Available online at http://scik.org

J. Math. Comput. Sci. 10 (2020), No. 6, 2208-2232

https://doi.org/10.28919/jmcs/4825

ISSN: 1927-5307

INTERNET OF THINGS BASED HYBRID CRYPTOGRAPHY FOR PROCESS DATA SECURITY

J.S. PRASATH[1,*], U. RAMACHANDRAIAH[2], S. PRABHURAJ[3], G. MUTHUKUMARAN[2]

[1]Department of EIE, KCG College of Technology, Anna University, Chennai 600097, India

[2]Centre for Sensors and Process Control, Hindustan Institute of Technology and Science, Chennai 603103, India

[3]Department of EEE, KCG College of Technology, Anna University, Chennai 600097, India

Abstract. This manuscript addresses security issues, security mechanisms of Internet of Things (IoT) and implementation of hybrid cryptography for preserving the process information against unauthorized access and modification. Modern industrial devices use smart sensors, intelligent controllers, smart transmitters and wireless networks for process monitoring and control applications. The industrial networks are integrated with the information technology (IT) networks, which allow the process monitoring through the internet. Various software algorithms are available for data security, but hackers break the security and corrupt the industrial data. The corrupted data alter the industrial process activity. It is essential to have security algorithms with hardware to protect the data. In this proposed work, a novel hybrid secured wireless algorithm is developed and implemented in real-time using an embedded system. This proposed security algorithm uses 128-bit encryption and decryption as well as hash value generation along with an embedded system, which becomes transceiver for the industrial wireless network. This proposed security algorithm enables alerts and assures the security for monitoring of industrial

*Corresponding author

E-mail address: jsprasath@gmail.com

Received July 3, 2020

processes through the internet.

Keywords: encryption; decryption; embedded system; hybrid cryptography; industrial IoT.

2010 AMS Subject Classification: 68P25.

1. INTRODUCTION

IoT is a growing technology with large number of objects which has ability to communicate information without manual operation. The control action has to be taken based on the sensor data and the command given to implement the decisions. The IoT are widely used in various applications include home automation, medical field, industrial plants, fitness equipment, smart cities etc. The security concern needs to be addressed for constrained and various network environment. The design objectives, challenges and solutions for industrial Wireless Sensor Networks (WSN) are presented [4]. The existing standards and industrial protocols are reviewed. The challenges in WSN limit the performance in industrial environments.

The IIoT has the potential for substantial improvements in manufacturing productivity. IIoT provides improvement in efficiency of operation through predictive maintenance and remote management. The various energy efficient mechanisms are addressed [3] in IoT security services. The energy saving mechanisms is applied to the deployment environment and the target protocol. The energy efficiency can be achieved by incorporating low energy security protocols. IIoT performs machine-to-machine communication and it ensures manufacturing of quality products. The major challenges in IIoT are security, adaptability, scalability, maintenance and flexibility.

The security issues in IoT systems and simulation technologies are used for risk assessment of cyber security. The cyber security involving IoT settings are addressed [6]. The case study is done for smart home security which is evaluated by Small World platform. The security loop holes are identified which are due to the malware ability to access the home LAN. The attackers can disturb the network by monitoring or altering the information of the process by intrusion. A new hardware device is proposed [5] that can detect Denial of Service (DoS) attack by only observing electrical signals in the circuit. The security of the IoT device is focused which is used

in endpoints of industrial control system. Due to the limitations in capacity and performance of IoT devices, implementation of security measures at the endpoint becomes complex by adding new software.

The intrusion detection system (IDS) can be utilized to monitor the malicious traffic in certain node and network to protect information systems. The trends, issues and future research of IDS for IoT are addressed [7]. The focus on research towards IoT is to investigate various detection methods and placement strategy, to enhance the attack detection range, to address more IoT technologies, to increase strategies for validation and alert traffic and security management need to be improved.

This paper is framed as:

Section 2 presents preliminaries which include architecture, security issues, security mechanisms, security requirements, key management and security challenges of IoT. Section 3 deals with the proposed hybrid cryptography algorithm. Section 4 contains the hardware implementation of proposed hybrid cryptography algorithm. Section 5 gives the results and discussion of hardware implementation of hybrid cryptography algorithm. Conclusions are given in Section 7.

2. PRELIMINARIES

This section includes the architecture, security issues, security mechanisms, security requirements, key management and security challenges of IoT.

IoT Architecture 2.1. The architecture of IoT includes three layers, which are Perception layer, Network layer and Application layer. The perception layer is used to get the plant information through the sensors. The network layer is authoritative for routing and transmits process data to other devices. The application layer is used to analyze the information received and takes the control decisions. IoT provides connectivity among variety of computing systems, sensor nodes, mobile devices, control systems and cloud computers. The equipment connected to IoT is enabled to sense and control the process parameters remotely across wireless networks. IoT devices have the capability to self-configure and allow a huge number of equipment to serve

jointly to perform specific functions. The current IIoT devices are combined into the IT network, which enables data exchange and communication between devices and systems.

Security Issues in IoT 2.2. The physical devices are connected in an IoT network which includes embedded processors and sensors to monitor the internal and external status of the environment. The target attacks are increased against industrial control systems. The unidirectional security gateway system is proposed [13] to guarantee the security and reliability of transmitted message. The security issues need to be addressed in order to protect the sensitive plant information from unauthorized access. The security requirement of perception layer is to ensure security of physical sensing devices and secure information retrieval. The security issues in perception layer include capturing of gateway node, capturing of physical nodes, unfair attacks, congestion attack, and forward attack. The security issues in network layer include confidentiality, eavesdropping of information, Denial of Service (DoS) attacks, integrity, man-in-the-middle attack etc. The security issues in application layer include unauthorized access of data and destroying the network by the attackers.

