Heterogeneous Cryptographic Algorithm for Internet of Things Based Embedded Wireless Security

Prasath J S (jsprasath@gmail.com)
KCG College of Technology https://orcid.org/0000-0002-8718-1494

Research Article

Keywords: Encryption, Decryption, IoT, Embedded System, Wireless Networks

Posted Date: June 24th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-397546/v1

Abstract

The technologies in monitoring and control of industrial process have changed due to the rapid growth of emerging technologies especially the most popular Internet of Things (IoT). The Internet is an essential part of day-to-day life and it is used to gather more information. The emerging trend in the field of industrial automation is the integration of embedded systems with wireless technologies which enables monitoring of process information through the internet. As the internet is the open environment, a lot of security issues and vulnerabilities arise to the industrial devices. The usage of internet in process monitoring enables attackers to monitor and change the process data. The unsecured industrial operations lead to failure of process equipment and safety issues to plant operators. The security mechanisms are essential in order to protect the embedded systems and wireless networks from unauthorized access. This proposed heterogeneous security algorithm includes symmetric, asymmetric and hash algorithms which strengthen the level of security. The novelty of the proposed work is it employs 128-bit key size for symmetric encryption, 1024-bit key size for asymmetric encryption along with the use of hash algorithm all together strengthens the security and it is tested in real time using embedded system with IoT. It takes less time for execution of data encryption and decryption. This proposed hybrid security algorithm is implemented and tested in an embedded system with wireless monitoring of process information through the internet. It ensures secure communication and monitoring of process data through the internet. The attacker cannot identify and modify the plant information transmitted across internet. This proposed work can be applied to industries dealing with sensitive process information.

I. Introduction

The embedded system with wireless networks is the future trends in process industry applications. With the advent of IoT, the process data can be transmitted and monitored through the internet. The wireless networks are subjected to a variety of attacks and the challenging task is to secure the plant sensitive data from the attackers. The internet is an open environment and the attackers try to access and modify the process data. This results in data loss and failure of process equipments. It also leads to unsafe operating conditions. The security mechanisms are required in order to ensure smooth plant operations. The varieties of security algorithms are available for securing the process information. The security algorithms differ from key size, number of rounds and number of bits used for encryption. The optimized security algorithm should be chosen depends on the type of process and information to be transmitted.

The real world data is acquired, collected and processed by the IoT. The major issue of IoT is to ensure data security and privacy protection. The wide usage of IoT requires strong security mechanism to preserve the resources from the third party attacks. The security is essential at all layers of the IoT system. The various challenges in securing the IoT are addressed [2]. The security mechanisms are required for the various challenges include authentication, authorization and privacy. The lack of awareness and mechanisms exists in industrial network security. With the advent of IoT, the sensitive plant information can be monitored through the internet. The enterprises and end user based IoT

applications framework and platforms are analyzed [3]. The study of the frameworks was carried out depend on the hardware agreeableness, architecture, software concerns and security. The challenging task is to develop the applications for IoT due to the highly complicated shared computing, inadequacy of frameworks that handle low level interchange and make easier high level application, heterogeneous coding languages and different protocols for data transmission. The various energy efficient mechanisms are addressed [9] in IoT security services. The energy saving mechanisms are applied to the deployment environment and the target protocol. The energy efficient services can be provided by incorporating security protocols which consumes less power.

Ii. Security Issues In Wireless Networks

The security is a major issue in sensor networks due to the communication of plant sensitive information. The security becomes complexity and the risk of physical attacks is high due to the limitations of resource constrained Wireless Sensor Networks (WSN). The security and privacy challenges of IoT are addressed [4] which are related to privacy, faith, identification and access control. The powerful authentication standards to be proposed for IoT and attention need towards IoT ecosystem. The authentication, ID and password are necessary for internet enabled devices.

The security mechanisms are essential to protect the sensor network from all kinds of attack. The security issues regarding layered architecture of IoT, network protocols, communication and network management are addressed [5]. The security issues are categorized into low level, intermediate level and high level. The bottom level security issues are concerned with physical and data link layers of communications as well as hardware level. The medium level security issues deals with the communication, routing and managing the sessions related to network and transport layers of IoT. The top level security issues are concerned with the IoT applications. The cryptography mechanisms are the most crucial tools that ensure security in WSNs. The protocols and texture to secure communications in the IoT are analyzed [13]. The Internet Engineering Task Force (IETF) and the IEEE together designed the advanced communication and security protocols which enables wide usage of IoT in various applications. The research issues and proposals for security at different layers are discussed. This extensive survey enables researchers to develop modern solutions to notify the security issues with regard to communication protocols of IoT.

The sensor network is growing rapidly and a great issue for security administrators is to ensure secure network operations. The security threats increases due to the usage of Local Area Networks (LAN) and Internet. The security challenges are analyzed based on the significant characteristics of the IoT systems and the advanced features of the IoT applications [6]. Most of the end devices are inadequate to support lightweight protocols. The public key schemes are utilized in most of the existing all around security solutions in the protocol design. There are open research issues regarding end-to-end security. The challenging task is to address the safety issues of end devices. It is necessary to ensure privacy and security of sensitive information over internet. Authentication plays a major role in securing the messages transmitted across wireless networks. The remote user authentication is essential for ensuring secure

communication. An efficient password based remote user authentication scheme is proposed using smart card [10]. It offers low computational cost and very strong against all well-known security attacks. The server and the user agree on common session key and the messages communicated between the user and the server is encrypted with this session key. This type of authentication is required for corporate networks. The unique methodology is necessary to provide the complete security solutions for securing the process information and the entire network system.

The conventional encryption algorithms are unsuitable for rapidly increasing security issues. The attackers can easily hack the process information and modify the data. The existing security threats, vulnerabilities and potential attacks on IoT are analyzed [7]. The analysis of security threats are based on architecture, communication and application. The IoT applications can be secured with the support of universal IoT security architecture. The security issues of the dispersed approach of the IoT are reviewed [16]. The decentralized approach increases the complexity of various security mechanisms. The applications of IoT will have to undergo particular amount of fake data. Although the numbers of attack vectors are lesser, a single vulnerability results in severe breakage to the entire network. If the network resources are disseminated, the number of successful attack becomes less, but the number of attack vectors continues to rise.

