Chapter

Compound Cryptography for Internet of Things Based Industrial Automation

J.S. Prasath

Abstract

Internet of things based industrial automation systems are widely used for process monitoring, and control applications. The security threats increase due to the internet is an open environment. This proposed work is the implementation of secure monitoring of plant information through the Supervisory Control and Data Acquisition (SCADA) system. The modified asymmetric and hash algorithm is proposed which generates the large key size of 4096-bit and 512-bit respectively. This proposed security algorithm is implemented using the ARM Cortex A53 processor which performs data encryption and decryption. It provides authentication and integrity of process information across the internet. It achieves a data transfer rate of 300 Megabits per second and more than 95 percent efficiency. This proposed work can be applied for securing the internet-enabled industrial automation process and allows secure monitoring of plant information in remote areas. The security of sensitive process parameters is enhanced through the proposed large key size in asymmetric algorithms. This proposed security algorithm prevents the damage to industrial devices from unauthorized access and modification. It assures the smooth functioning of plant operations and also provides safety to plant operators.

Keywords: Security, industrial networks, SCADA, encryption, decryption, Internet

1. Introduction

Industrial automation plays a major role in real-time data acquisition and control applications. Modern industries depend on vastly more automation and intercommunication. Industrial process equipment is automated to do periodic data collection, event detection, control operation, real-time data acquisition, real-time inventory management, alarming etc. Industrial automation system makes installation flexibility, reduces the repairs costs, disintegration of machine control functions, monitoring the mechanical equipment parameters, error detection and improves the overall efficiency of plant operations. An industrial automation system is a computer system which monitors and controls the various industrial processes such as petrochemical plants, power plants, water treatment plant, oil and gas, food production etc. The behavior of the process changes due to the attack during data communication between devices. Automation devices such as SCADA and Programmable Logic Controller (PLC) does not have inbuilt security mechanisms.

The suitable security algorithm is essential to protect the process equipment and its information from unauthorized access.

The SCADA system is widely used in industrial automation for monitoring and controls the process parameters. It is used for data gathering in a variety of applications such as power generation, petrochemical, sewage and water treatment systems, food and pharmaceutical industry. The monitoring and control of process parameters takes place in remote areas to keep up the steady state of process. SCADA systems include Master Terminal Unit (MTU), Remote Terminal Unit (RTU), network devices and SCADA software. SCADA alerts operators by alarm when conditions become hazardous. The SCADA system includes RTU, and Programmable Logic Controllers (PLC) which collect data from end-point devices like actuators, pumps, or other sensors and control ongoing processes in a plant. The plant sensitive information is transmitted between MTU and RTU that is unsecure and unsafe plant operations. The process data can be accessed and modified by the attackers. The security mechanisms are essential to protect the SCADA system from unauthorized access and to give safety for plant operators.

PLCs are used to control the process parameters and to ensure smooth plant operation. PLC and SCADA system is used together in automation and management of processes in real-time. PLCs are connected to a Human-Machine Interface (HMI) which presents current input and output values to the operators and accepts commands from the user. In SCADA system, RTU provide high processing power, communication capabilities and flexibility as compared to PLCs. The data transmitted from the PLC need to be protected from the attackers. The process data must be encrypted using suitable cryptography and the cipher text is to be transmitted over the internet to ensure confidentiality. The decryption algorithm is to be used at the receiver to get the process data in original plain text. The security policies and security mechanisms are essential for internet enabled industrial automation system.

2. Advances in industrial automation system

The industrial data gathering and monitoring has greatly improved by the wireless standards and internet. The real-time process information can be transmitted through wireless medium and monitored through the internet anywhere in the world. The plant information can be monitored and controlled with the SCADA system through the internet. The control operations and management of sensitive process information are carried out in the master station. Human Machine Interface (HMI) allows operators to read various physical parameters and status of alarm. The general monitoring and supervisory functions are carried out in the corporate networks. The functions of Remote Terminal Unit (RTU) are to monitor the field analog and digital parameters and transmit data to the central control room. RTUs are connected through the remote networks.