Security Mechanisms in IoT 2.3. The security mechanisms are considered depending upon the type of work performed by the IoT. The communication security in IoT can be achieved by incorporating lightweight security protocols for constrained environments. The lightweight devices are relatively small and the secure memory is often implemented in a smartcard. It combines the functionalities of both broadcast encryption and attribute-based encryption. A location privacy protection method is proposed [1] that satisfies differential privacy constraint to protect location data privacy and maximizes the utility of data and algorithm in Industrial IoT. It achieves significant improvements in terms of security, privacy, and applicability. The effective cryptographic algorithm is required to increase the level of data security. The challenging task is the protection of information from unauthorized access and security of communication channels. A new public key encryption scheme is proposed [11] which Cramer–Shoup encryption scheme with shorter cipher texts. The security is based on plain decisional Diffie–Hellman (DDH) assumption. It reduces the overall computational complexity and it obtains the Password-based

Authenticated Key Exchange (PAKE) schemes. It is essential to propose strong security algorithm and key management mechanisms. The various security threats and vulnerabilities of IoTare addressed [8]. The universal IoT security architecture can be implemented to ensure security in IoT applications. The analysis made for the security mechanisms of IoT which includes services and attacks.

The cryptography is used for transforming the information from the IoT into an unreadable format in order to protect the process data from unauthorized access. The energy efficient security architecture is proposed for wireless based industrial automation systems [16]. The packet protection based on encryption consumes energy in the case of battery powered devices. The development of lightweight security algorithm keeps the computational complexity at moderate level in IoT environment. The architecture level attacks include physical, software, side channel, logical, timing and power analysis. A self-organizing approach is proposed which detects the abnormal behavior of program [17]. The algorithm is developed for detecting the program behavior and it enhances the security of embedded systems. The system of attack may also vary for users, content providers and manufacturers. Software attacks use communication channels to exploit weaknesses in the embedded architecture. The malicious code can be introduced remotely through the network in the code injection attacks. A cost effective method is proposed for protecting embedded software against passive side channel attacks [19]. The protocols are vulnerable to software attacks and could result in a malevolent behavior such as unknown destination, packet replay or deadlock. The buffer overflow attack becomes dangerous to application-specific embedded systems.

Security Requirements in IoT 2.4. The IIoT introduces different architectures for operational technology which includes manufacturing, transportation, healthcare, energy production, and distribution. The attacks on IoT include hardware, software, and networks. The operational assets should be protected against cyber-attacks by incorporating security directly into the endpoint devices. Software attacks include accessing cryptographic keys, stored data, and system software. The current risk assessment approaches are ineffective for highly dynamic systems.

Confidentiality 2.4.1. The process information must be secured during transmission over wireless networks. Attackers can easily capture the information which is transmitted through the internet. The stored data inside the IoT device should be protected from the unauthorized access. The key size, security level, power consumption and the time required for execution of cryptographic algorithm is to be considered while used for secure process monitoring applications.

Integrity 2.4.2. The integrity ensures that the sensor data has not been modified or dropped during transmission over wireless networks. It is essential to secure the plant information and to safe the process equipment from the attackers. The hash algorithm can be used to ensure the data integrity. The lightweight hash function is proposed [12] which reduce complication in terms of hardware implementation and standard security can be achieved. The lightweight hash function is essential for constrained devices include wireless sensors and embedded systems.

Availability 2.4.3. It is essential to consider the availability of IoT data, web and mobile applications, as well as physical things to the authorized users. The firewall security is required to countermeasures the attacks on the Denial of Service (DoS), which can deny the data availability to the end-user. The impact of availability leads to damage of process devices, loss of revenue and even loss of life.

Authentication 2.4.4. The process information transmitted through the internet should be authenticated. The process data should be monitored and controlled only by the authorized users. The users need to enter a password for accessing the websites and the browsers authenticate the websites through the Secure Socket Layer (SSL) protocol in the internet. The IoT authentication is based on machine-to-machine without any human intervention.

Authorization 2.4.5. It is the mechanism of verifying that the access rights for user to access the sensitive process information. The devices connected to the IoT must only be reprogrammed by the authorized users. The various access control solutions in IoT are highlighted [10]. The commonly used internet protocols cannot suit for constrained environments. The effective access control system should satisfy the security properties such as confidentiality, integrity and

availability. Authorization involves defining of security policy, modeling of access control and enforcing the access control protocols.

Key Management System 2.5. The key management is an important mechanism which protects the process data from the attackers. It is the process of managing the process information throughout the transmission from the sensor to the internet. The requirement of key management is to pre-distribute all the secret keys to the sensor nodes. A key management scheme is proposed that integrates the random seed distribution with transitory master key mechanisms [20]. The nodes are unable to establish new keys after the specific time period and it is suitable for static networks. The key size of any security algorithm is an important consideration in order to strengthen the security. The key management mechanisms used for protecting IoT data should be strong so as to ensure confidentiality and integrity. The security algorithm is proposed [18] which provide end to end privacy for sharing the data. The key size is increased to prevent the information from brute force attack. The constraints in the hybrid security algorithm are cost, power and performance.

Security Challenges in IoT 2.6. The security is an important concern in exchanging information between IoT devices. The major challenge in securing IoT is to identify theft, to secure the information, to authenticate the information and to secure the end devices. The challenges related to the need of energy efficiency, real-time performance, coexistence, interoperability, and security and privacy are addressed [2]. The various security algorithms may be adopted which is a challenge to privacy preserving. The symmetric algorithm is capable to provide a lightweight solution for IIoT devices. The information should be routed between nodes should not be accessed and modified by the attackers. The routing algorithms and protocols are necessary to ensure the secure transmission of messages. The protocols and mechanisms related to secure routing in IoT are analyzed [15]. The standard secure routing algorithm is essential for IoT devices. The IoT networks have the ability to self-organize and serve without manual operations. The features and challenges of the distributed approach of the IoT are analyzed [21]. The distributed approach increases the complexity of security mechanisms. The IoT uses wireless

communications which is vulnerable to number of attacks including Denial of Service (DoS), man-in-middle, eavesdropping, masquerading, and saturation. The table shows the security issues at each IoT layer. The major security issues in IIoT are physical devices attacks, eavesdropping of process information by the attackers, unauthorized monitoring of process data, makes denying of process information to authorized users.