The security attacks are rapidly growing in wireless networks. The attackers can damage the network and target the end system. The attacks lead to failure of equipments, malfunctioning, operator safety issue and major loss to enterprises. The process information should also not modified by the attackers. Embedded system architecture is proposed for medium to high level processors which assures integrity and confidentiality [18]. The configured processor operates in a secure mode which allows compilation of only trusted programs. It is essential to propose the high performance hardware system to protect the data. The process industries should consider the security as a primary concern and implement suitable security mechanisms depend on the possible attacks.

Iii. Security Requirements In Wireless Networks

The security requirements are increasing due to the open nature of the wireless medium. The attackers can monitor or alter the sensitive information that is transmitted across wireless networks. It is necessary to ensure that the message is sent to the destination without alteration. A Dynamic Security management mechanism is proposed [14] which reduce the risk related to security and process rejection ratio of aperiodic real-time tasks running on servers. The performance of security algorithms are measured with respect to time and energy. The major security issues in wireless networks include confidentiality, availability, integrity, authentication and access control.

A. Data confidentiality

It is the process of ensuring that the information should not be leaked to the attackers. The performance of the security algorithms on constrained devices are accessed which generally arise in IoT networks [11]. The analysis of symmetric and asymmetric algorithms shows that the implementation of symmetric

ciphers and hash functions into the IoT is easy task. On the other hand, asymmetric algorithms take more time for execution which causes a delay in processing of IoT applications.

B. Data integrity

It ensures that the information should not be modified during the transmission. A methodology proposed for code integrity monitoring for application-specific processors [17]. The execution trace is monitored online and tests whether it fix with the program behavior that is expected. This proposed system can be used to detect the program code integrity over a wide range. The data should be accessible only to authorized users.

C. Authentication

It ensures the identification and confirmation of users in wireless networks. Each user must have username and password in order to access the resources. It enables the enterprises to keep their networks secure by allowing only authenticated parties to access the resources include databases, networks, files, systems, and other network-based services. An end-to-end authenticated double encrypted messaging architecture is proposed [1]. It is based on hybrid RSA algorithm which is specifically applied for future internet architectures. It can work without external digital certificates, provides strong confidentiality and no need of third party authentication. It is an essential security mechanism to ensure data security and privacy.

D. Availability

It is the process of assuring the resources and networks are available for authorized access. The attack prevents the end system to be accessed by the authorized parties.

E. Access Control

It ensures that only the authorized parties should access the resources and the information communicated across the networks. The main challenges in employing access control mechanisms to IoT are addressed [8]. The widely used internet protocols cannot be suitable for constrained environments. A modern access control technique is required for network sharing of IoT.

F. Data freshness

It is the process of confirming that the received process information is latest and previous information has not been replayed. A counter should be included along with the process information to ensure data freshness.

G. Self-Organization

A WSN requires all wireless nodes to be independent and it should have the capability of self-organizing. In sensor network, the infrastructure keeps on changing which are used for the managing the network,

which make WSN security more challenging.

H. Time synchronization

The sensor network used in applications is based on some form of time synchronization. It is essential for basic communication and it detects movement, location and proximity. The issues in synchronization include access time, transmit time, receive time and propagation time. It is the problem of synchronizing the clocks across a set of sensor nodes.

I. Secure Localization

The usage of sensor network mostly relies on its ability that it automatically and accurately detects each sensor in the network. In order to point out the accurate fault, the location information is required in a sensor network. An attacker can easily exploit this situation and can manipulate non-secured location information.

Iv. Proposed Hybrid Security Algorithm

This proposed hybrid security algorithm combines the asymmetric, symmetric and hash function cryptography which provides strong security during transmission of data. The random private key is generated using RSA security algorithm, where the key size is 1024-bits. The AES (Advanced Encryption Standard) symmetric encryption of 128-bits key size is used which converts sensor data into cipher text. The hash algorithm is used to generate the hash value for a given key. The use of hash algorithm ensures data integrity over internet.

The modified AES algorithm with two keys is proposed [12] which are used to generate encrypted file for secure transmission. The MD5 hash algorithm is applied to the encrypted file that will produce a hash code. The file is transmitted to the receiver using client-server architecture. The receiver verifies that no modifications have been made to the files by matching it with the hash code received in hash file. This security mechanism provides integrity and data confidentiality to the files. The computations of this algorithm is fast, takes less time and provides better solution for data security.

A. Key Generation

Data Encryption

- Generate two Prime numbers, x and y
- Compute z=x*y and φ = (x-1) (y-1)
- Choose a value for p, 1 < p < φ, such that gcd (p, φ) = 1
- Compute the secret component q, 1 < q < φ, such that p*q=1 mod φ
- The public key is (z, p) and the private key is (z, q)

- Retain all the values q, x, y and φ secret
- Computes the cipher text, $c = m^p \bmod z$
  z – Modulus, p – Public key, q- Private key
  c- Cipher text, m –Original message/data
- Performs symmetric encryption
- Generate hash value for a given key

Data Decryption

- For decryption, compute the original text, $m = c^q \bmod z$
- Performs symmetric decryption
- Plain data is read through internet

V. Flow Chart

The flowchart for the proposed hybrid encryption and decryption security algorithm is shown in Fig. 1 and Fig. 2.

The temperature and gas sensor data is taken as input. The key is essential to encrypt the sensor data. The symmetric encryption is performed to get cipher text for the sensor data. The message digest (MD5) algorithm is used to generate hash value for a given key. The key cannot be modified by the attackers during the transmission and it ensures integrity of process information. The IP address is necessary to view the cipher text and key in hash format.

