 118-137, 2018.
[13] Minhaj Ahmad Khan, Khaled Salah, "IoT security: Review, block chain solutions, and open challenges," Future Generation Computer Systems, Vol. 82, pp. 395-411, 2018.
[14] Kewei Sha, WeiWei, T.AndrewYang, Zhiwei Wang, Weisong Shi, "On Security Challenges and open issues in Internet of Things," Future Generation Computer Systems, Vol. 83, 326-337, 2018.
[15] Chunyong Yin, Jinwen, Xi, Ruxia, Sun, Jin, Wang, "Location Privacy Protection based on Differential Privacy Strategy for Big Data in Industrial Internet of Things," IEEE Transactions on Industrial Informatics, Vol. 14, No. 8, 3628-3636, 2018.
[16] Fadele Ayotunde Alaba, Ibrahim Abaker Targio Hashem, "Internet of Things security: A Survey," Journal of Network and Computer Applications, Vol. 88, pp. 10-28, 2017.
[17] Sikhar Patranabis, Abhishek Chakraborty, Debdeep Mukhopadhyay, Partha Pratim Chakrabarti, "Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-Like Block Ciphers," IEEE Transactions on Information Forensics and Security, Vol. 12, Issue 5, pp. 1092-1102, 2017.
[18] Aafaf Ouaddah, HajarMousannif, AnasAbou Elkalama, Abdellah Ait Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," Computer Networks, vol. 112, 237-262, 2017.
[19] Hamed Hellaoui, Mouloud Koudil, Abdelmadjid Bouabdallah, "Energy-Efficient mechanisms in Security of the Internet of things: A Survey" Computer Networks, Vol. 127, 173-189, 2017.
[20] Sandeep K. Sood, "Advanced dynamic Identity-based Authentication Protocol using Smart Card," International Journal of Information and Computer Security, Vol. 8, No. 1, pp. 11-33, 2016.
[21] Lukas Malina, Jan Hajny, Radek Fujdiak, Jiri Hosek, "On perspective of Security and Privacy-preserving solutions in the Internet of Things," Computer Networks, Vol. 102, 83-95, 2016.
[22] Puneet Kumar, Shashi B. Rana, "Development of modified AES algorithm for Data Security," Journal of Optik, Vol. 127, Issue 4, 2341-2345, 2016.
[23] Mohamed Elhoseny, Hamdy Elminir, Alaa Riad, Xiaohui Yuan, "A secure data routing scheme for WSN using Elliptic Curve Cryptography and homomorphic encryption," Journal of King Saud University - Computer and Information Sciences, Vol. 28, Issue 3, pp. 262-275, 2016.
[24] Rakesh Kumar, Geetu Mahajan, "A novel framework for secure file transmission using modified AES and MD5 algorithms," International Journal of Information and Computer Security, Vol. 7, No. 2, pp. 91-112, 2015.
[25] Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communication Surveys and Tutorials, Vol. 17, No. 3, pp. 1294-1312, 2015.
[26] Wei Jiang, Yue Ma, Nan Sang, Ziguo Zhong, "Dynamic Security management for real-time embedded applications in Industrial Networks", Computers and Electrical Engineering, Vol. 41, pp. 86-101, 2015.
[27] RawyaRizk, YasminAlkady, "Two-phase hybrid cryptography algorithm for Wireless Sensor Networks," Journal of Electrical Systems and Information Technology, Vol. 2, Issue 3, pp. 296-313, 2015.
[28] Prakash Kuppuswamy, Saeed Q.Y. Al-Khalidi, "Hybrid Encryption/Decryption technique using new Public Key and Symmetric Key algorithm," International Journal of Information and Computer Security, Vol. 6, No. 4, pp. 372-382, 2014.
[29] Rodrigo Roman, Jianying Zhou, Javier Lopez, "On the features and challenges of Security and Privacy in distributed Internet of Things," Computer Networks, Vol. 57, 226-2279, 2013.
[30] Wei Jiang, ZhenlinGuo, Yue Ma, Nan Sang, "Measurement-based research on Cryptographic Algorithms for Embedded real-time systems," Journal of Systems Architecture, Vol. 59, 1394-1404, 2013.
[31] ChalapathiRao, Santhi Rani, Lavanya, "Monitoring and Protection of Oil and Gas Condition in Industrial Using Wireless Sensor Networks," International Journal of Electronics Communication and Computer Technology, Vol. 2, No. 5, 213-218, 2012.
[32] Hai Lin, YunsiFei, Xuan Guan, Zhijie Jerry Shi, "Architectural Enhancement and System Software Support for Program Code Integrity Monitoring in Application-Specific Instruction-Set Processors", IEEE Transactions on Very Large Scale Integration Systems, Vol. 18, pp. 1519-1532, 2010.

Authors' Profiles

J. S. Prasath received Master of Engineering degree in Process Control and Instrumentation Engineering from Annamalai University, Chidambaram and Doctor of Philosophy degree in Wireless Sensor Networks for Industrial Security from Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as an Associate Professor in the Department of Computer Science and Engineering at Sapthagiri NPS University, Bengaluru, India. He is an interdisciplinary and guiding many Research projects at Under graduate and Post graduate level. Earlier he served as Assistant Professor in SRM University, Hindustan University, KCG College of Technology and Narayana Engineering College. His research interests are Embedded Systems, Wireless Sensor Networks, Internet of Things, Process Control and Industrial Automation. He has published eighteen articles in International Journals, presented sixteen papers in International Conference, published two patents, written one book and one book chapter. He received the best teacher award and the two innovation awards for his research work.

How to cite this paper: J. S. Prasath, "Implementation of Internet of Things Based Data Security Using Hybrid Cryptography", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.15, No.3, pp. 66-77, 2025. DOI:10.5815/ijwmt.2025.03.05