The various existing protocols for ensuring security and protect communications in IoT are addressed [14]. The protocols currently used for IoT are IEEE 802.15.4 which is low-energy communications used at the physical layer and Medium Access Control (MAC) layer, 6LoWPAN adaptation layer which enables transmission of IPv6 packets over IEEE 802.15.4, IPv6 Network routing and Constrained Application Protocol (CoAP), which supports communications at the application layer.

TABLE I

SECURITY CONCERNS OF IOT LAYERS

S. No.	Layers	Security Issues
1.	Perception	Wireless Signal Potency, Attacks on Physical nodes and Dynamic IoT Topology
2.	Network	Traffic analysis, Eavesdropping, Passive monitoring, Variety of Network Components and Protocols
3.	Application	Privacy Protection, Authentication, Data Integrity, Information Availability

The gateway performs various critical functions which include protocol translation, data filtering, and processing, device connectivity, security etc. The network related challenges in IoT are scalability, bandwidth, security and privacy. The security issues for distributed industrial control systems are addressed [22].The various aspects to be considered such as security at the

architecture level, security at the terminal level, security at the transport level, security at the control level, privacy protection, managing the security and mechanisms for security evaluation in order to achieve higher security level in IoT systems. The number of security issues and privacy increases due to the wide usage of IoT in various environments.

3. Proposed Hybrid Cryptography Algorithm

This proposed security algorithm includes AES (Advanced Encryption Standard) 128-bit encryption which converts sensor data into cipher text. The encryption is performed at the transmitter node. The AES decryption is performed at the receiver node which converts encrypted data to original data in numerical form. The AES algorithm is chosen in this work because it achieves higher level of security.

AES Encryption 3.1. The 128-bit AES is used in this proposed work for input and output blocks. It is based on the state operation and it provides the intermediate value of AES encoding and decoding operation. The block and the key are represented as an array of columns. Each array contains 4 rows and each column represents 8-bits. The round function to be carried out during compilation is based on the length of the block and key.

The AES encryption process involves:

- AddRoundKey transformation
- The round function comprises of:
  - Bytes Substitution
  - Rows Shifting
  - Columns Mixing
  - AddRoundKey
- A final Round comprising:
  - Bytes Substitution
  - ShiftRows
  - AddRoundKey

Sub Bytes () 3.1.1. The S-Box is formed which contains 256 data where non-linear byte substitution is done for each byte of the state. The byte input is broken into two 4-bit halves to read this table.

TABLE II

SUBSTITUTION BOX

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Shift Rows () 3.1.2. The bytes in the last three rows of the state are shifted with different number of bytes. The 128-bit internal state of the cipher in each row is shifted. The first row should leave unshifted.

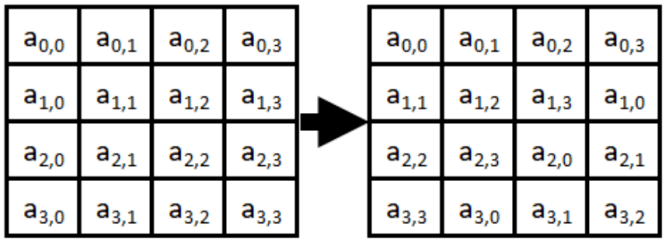

Fig. 1 Shift Rows

Mix Columns () 3.1.3. Each column in this transformation is treated as a four-term polynomial which works on state column by column.

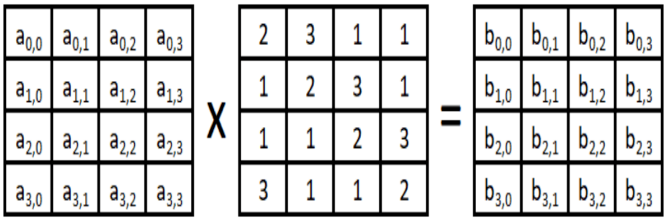

Fig. 2 Mix Columns

Add Round Key () 3.1.4. The Round Key is appended to the state in which the bitwise XOR operation is performed.

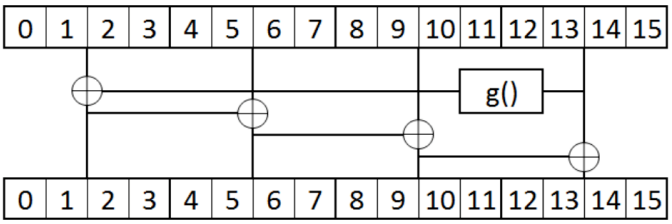

Fig. 3 Round Key Transformation

The 10 rounds are performed for 128-bit AES encryption. The ciphertext is obtained at the end of the 10^{th} round.

AES Decryption 3.2. Since the AES is a symmetric encryption standard, the decryption of data is performed by inverting all the encryption operations with the identical key with which it is encrypted. The key expansion of 128-bit block is performed and then the round key process is done. The inverse Add Round key is executed between cipher text and the modified key from the key expansion.

The AES decryption operation involves:

- Inverse Shift Rows
- Inverse Bytes Substitution
- Inverse Mix Columns
- Inverse Add Round Key

At the last iteration, except Inverse Mix Columns, Inverse Shift Rows, Inverse Sub Bytes and Inverse Add Round Key is performed to generate the original plain text.

Inverse Shift Rows 3.2.1. It performs the inverse of the Shift Rows transformation. The shifting process takes place in which the last three rows bytes of the state are shifted cyclically with different number of bytes.