When the process data changes in a decimal point, the public and private keys also change. The 1024-bits private key is generated which is larger in size and it strengthens the security. This private key is used for decryption and public key is used for encryption. A two way secured data encryption system is proposed [15] which address the concerns of user's privacy, authentication and accuracy. The two different encryption algorithms are applied in which one is based on linear block cipher and the other is symmetric algorithm. It enhances the level of security and provides authentication. The use of AES along with RSA algorithms is more efficient for key management to ensure data security during transmission.

Vi. Key Management In Embedded Based Wireless Network Security System

The key management is an essential part in secure communication of process information over wireless networks. The different techniques are available for key management throughout the communication. A secure path should be identified in order to communicate process data between source and destination nodes. This path travels through a series of nodes that contains secure channels. The transmitter node initiates secure data transmission, when the path is established.

Vii. Implementation Of Proposed Security Algorithm Using Embedded System

This proposed hybrid security algorithm is a combination of symmetric, asymmetric and hash algorithms which achieves higher level of security. It reads the sensor data and performs asymmetric encryption using public and private keys. The cipher text obtained from the asymmetric encryption is further given to symmetric encryption to generate new cipher text.

The hash algorithm used in this proposed work generates hash value and it ensures data integrity. The encryption algorithm is performed using embedded system. The final encrypted data is transmitted across internet. The decryption algorithm is performed at the receiver. The encrypted data and the original sensor data can be monitored through the internet by providing the IP address.

This proposed hybrid security algorithm is implemented in embedded system with wireless monitoring of process information through the internet. The temperature process is monitored from the process station. The temperature transmitter generates current signal equivalent to process temperature. This current signal is converted into voltage by using current to voltage converter. The continuous time voltage signal is converted into digital value by using Analog to Digital Converter (ADC). This digital signal of process data is fed to the raspberry pi.

The process data is encrypted using raspberry pi and transmitted through internet. The encrypted data is received through the internet at the receiver. The decryption is performed using raspberry pi at the receiver. The decrypted data can be monitored through the internet.

Viii. Results And Discussion

This proposed hybrid security algorithm is programmed using python language. The proposed security algorithm reads the temperature process data through the sensor. This process data is encrypted using asymmetric and symmetric cryptography. The hash algorithm is also included in order to generate hash value for a given key. It enables monitoring of process data in cipher text through the internet. The experimental setup of the embedded based wireless security system is shown in the Fig. 4.

The Fig. 5 shows the transmitter section of the embedded based wireless process data monitoring system. It includes current to voltage converter which converts temperature transmitter current into voltage, Analog to Digital Converter which converts analog temperature data into digital and raspberry pi processor board which performs data encryption. It enables to read the temperature process data in encrypted form through the internet.

The Fig. 6 shows the temperature process data obtained by compiling the python code. It enables to read the process data to be monitored online.

The Fig. 7 shows the public key and private key. The private key of 1024-bits is generated which is larger size. The large key size strengthens the level of security. The public key is used for encrypting the process data to obtain the cipher text and the private key is used for decrypting the cipher text to obtain the sensor data in numerical form.

The Fig. 8 shows the encrypted data monitored through the internet. The IP address is essential to read the sensor data in cipher text.

The Fig. 9 shows the receiver section of embedded based wireless process monitoring system. It receives the cipher text and performs decryption to read the process data in original form. It is connected to the internet which enables monitoring of temperature data through the internet by providing the required IP address.

The Fig. 10 shows the decrypted data obtained by compiling the decryption algorithm at the receiver. The time taken for execution of decryption algorithm is very less which is 0.027 milli-seconds.

The Fig. 11 shows the decrypted data monitored through the internet. The receiver node IP address is essential to obtain the temperature data.

This proposed work allows secure monitoring of industrial process parameters through the internet. This proposed hybrid cryptographic algorithm provides confidentiality and authentication of sensitive plant information and hash algorithm ensures data integrity over wireless networks. This proposed hybrid security algorithm is implemented and tested with the embedded system and accessing the process data through internet. This proposed security algorithm consumes very less time for execution and achieves higher level of security. The benefit of this proposed work is the cost-effective embedded system, multi-level security algorithms, wireless transmission and monitoring of process parameters through internet. It is applicable for secure transmission and monitoring of any industrial sensitive process information over internet.

Ix. Conclusion

The security is an essential part in monitoring and control of industrial process information. The modern technologies enable access to process data through the internet. The sensitive process information can be accessed and modified by the unauthorized parties. The industrial equipments are susceptible to security attacks. It is necessary to incorporate the security mechanisms in process monitoring in order to protect the industrial devices. The novelty of the proposed heterogeneous security algorithms is it performs multiple encryptions and the use of hash algorithm which ensures data integrity. This proposed hybrid security algorithm is implemented in embedded systems with wireless monitoring of process information through the internet. It enables secure transmission and monitoring of various industrial processes with the internet. It achieves low latency during the execution of data encryption and decryption. This proposed work is the cost effective solutions and it can be used for broad range of

industrial applications. The security algorithm protects the expensive industrial devices and provides safety to plant operators.

Declarations

I hereby declare that the manuscript titled “Heterogeneous Cryptographic Algorithm for Internet of Things based Embedded Wireless Security” submitting to the Journal “Wireless Personal Communications”.

This article has no funding support and the research work undertaken is self-sponsored.

I assure that there is no conflicts of interest in submitting this article to the Wireless Personal Communications Journal.

The research data and material which was used is described in this article.

I used the python coding to perform the data security.

References

1. Aniruddha Bhattacharjya, X., Zhong, J., & Wang (2018). 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, 10*(1), 63–79.
2. Mauro Conti, A., Dehghantanha, K., Franke, S., & Watson (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.
3. Mahmoud Ammar, G. 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.
4. Arbia Riahisfar, E., Natalizio, Y., Challa, Z., & Chtourou (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks, 4*, 118–137.
5. Khan, M. A., & Salah, K. (2018). IoT security: Review, block chain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.
6. Kewei Sha, WeiWei, T. AndrewYang, Wang, Z. Shi, W., “On Security Challenges and open issues in Internet of Things,” Future Generation Computer Systems, 83, 326–337, 2018.
7. *Fadele Ayotunde Alaba*, Hashem, I. A. T. “Internet of Things security: A Survey,” Journal of Network and Computer Applications, *vol.* 88, *pp.* 10–28, 2017.
8. Aafaf Ouaddah, HajarMousannif, Elkalama, AnasAbou, & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks, 112*, 237–262.
9. Hamed Hellaoui, M., Koudil, A., Bouabdallah, “Energy-Efficient mechanisms in Security of the Internet of things: A Survey” Computer Networks, vol. 127, 173–189, 2017.
10. Sandeep, K., & Sood (2016). Advanced dynamic Identity-based Authentication Protocol using Smart Card. *International Journal of Information and Computer Security, 8*(1), 11–33.

11. Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of Security and Privacy-preserving solutions in the Internet of Things. *Computer Networks, 102*, 83–95.
12. Kumar, R., & Mahajan, G. (2015). A novel framework for secure file transmission using modified AES and MD5 algorithms. *International Journal of Information and Computer Security, 7*(2), 91–112.
13. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communication Surveys and Tutorials, 17*(3), 1294–1312.
14. Wei Jiang, Y., Ma, N. S., & Zhong, Z. (2015). Dynamic Security management for real-time embedded applications in Industrial Networks. *Computers and Electrical Engineering, 41*, 86–101.
15. Prakash Kuppuswamy, Saeed, Q. Y., & Al-Khalidi (2014). Hybrid Encryption/Decryption technique using new Public Key and Symmetric Key algorithm. *International Journal of Information and Computer Security, 6*(4), 372–382.
16. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of Security and Privacy in distributed Internet of Things. *Computer Networks, 57*, 226–2279.
17. Hai Lin, YunsiFei, X., Guan, Z. J., & Shi (2010). 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, 18*, 1519–1532.
18. Austin Rogers, A., Milenkovic, “Security extensions for integrity and confidentiality in Embedded processors”, Microprocessors and Microsystems, Elsevier, vol. 33, pp. 398–414, 2009.

Figures

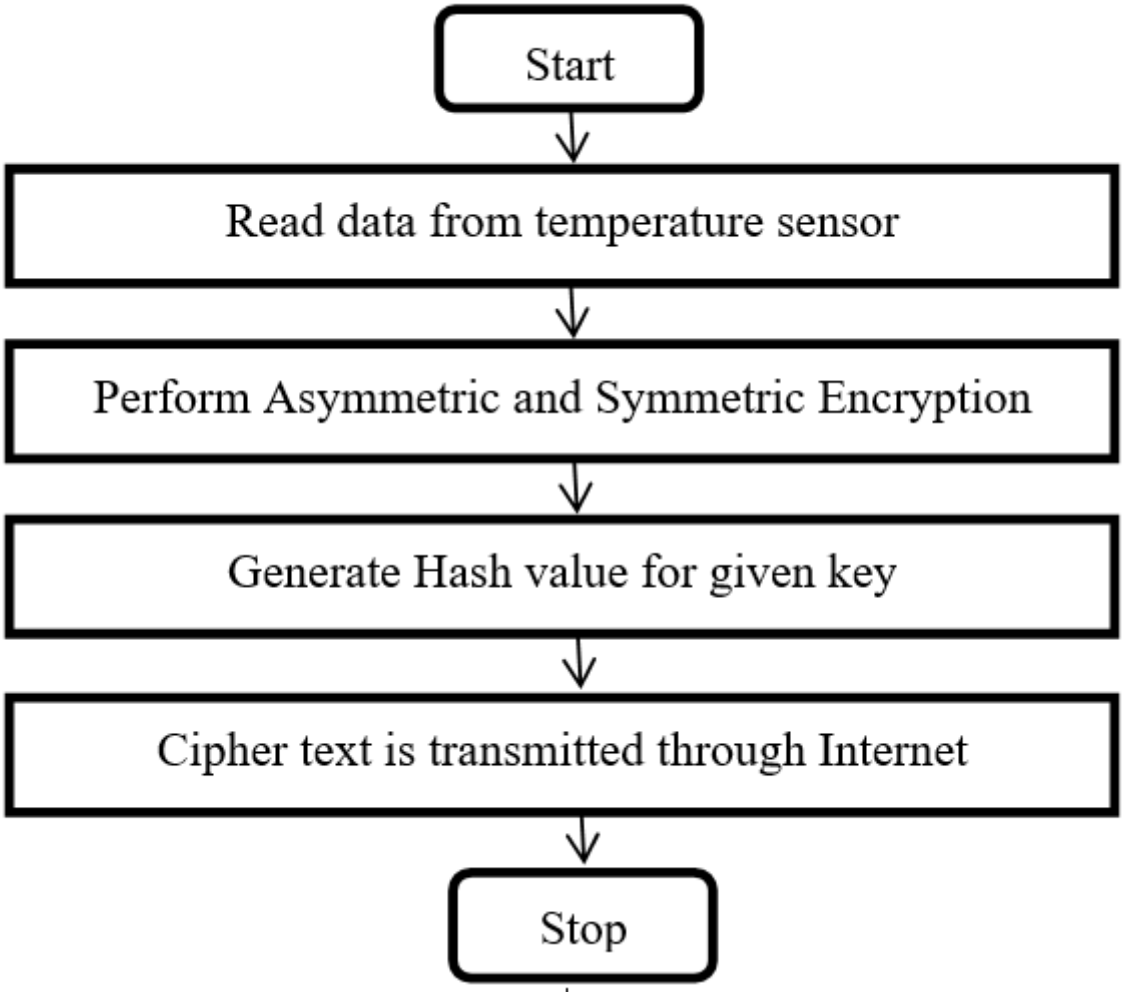

Figure 1

Flowchart for proposed Hybrid Encryption algorithm

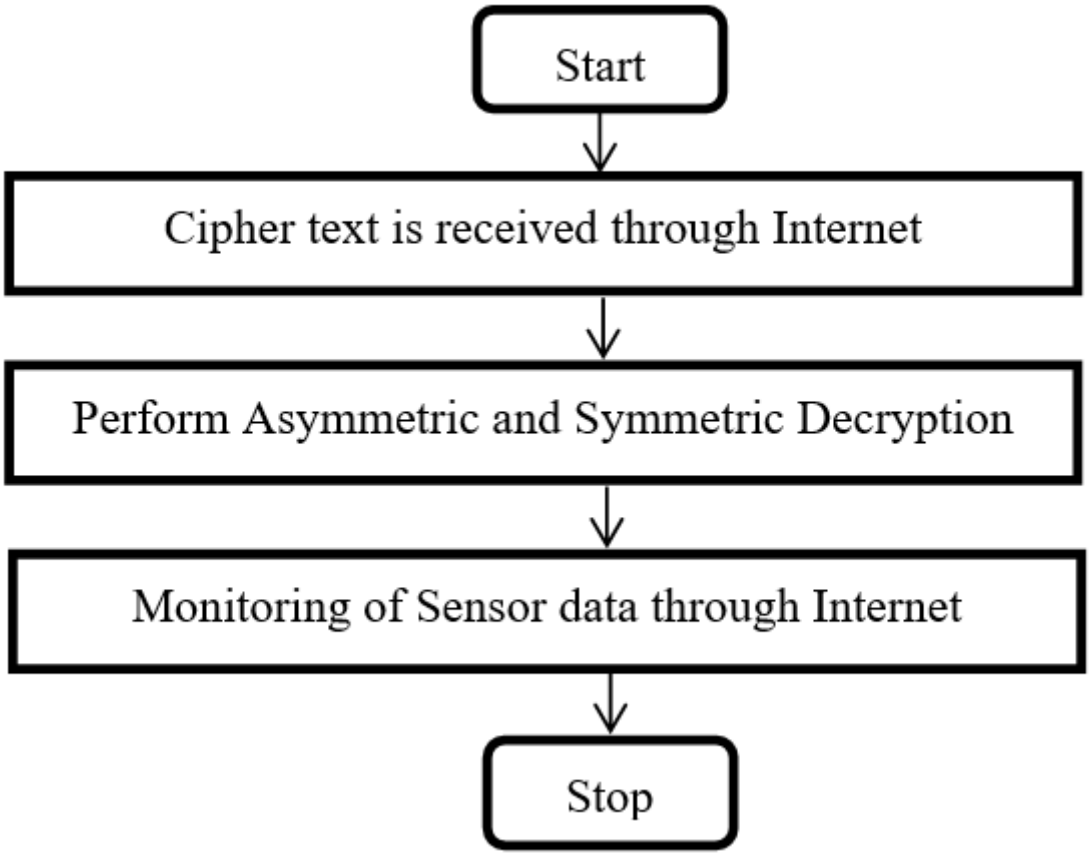

Figure 2

Flowchart for proposed Hybrid Decryption algorithm

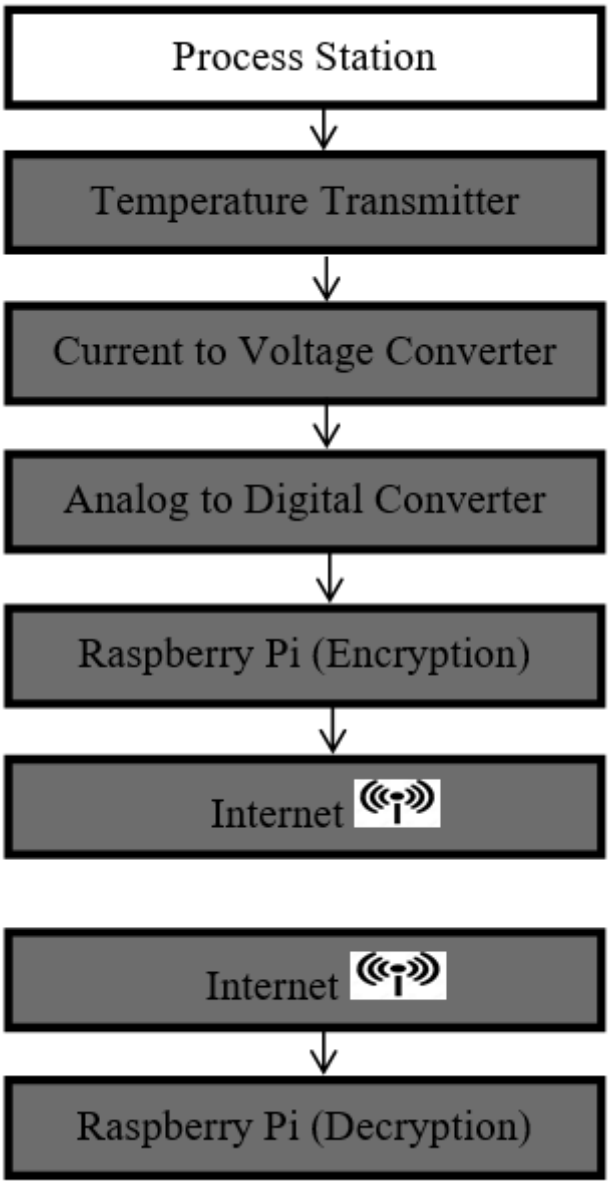

Figure 3

Flow diagram of Encryption and Decryption of Process Data with Embedded System through Internet

Figure 4

Experimental setup of Embedded based Wireless Secured Transmission of Process data