The need for security increases due to the integration of industrial networks with Information Technology (IT) networks. Wireless and Internet technologies are essential to monitor and control the process data efficiently. The benefit of wireless technologies in industrial networks provides mobility, to manage substations, and it requires little installation and preservation cost. The control and automation functions can be performed in real-time over the internet by the use of TCP/IP standard in SCADA transmissions. The technological advancement in industrial network operations gives rise to various security risks and challenges in managing IT networks while integrating with both SCADA and corporate networks. The use of Internet in industrial networks creates additional security hazards and safety

issues in the automation system. The major intrusion takes place in communication medium and data modification. The existing industrial automation equipments were not built with security mechanisms. Attackers may create new process information, can alter the process data and capture the physical channels. This leads to failure of process equipments and heavy loss to industries. It is essential to propose the novel security mechanism for secure operation in web-based industrial networks.

3. Review of security issues in SCADA networks

The major technological, operational and organizational changes increase the security problems. Most of the industries focus on improving the security in data communication, safety standards and cost reduction by applying innovative technology design. The standards and regulations of data security have to be applied during design, implementation and execution of the industrial process to ensure adequate safety, consistency and lifecycle effectiveness for all parties involved in the plant operations. Industrial Control System security requires secure management of work flow and policies. The security management involves physical access control, physical intrusion detection etc. It also requires the device security where the hardware, software and firmware need to be protected. The security in communication is another aspect where the message or data need to be protected. The supervisory and control operations are carried out by integrating the SCADA devices with remote web-based networks. Due to the web-based operation, SCADA devices become more vulnerable to various attacks.

Intrusion detection system is one of the software applications which monitors the network activities for violations and produces reports to the management. The status of security is to be monitored and tested by the continuous security assessment in the security management system. Cryptography is used to address important aspects of communication security, such as, message authentication and integrity as well as confidentiality. The hybrid cryptography algorithm is proposed which combines the asymmetric, symmetric and hash algorithms along with the dedicated hardware key all together strengthens the plant information security [1]. This hybrid algorithm provides confidentiality, integrity and ensures privacy in accessing the sensitive process data. It is essential to propose strong security mechanisms for accessing the process information through internet. The highly secure encryption decryption algorithm is proposed which is simple and it can be used for cloud computing-based applications [2]. This algorithm is based on efficient logical operations, such as XORing, addition, and subtraction as well as byte shifting. It allows selecting the secret key length and the number of rounds to generate the cipher text. Key management is the most dynamic field of research in cryptography and there are challenges in the area of industrial plant key management. The critical information such as passwords and encryption keys should be kept confidential due to security concerns in industries.

The industrial process parameters should be protected from unauthorized access during transmission. The security mechanisms are essential for data monitoring, storage and control. An enhanced data security algorithm is proposed to ensure security in the cloud [3]. The SHA-256 hashing and AES encryption algorithms are used to maintain integrity and confidentiality in the cloud. A novel parallel cryptographic algorithm is proposed which overcomes the drawback of symmetric security algorithm and hash algorithm [4]. The analysis was done with respect to computation time. The run time is less as compared to the RSA-MD5 algorithm. The additional layers of hybrid function can be performed to enhance the data integrity and security. A peculiar security protocol is formed to increase the level of security [5]. It increases

the level of security by incorporating MD5 algorithm and combining the AES with RSA algorithms. The encryption and decryption of image files can be performed using the hybrid algorithm. A hybrid cryptographic algorithm is proposed which combine the Blowfish and MD5 hashing algorithm to increase data security in the cloud [6]. The various parameters include file size and execution time is evaluated. It takes less time for encryption and decryption and it occupies less storage space. An innovative identity based hybrid encryption is proposed to increase the security of outsourced data [7]. The encryption is performed using RSA and Elliptic Curve Cryptography (ECC). The data is encoded along with receiver identification. The identity and the keyword are encrypted using Proxy Re Encryption. It achieves efficiency and assures the security of user message. The hybrid cryptography algorithm is proposed which includes symmetric and hash algorithms that ensure confidentiality and integrity of process parameters [8]. It is implemented with the embedded system which enables secure monitoring of plant information over internet.