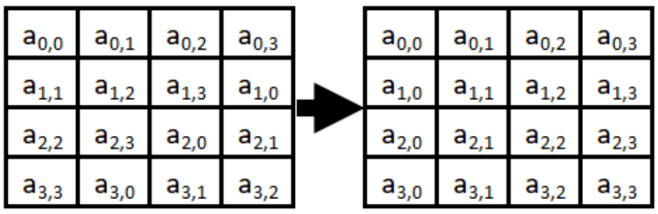

Fig. 4 Inverse ShiftRows

Inverse Sub Bytes 3.2.2. It performs inverse operation with the byte substitution. Each byte of the State is applied with the inverse S-Box.

TABLE III

INVERSE SUBSTITUTION BOX

	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f	
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
70	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Inverse Mix Columns 3.2.3. It performs inverse operation with the Mix Columns function. Each column is treated as a polynomial, which works on the State column-by-column.

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \times \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

Fig. 5 Inverse MixColumns

Inverse Add Round Key 3.2.4. The round key should be selected in the reverse order. It is own inverse function which performs XOR operation.

The advanced form of block cipher encryption is proposed, which is Cipher Block Chaining (CBC) mode that provides additional complexity to the encrypted data. The Plain text and the IV are used to produce the cipher text. The countermeasure technique is proposed which are based on fault space transformation to protect AES-128 bits against biased fault attacks [9]. The fault collision based attacks are prevented. The time and hardware redundant versions of AES (Advanced Encryption Standard) are performed for biased fault attacks. This proposed AES encryption is performed using CBC mode. Each block of plain text is XORed with the previous

cipher text block before being encrypted and then the result is encrypted with the key. The currently generated cipher text is decrypted and then adding the previous cipher text block to obtain the original plain text. The advantage of CBC mode is it generates different cipher text for identical input message by changing the initialization vector.

This proposed hybrid cryptography algorithm combines the asymmetric, symmetric and hash function cryptography which provides strong security during transmission of process information. The random private key is generated using RSA security algorithm where the key size is 2048-bits.

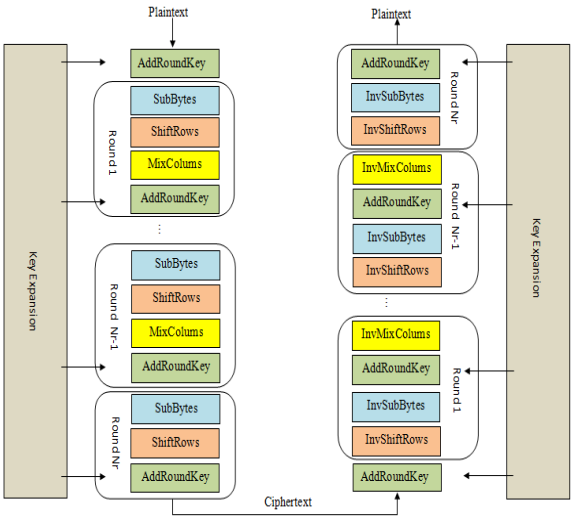

Fig. 6 AES Encryption and Decryption

The key and an initialization vector (IV) are required for symmetric algorithms. The advanced form of block cipher encryption is proposed which is Cipher Block Chaining (CBC) mode that provides additional complexity to the encrypted data. The cipher text of each encrypted block depends on the IV and the plaintext of all preceding blocks. The symmetric cipher is generated by using Advanced Encryption Standard (AES) encryption which is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). The CBC mode is incorporated with the AES encryption.

Fig. 7 shows the AES encryption using CBC mode. Each block of plain text is XORed with the previous cipher text block before being encrypted and then the result is encrypted with the key. The currently generated cipher text is decrypted and then adding the previous cipher text

block to obtain the original plain text. The advantage of CBC mode is it generates different cipher text for identical input message by changing the initialization vector.

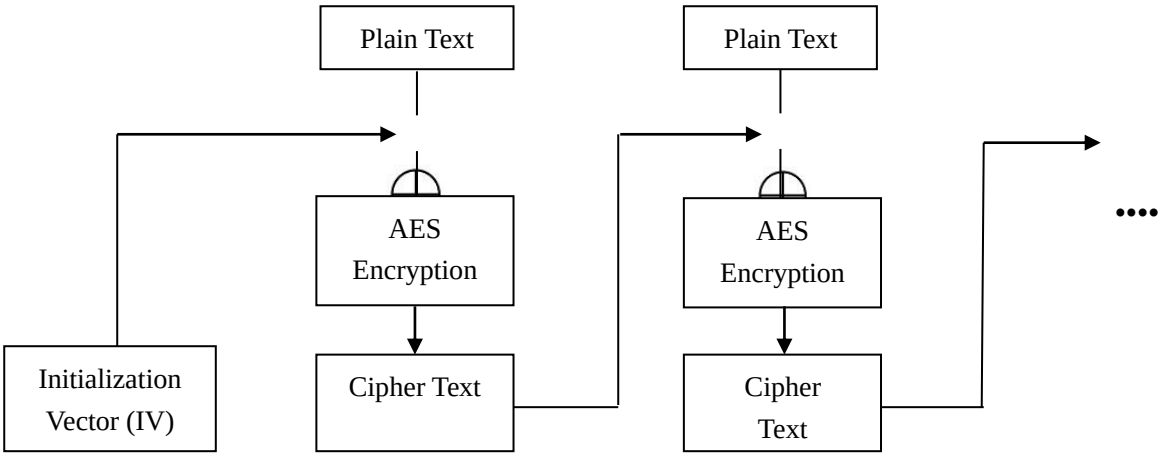

Fig. 7 AES Encryption with Cipher Block Chaining (CBC) mode

This proposed hybrid cryptography algorithm generates a random key from the RSA algorithm, initialization vector and plain text. This random key is applied as an input to the AES encryption to generate cipher text. The AES encryption is performed for ten rounds and the encrypted data is taken at the end of the tenth round. This encrypted data is given as input to the AES decryption. The random key generated from the RSA algorithm is secured by converting it into a hash value by using hash function cryptography. This generation of hash value ensures data integrity.