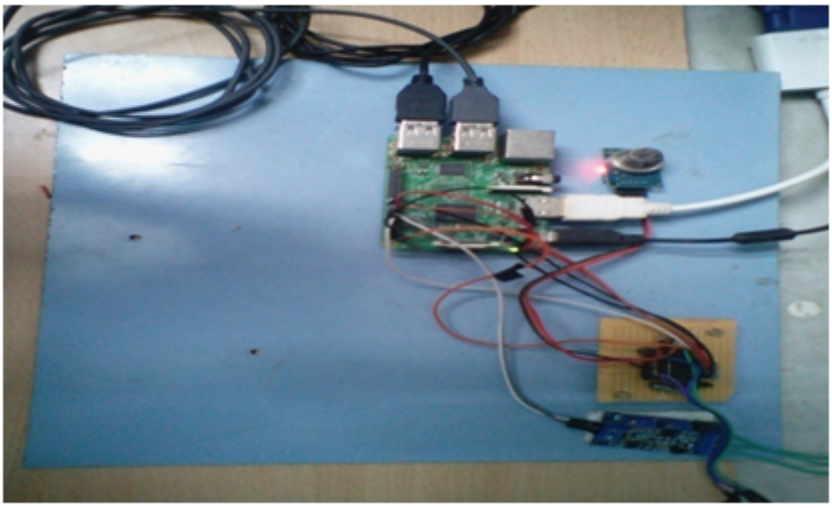

Figure 5

Transmitter section of Embedded based Wireless monitoring of Process data

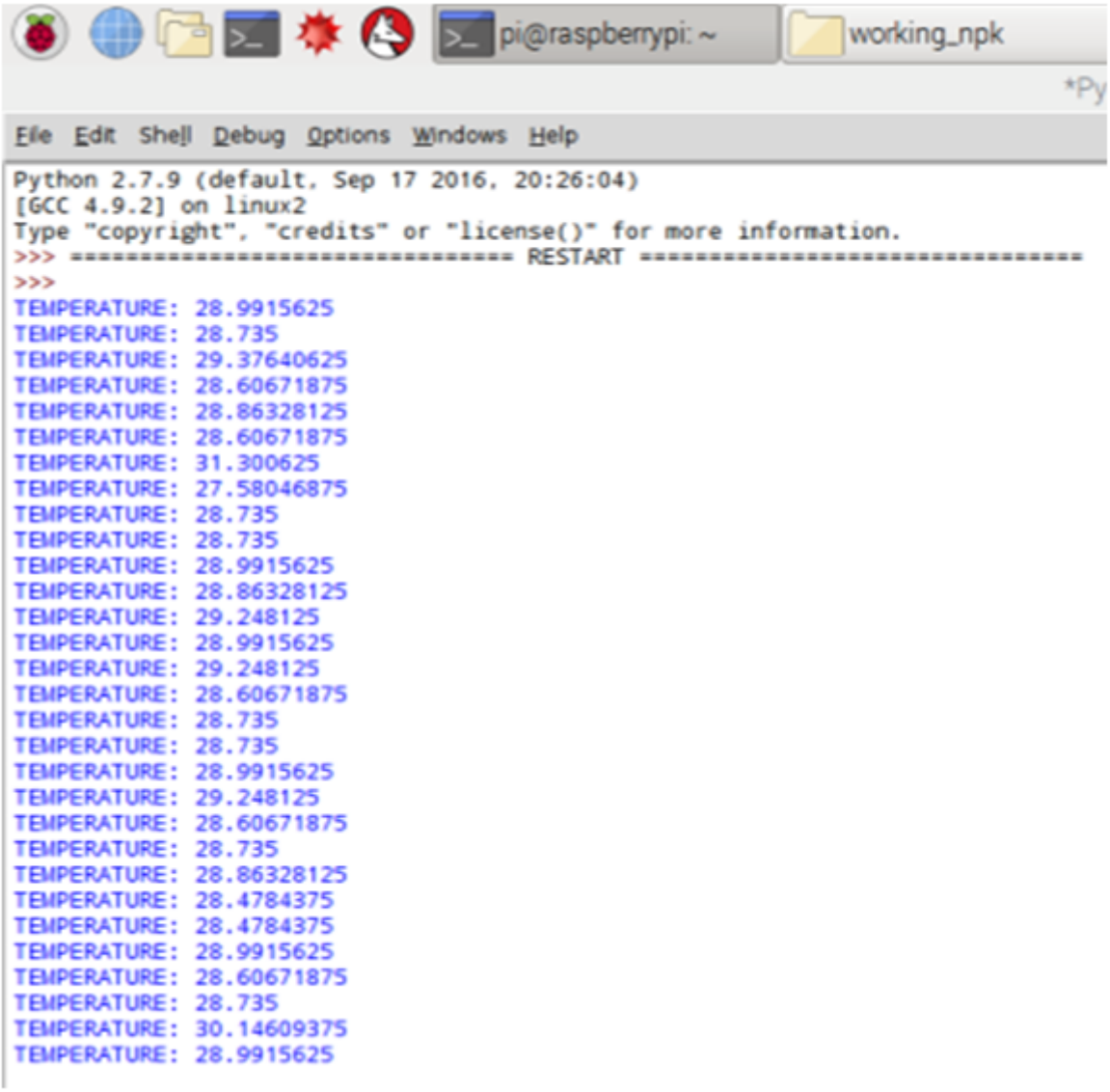

Figure 6

Monitoring of temperature process data using Embedded System

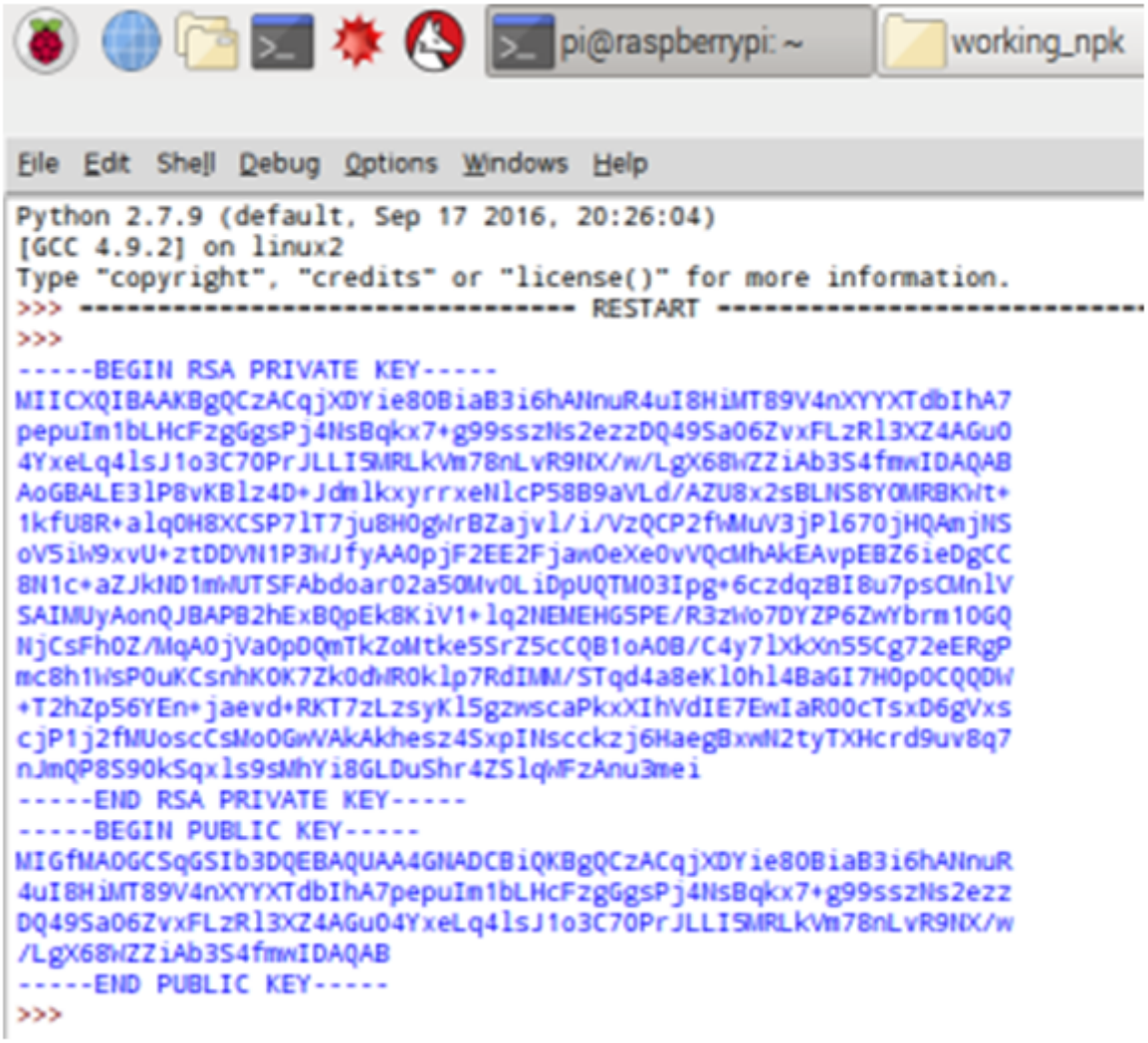