The Intrusion Detection System (IDS) is essential to preserve the SCADA system from internet attacks. IDS monitor the network activities and host to detect the security threats. The clustering based IDS are proposed to detect the attacks on SCADA systems [9]. SCADA attacks were detected by normal and critical states of process parameters of target system. When the process parameter reaches the critical state, alarms are raised. The criticality scoring algorithm is proposed to determine the state of the target system. The distributed and networked approach of SCADA system increases the cyber-attacks. The major threats are unauthorized access to the control software and network intrusion. The various possibilities of cyber-attacks on SCADA system is evaluated by using two Bayesian attack graph models [10]. The probabilities of the intruder influence the destination is determined by the Bayesian attack graph model. The evaluation results infer that the reliability of the power system becomes less due to the increase in attacks against cyber components and skill levels of attackers. The energy efficient security architecture is proposed for wireless based industrial automation systems [11]. The packet protection based on encryption consumes energy in the case of battery powered devices. The packet based selective encryption is also proposed which reduces energy consumption and detection of attacks. The results infer that the intrusion is difficult to distinguish from normal disruption at industrial operations. A Dynamic Security management mechanism is proposed which reduces security hazard, deadline miss ration and process elimination ratio of discontinuous actual process compiling on server systems [12]. The time and power utilization of extensively used security mechanisms are measured. A security hazard measures is introduced which quantifies the strength of security in real-time operations. A dual-level feedback control scheme is designed to notify the task scheduling issues. The future work includes proposal of security assessment for shared control in enterprise networks and integrity protection. A multilayer cyber-security scheme is proposed which is based on Intrusion Detection System (IDS) for safeguarding SCADA in smart grids [13]. In this work, external malicious attack is identified by a SCADA-specific IDS technique. A cyber security test-bed used to investigate vulnerabilities and hybrid intrusion detection approach is implemented in a SCADA system. The test-bed is the setup of grid connected solar panel based SCADA system in real-time. This proposed multi-attribute SCADA-IDS provides early alert, intrusion detection and prevention and abnormal behaviors in SCADA based automation system. A key management scheme is evaluated which includes session and master key updates [14]. The master station is responsible for producing the session keys. The Elliptic Curve Diffie-Hellman protocol is used in the master key update phase. This scheme of key management supports the MODBUS implementation with the required speed, greater efficiency and achieves high degree of security in SCADA communication.

The cryptography is essential for secure communication of plant information through SCADA networks. The characteristics of cryptographic algorithms are analyzed in terms of energy and time related for embedded real-time systems [15]. The analysis indicates that energy consumptions of security algorithms are non-linear to the size of the plain text. The energy cost is proportional to the run time of security algorithm with variable data size. Based on this analysis, the application of cryptographic algorithms can be extended in embedded real-time applications. The security issues in Industrial Automation and Control System (IACS) are analyzed which includes risk assessment, countermeasures, validation and monitoring of results [16]. The analysis ensures the satisfied security level can be achieved for a distributed industrial system. The efficient security management solutions will become tough due to the complexity and size of IACS. It is essential to propose advanced mechanisms to support IACS security.

A network filtering approach is proposed for the detection and mitigation of cyber-attacks [17]. It is based on the packets analysis of communication between master and slaves of SCADA system and monitoring the state of the protected system. The benefit of this proposed work is that it provides less number of negative results. A Critical State Analysis and State Proximity for detection of intrusion are proposed for SCADA systems [18]. A multidimensional metric approach is introduced which provides the measurement related to the length between a critical state and the given states. The unique security issues in electric power system are addressed which is based on SCADA Networks [19]. The SCADA system is secured by using symmetric encryption. The master station takes the Key Distribution Center (KDC) and it initiates the communication. The slave station includes security devices which generate the session key, perform the key encryption with the master key and transmit it to the equipment on the master station.