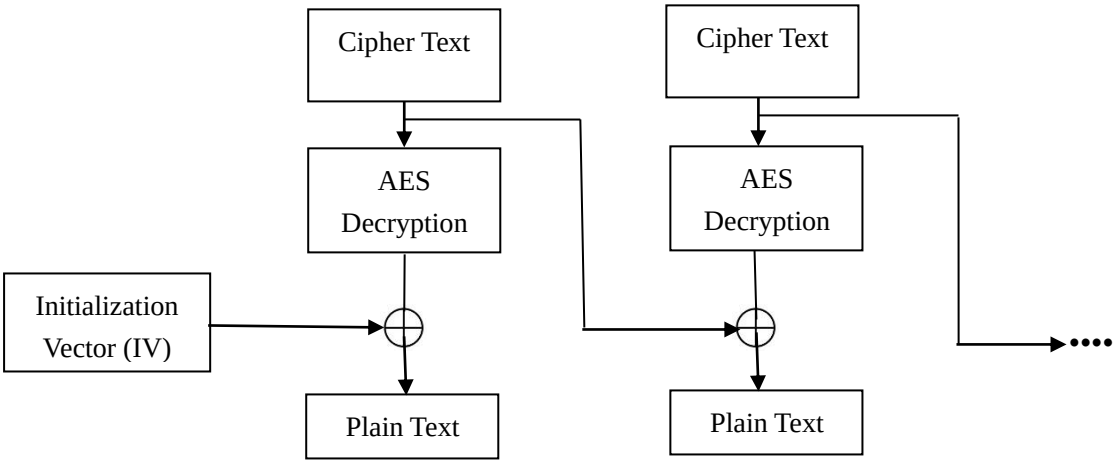

Fig. 8 AES Decryption with CBC mode

Fig. 8 shows the AES decryption using CBC mode. In the decryption side, the hash value is converted back to a random key which is applied to the AES decryption. The encrypted data is given as input to the decryption algorithm. Each block of cipher text is decrypted by using AES decryption and then performs XOR operation with the previous cipher text to generate the plain text. The AES decryption is performed for ten rounds and the original plain text is obtained at the end of the tenth round.

The hybrid cryptography is proposed [Jigar Chauhan et al., 2013] which is a combination of DES and AES algorithms. The plain text of 256-bits is given as input to DES and the encrypted text of 384-bits is produced as output. The AES algorithm takes 384-bits as input and produces the encrypted text of 704 bits. The time taken to perform this data encryption is very high. The symmetric encryption is performed to obtain the cipher text for the sensor data. The message digest (MD5) algorithm is used to generate hash value for a given key. It takes the input data of any size and produces the output in fixed length digest value. It performs processing of input data in 512-bit blocks, divided into 16 words composed of 32- bits each. The MD5 produces the output of 128-bit message digest value.

Message Digest (MD5) Algorithm 3.3. MD5 is a hash function that ensures the message has been unaltered during transmission. The input message is first split into blocks of 512-bits each. At the end of the block, 64-bits are inserted. The additional bits are padded at the end of the last block is less than 512-bits.

Flowchart 3.4. The flowchart for the proposed encryption algorithm is shown in fig. 9. The temperature and gas sensor data is taken as input. The key is essential to encrypt the process data. The symmetric encryption is performed for the given input process data and the cipher text is generated. The MD5 hash algorithm is proposed which generates hash value for a given key. When the input plant data changes, the hash value also gives different values. The hash algorithm ensures data integrity during transmission of process information over internet. The cipher text can be monitored through the web page by providing the required IP (Internet Protocol) address.

The flowchart for the proposed hybrid decryption algorithm is shown in fig. 10. The cipher text is obtained by entering the IP address at the receiver. The symmetric decryption is performed for the received cipher text to obtain the sensor value in plain data.

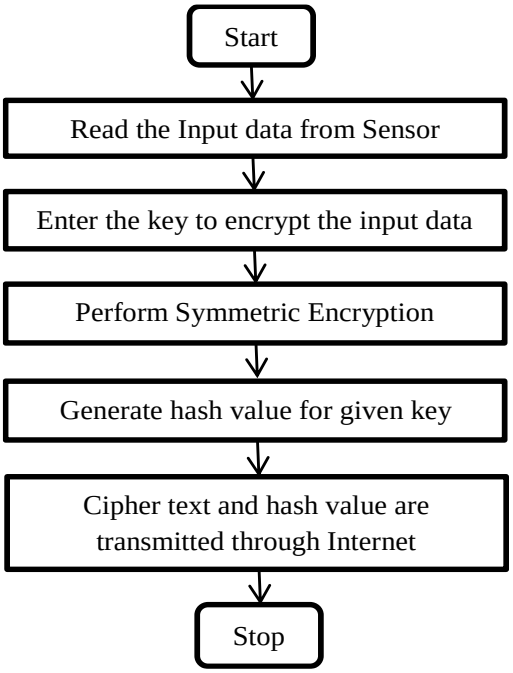

Fig. 9 Flowchart of Proposed Hybrid Encryption algorithm

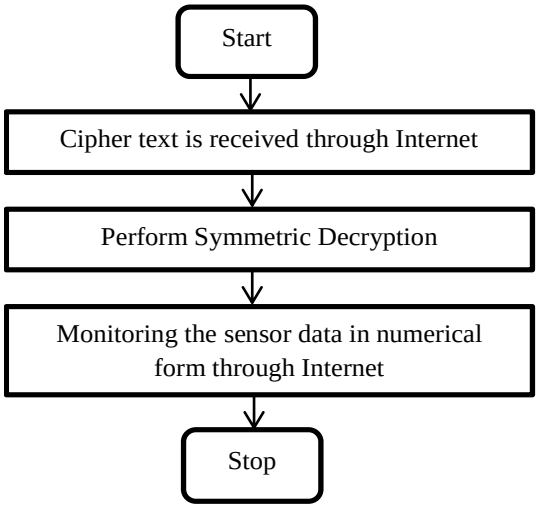

Fig. 10 Flowchart of Proposed Hybrid Decryption algorithm

4. HARDWARE IMPLEMENTATION OF PROPOSED SECURITY ALGORITHM

This proposed hybrid security algorithm is implemented in embedded hardware with process parameters transmitted over wireless medium. The process data can be monitored through the internet both at the transmitter and the receiver.