Figure 7

Generation of Private key and Public key

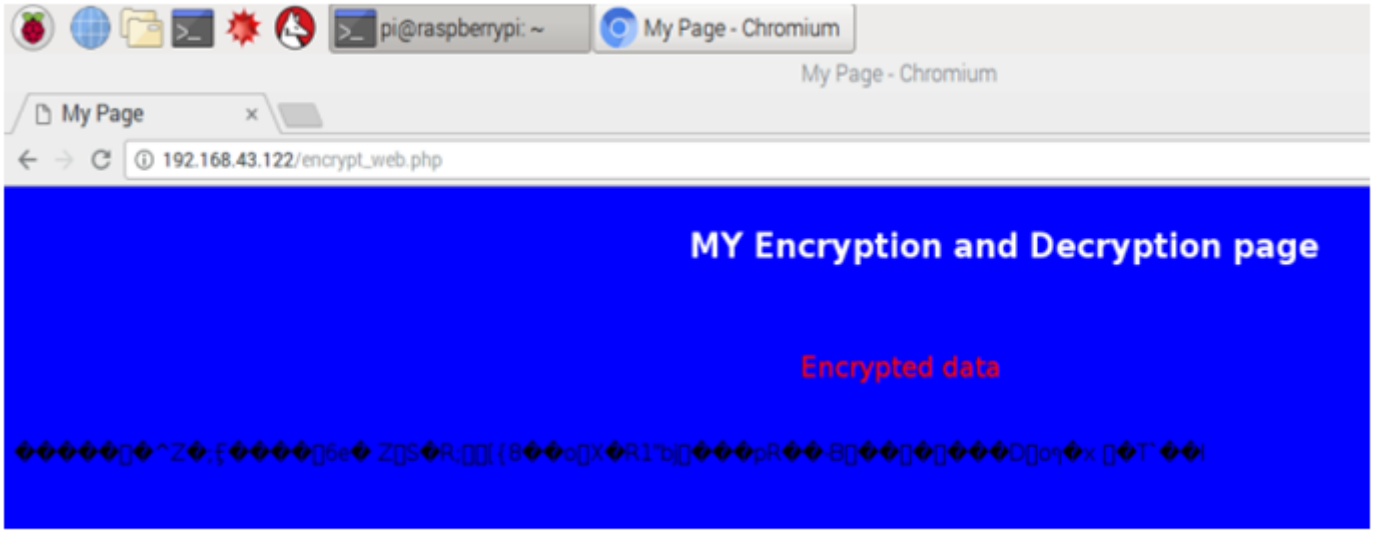

Figure 8

Temperature process data in Encrypted form monitored through Internet

Figure 9

Receiver section of Embedded based Wireless monitoring of Process data