Fig. 11 shows the block diagram of secure monitoring of process data using embedded systems with IoT. The transceiver node is a raspberry pi in which the encryption and decryption algorithm is written using python code.

The transceiver node converts the temperature and gas process data in numerical form to unreadable format which is cipher text. It also converts the cipher text into plain data. The encrypted data is transmitted through Wi-Fi to the receiver node.The IP address is essential to monitor the sensor data in both transmitter and receiver side through the internet.

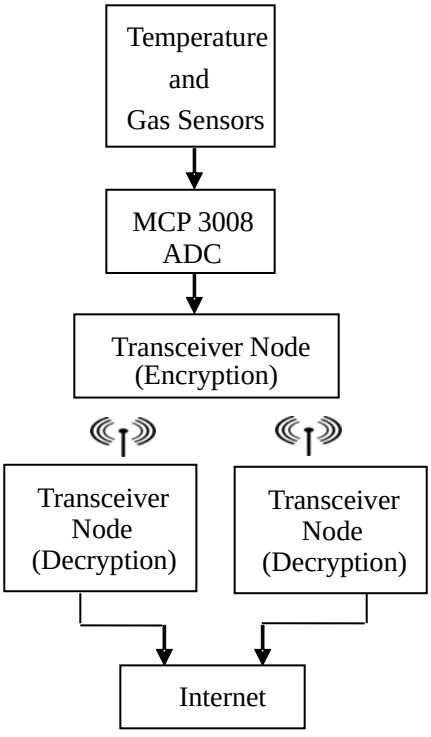

Fig. 11 Block Diagram of secure monitoring of process data using Embedded System through IoT

This proposed work is used for secure transmission and reception of process data using three nodes. Fig. 12 shows the transceiver node1 which performs encryption in order to protect the process information from the unauthorized access. The MQ2 gas sensor is used in this work which detects the presence of flammable gases such as methane, propane, butane, alcohol, hydrogen and liquefied petroleum gas. The MQ2 sensor has four pins which are analog pins, digital pins, power supply, and ground. The LM35 temperature sensor is used in this work to sense the ambient temperature.

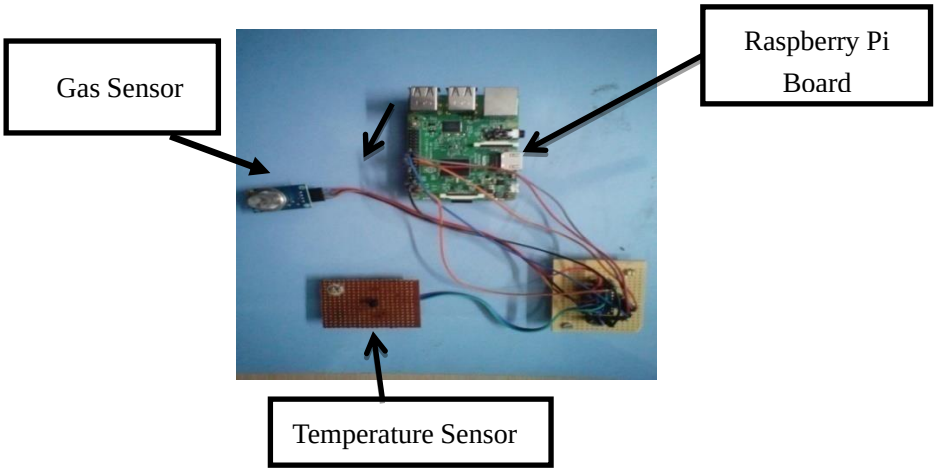

Fig. 12 Transceiver Node1 for Secure transmission of Process data

The transceiver node1 reads the gas sensor data. The encryption algorithm is written using Python language in order to generate the cipher text.

Fig. 13 shows the transceiver node2 used at the receiver for secure monitoring of gas sensor data. It receives the encrypted data through Wi-Fi and performs decryption to obtain the sensor data in numerical form. The decryption algorithm is written in Python which converts cipher text into plain text. The IP address is essential to monitor the sensor data through the internet.

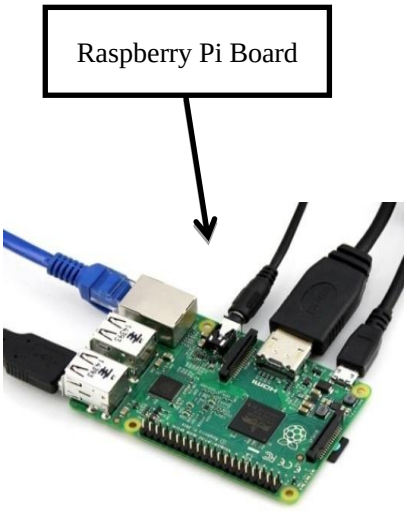

Fig. 13 Transceiver Node2 for secure monitoring of Process data

Fig. 14 shows the transceiver node3 used at the receiver to enable secure monitoring of process data through internet in remote areas. This proposed hybrid security algorithm strengthens the sensitive process information during transmission across the wireless networks.