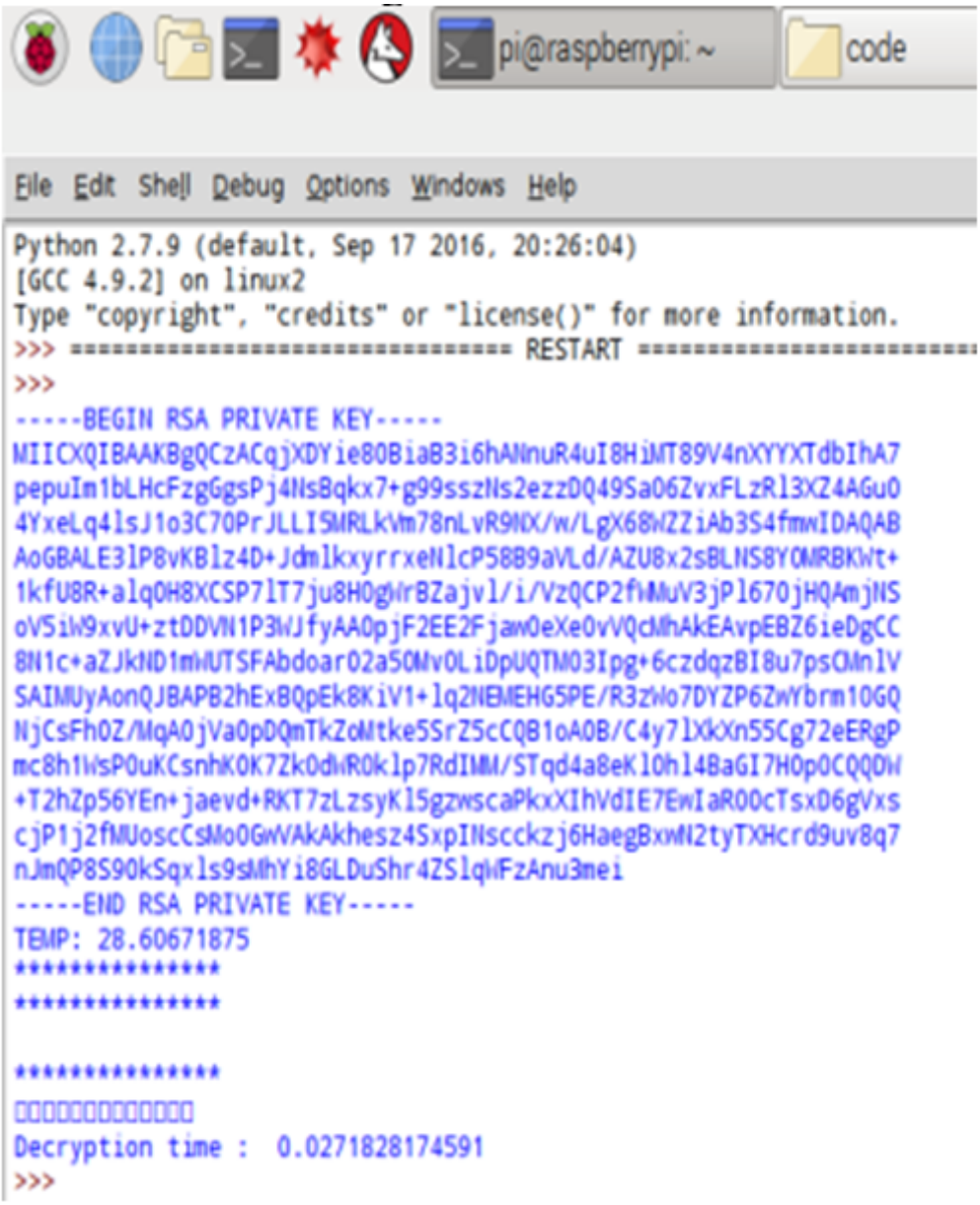

Figure 10

Receiver section of monitoring of Temperature Process Data in Original form

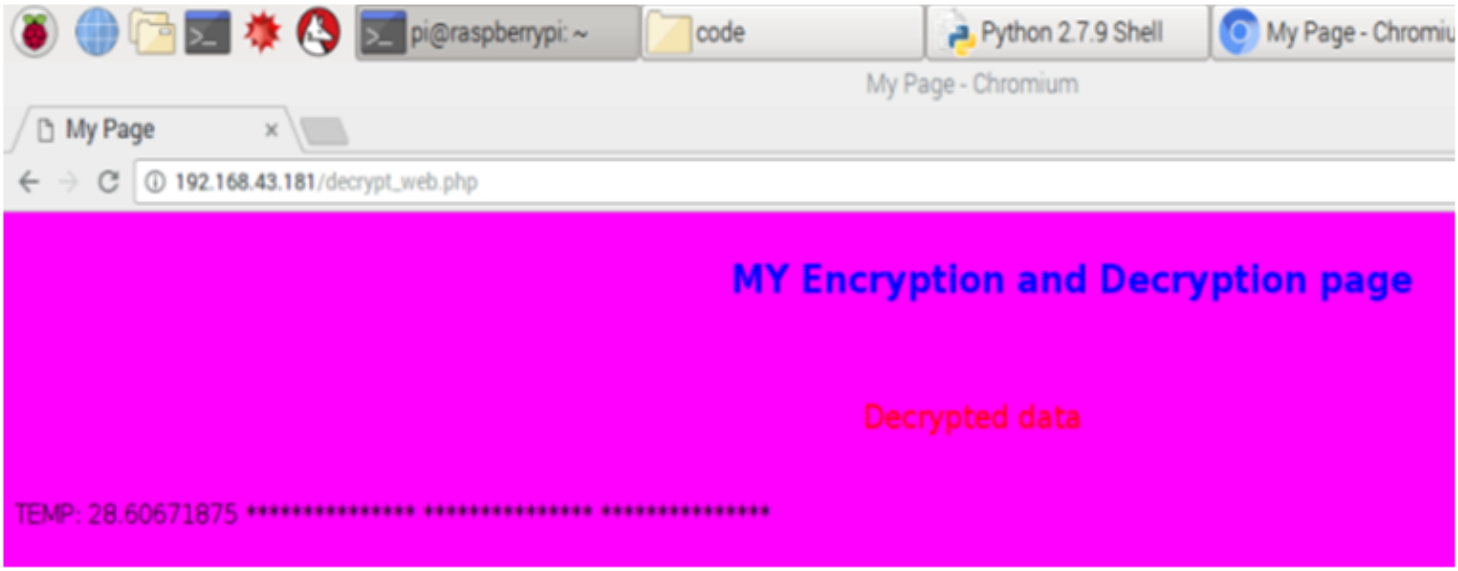

Figure 11

Temperature process data monitored through Internet at the receiver