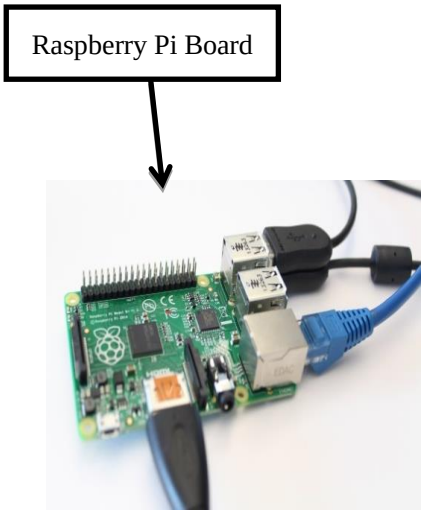

Fig. 14 Transceiver Node3 for Secure monitoring of Process data

5. Results and Discussion

The AES 128-bit algorithm is proposed which is described below.

Plain Text (128-bits) in Hex value

64 77 4F 60 8F 6D 75 40 8E 39 2E 85 90 44 47 5E

AES Algorithm – First Roundkey

Key (128-bits) in Hex value

84 28 71 24 93 70 3D 49 80 6B 35 2E 97 50 36 95

Byte Substitution (S-Box): (37, 7A, 4D, 55)

First Roundkey

B2 72 EC F6 94 17 41 83 B7 79 E6 5B D4 89 6C 7B

Substitution Bytes

The current State Matrix is

$$\begin{pmatrix} 00\ 3C\ 6E\ 47 \\ 1F\ 4E\ 22\ 74 \\ 0E\ 08\ 1B\ 31 \\ 54\ 59\ 0B\ 1A \end{pmatrix}$$

The each byte of current state matrix is substituted by corresponding entry in AES Substitution Box.

This leads to new State Matrix

$$\begin{pmatrix} 63\ EB\ 9F\ A0 \\ C0\ 2F\ 93\ 92 \\ AB\ 30\ AF\ C7 \\ 20\ CB\ 2B\ A2 \end{pmatrix}$$

Shift Row

The last three rows are shifted in the state matrix and the first row is not shifted.

The new State Matrix is

$$\begin{pmatrix} 63\ EB\ 9F\ A0 \\ 2F\ 93\ 92\ C0 \\ AF\ C7\ AB\ 30 \\ A2\ 20\ CB\ 2B \end{pmatrix}$$

Mix Columns

The fixed matrix is multiplied against current State Matrix.

$$\begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} X \begin{pmatrix} 63\ EB\ 9F\ A0 \\ 2F\ 93\ 92\ C0 \\ AF\ C7\ AB\ 30 \\ A2\ 20\ CB\ 2B \end{pmatrix} = \begin{pmatrix} BA\ 84\ E8\ 1B \\ 75\ A4\ 8D\ 40 \\ F4\ 8D\ 06\ 7D \\ 7A\ 32\ 0E\ 5D \end{pmatrix}$$

AddRoundkey

The Roundkey is added to the state in which the XOR operation is performed.

This yields new state matrix which is given below.

$$\begin{pmatrix} 6D\ B5\ 39\ 7A \\ C7\ 36\ 94\ D9 \\ 38\ EC\ 82\ F5 \\ 2B\ B7\ E5\ C8 \end{pmatrix}$$

The output of AES encryption after first Round is:

D8 87 C8 3B F5 B2 9C EA 39 A4 E7 5D 8D 79 2F FB

In this similar way, all the 10 rounds are performed with the above steps. At the end of the 10^{th} round, ciphertext is obtained.

The ciphertext at the end of the 10^{th} round for AES-128 bit is:

69 53 5A 8F C7 74 30 F370 2379 D3 5A 6B D47E

The MD5 hash algorithm is used in this work in order to ensure data integrity. MD5 is expressed as a 32 digit hexadecimal value. The length of the message before padding is appended as a 64-bit block.

The MD5 generates the hash value for a given input data.

Input Data (128-bits)

54 68 61 78 33 28 4D 83 60 6DB59E 5250 84 47

Hash value generated using MD5

b72966be9ef89d4cfa13f1aed3c38cca

This proposed hybrid cryptography algorithm is implemented in embedded system with data acquisition through internet. The python code is written which combines the AES and MD5 algorithms. The encrypted and decrypted data can be monitored through the internet.

Fig. 15 shows the gas sensor data in encrypted form monitored through internet at the transmitter. It is obtained by compiling the encryption algorithm written in python. The IP address is required to monitor the gas data in cipher text.

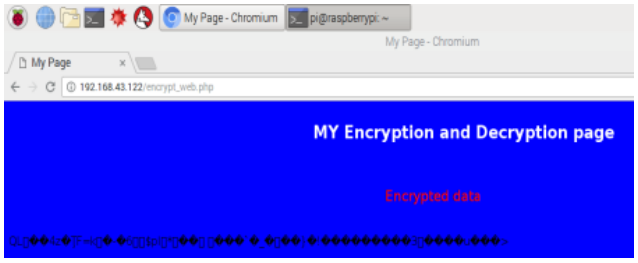

Fig. 15 Monitoring of encrypted data through Internet

Fig. 16 shows the gas sensor data in decrypted form monitored through the internet at the receiver. It is obtained by compiling the decryption algorithm written in python. The IP address is required to monitor the gas data in numerical form.

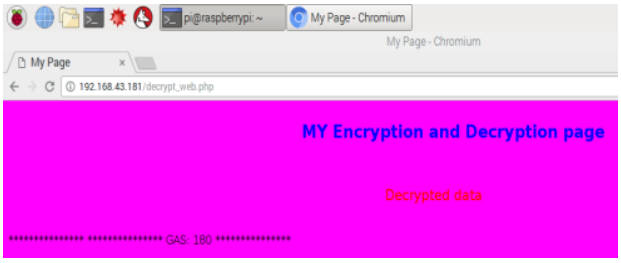

Fig. 16 Monitoring of decrypted data through Internet

The benefit of this proposed hybrid cryptography algorithm is that it generates different cipher text for the same messages by using different initialization vectors. The generation of random key size is larger that is., 256 bits and this key size can be expanded. In addition, this random key is secured by converting it into a hash value.

The benefit of this proposed work is it ensures secure transmission and monitoring of process data over wireless networks. It protects the process data and industrial devices from unauthorized access. The transceiver nodes can perform both encryption and decryption. It can be applicable for secure monitoring of any industrial process parameters through the internet.

6. CONCLUSION

This proposed hybrid cryptography algorithm combines the symmetric and hash algorithms that ensure confidentiality and integrity of process information during transmission over wireless medium. This proposed security algorithm is implemented in embedded system with process data transmitted over wireless networks. The symmetric block cipher is performed with CBC mode that provides additional complexity to the encrypted data. The hash algorithm provides authentication and to verify data integrity. It also provides privacy to industrial operators and engineers in monitoring the status of sensitive plant information. The encrypted and decrypted data can be monitored through the internet at the transmitter and receiver respectively. It allows secure monitoring of process data through the internet. This proposed work enables secure monitoring of harmful gases include liquefied petroleum gas, propane, methane, butane, alcohol and hydrogen present in the atmosphere. The incorporation of hybrid security algorithm ensures smooth functioning of plant operations and provides strong security as well as safety to the plant operators. It protects the highly expensive industrial devices from the attackers. The usage of embedded systems with wireless networks becomes cost effective. This proposedhybrid security algorithm provides authentic security for any industrial process to secure the sensitive plant information. It is essential to analyze the security attacks and to implement the security mechanisms associated with modern industrial automation systems.

CONFLICT OF INTERESTS

The authors declare that there is no conflict of interests.

REFERENCES

[1] Y. Chunyong, X. Jinwen, S. Ruxia, W. Jin, Location Privacy Protection based on Differential Privacy Strategy for Big Data in Industrial Internet of Things, IEEE Trans. Ind. Inform. 14 (2018), 3628-3636.

[2] S. Emiliano, S. Abusayeed, H. Song, J. Ulf, G. Mikael, Industrial Internet of Things: Challenges, Opportunities, and Directions, IEEE Trans. Ind. Inform. 14 (2018), 4724-4734.

[3] R. Jinnai, A. Inomata, I. Arai, K. Fujikawa, Proposal of hardware device model for IoT endpoint security and its implementation, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, Kona, HI, 2017: pp. 91–93.

[4] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, N.M. Khan, A Critical Analysis of Research Potential, Challenges, and Future Directives in Industrial Wireless Sensor Networks, IEEE Commun. Surv. Tutorials. 20 (2018), 39–95.

[5] H. Hellaoui, M. Koudil, A. Bouabdallah, Energy-efficient mechanisms in security of the internet of things: A survey, Computer Networks. 127 (2017), 173–189.

[6] F. Angelo, A. Luciano, P. Andrea, A. Piccolo, Using virtual environments for the assessment of Cyber Security issues in IoT scenarios, Simul. Model. Pract. Theory, 73 (2017), 43-54.

[7] B. Bruno, S. Rodrigo, K. Claudio, A. Sean Carlisto de, A Survey of Intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017), 25-37.

[8] A. Fadele, O. Mazliza, H. Ibrahim, A. Faiz, Internet of Things Security: A Survey, J. Netw. Comput. Appl. 88 (2017), 10-28.

[9] S. Patranabis, A. Chakraborty, D. Mukhopadhyay, P.P. Chakrabarti, Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-Like Block Ciphers, IEEE Trans. Inform. Forensic Secur. 12 (2017), 1092–1102.

[10] O. Aafaf, M. Hajar, E. Anas, O. Abdellah, Access control in the Internet of Things: Big challenges and New Opportunities, Computer Networks, 112 (2017), 237-262.

[11] M. Abdalla, F. Benhamouda, D. Pointcheval, Public-key encryption indistinguishable under plaintext-checkable attacks, IET Inform. Secur. 10 (2016), 288–303.

[12] M. Puliparambil, M. Sindhu, S. Chungath, S. Madathil, Hash-One: A Lightweight Cryptographic Hash function, IET Inform. Secur. 10 (2016), 225-231.

[13] Y. Heo, B. Kim, D. Kang, J. Na, A design of unidirectional security gateway for enforcement reliability and security of transmission data in industrial control systems, in: 2016 18th International Conference on Advanced Communication Technology (ICACT), IEEE, Pyeongchang Kwangwoon Do, South Korea, 2016: pp. 1–1.

[14] D. Aakash, P. Shanthi, Lightweight Security Algorithm for Wireless Node Connected with IoT, Indian J. Sci.

Technol. 9 (2016), 1-8.

[15] A. David, G. Jairo, K.R. Sayan, Secure routing for Internet of things: A Survey, J. Netw. Comput. Appl. 66 (2016), 198-213.

[16] R. Muradore, D. Quaglia, Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security, IEEE Trans. Ind. Inf. 11 (2015), 830–840.

[17] X. Zhai, K. Appiah, S. Ehsan, G. Howells, H. Hu, D. Gu, K.D. McDonald-Maier, A Method for Detecting Abnormal Program Behavior on Embedded Devices, IEEE Trans. Inform. Forensic Secur. 10 (2015) 1692–1704.

[18] J. Granjal, E. Monteiro, J. Sa Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, IEEE Commun. Surv. Tutorials. 17 (2015) 1294–1312.

[19] G. Agosta, A. Barenghi, G. Pelosi, M. Scandale, The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 34 (2015), 1320–1333.

[20] F. Gandino, B. Montrucchio, M. Rebaudengo, Key Management for Static Wireless Sensor Networks With Node Adding, IEEE Trans. Ind. Inf. 10 (2014), 1133–1143.

[21] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks. 57 (2013), 2266–2279.

[22] M. Cheminod, L. Durante, A. Valenzano, Review of Security Issues in Industrial Networks, IEEE Trans. Ind. Inf. 9 (2013), 277–293.