The trust system is proposed which perform active security analysis and response in order to increase the security of SCADA systems [20]. The status information delivery, issue of network node commands, packet delivery analysis in various protocols and arrangements are performed by the trust system.

The key management architecture is proposed for SCADA System that requires less number of keys stored in a RTU [21]. It reduces the operational cost for group communication. Group link is attained by using the key hierarchy configuration. The Master Terminal Unit (MTU) is able to send the information between a Sub-Master Terminal Unit and Remote Terminal Unit. In this proposed key structure, two classes of communication which includes communication between MTU and Sub-MTUs and between Sub-MTUs and RTUs. The impact of traditional Information and Communications Technologies (ICT) malware is focused on SCADA systems [22]. The experimental test-bed which includes software toolkit called MAlSim (Mobile Agent Malware Simulator). MAlSim agent class is used for simulation of malware. The vulnerabilities exist in the SCADA systems due to network connections, access control, protocols and software. A vulnerability estimation scheme is proposed to estimate the susceptibility of SCADA systems in terms of access points [23]. This work quantifies the potential impact on causes of attack. The method used in this work is to assess the losses in power system and computer networks susceptibility due to cyber-attack.

4. Overview of existing security mechanisms

The security is a major concern for industrial operations and the process plant information should be protected from unauthorized access. The existing security mechanisms are adopted for intrusion detection, cyber-attacks, risk management, data

Algorithm	Key size	Block size	Rounds	Encryption Speed	Security
AES	128, 192, 256 bits	128 bits	10, 12, 14	Fast	Considerably Secure
DES	56-bits	64 bits	16	Very Slow	Inadequate Security
3 DES	112-bits	64 bits	48	Very Slow	Adequate Security
RC2	8–128 bits	64 bits	18	Fast	Vulnerable
RC5	2040 bits	128 bits	255	Fast	Considerably Secure
Blowfish	32–448 bits	64 bits	16	Fast	Vulnerable
Proposed Algorithm (RSA and SHA)	4096-bits and 512-bits	470 bytes, 1024 bits	80	Fast	Highly Secure

Table 1.
Comparison between standard and proposed cryptography algorithms.

protection by cryptography, network firewall etc. The security threats increase due to process monitoring and control through internet. It is essential to ensure process data security and privacy in accessing the plant information in the automation system.

Table 1 shows the existing security mechanisms, its advantage and disadvantage. It is identified that there is a large number security issues arises due to the integration of SCADA Network with the Information Technology Networks. Traditional ICT countermeasures cannot provide complete protection to SCADA systems. Conventional Security mechanisms are not suitable to handle the new security problems. Even though the varieties of security mechanisms are proposed, still there is a lack of security in the modern industrial automation systems. It is essential to propose efficient and less complex security algorithm to secure the data communication takes place between SCADA Networks.

The existing security mechanism for SCADA networks are related to hybrid encryption, intrusion detection, key management, and packet based encryption etc. The lack of strong dynamic security management mechanisms exists related to cryptography for securing SCADA systems. The SCADA system deals with remote monitoring and control of sensitive process parameters. The strong cryptographic algorithm is essential to protect the process information and equipment from unauthorized access. The existing security mechanisms and algorithms are inadequate to achieve strong security. The attackers can easily capture the process data, modifies it and retransmit to the destination. The security attack leads to failure of process instruments, major losses to the management and unsafe working condition to operators. The hybrid security algorithm is proposed to secure the plant parameters in wastewater treatment process across the internet [24]. It includes symmetric and secure hash algorithm to protect the wastewater parameters from unauthorized access and modification. It is essential to implement the protocols for secure data transmission in embedded system with wireless networks.

This proposed work focuses on securing the process information by incorporating modified asymmetric and hash algorithms. It ensures secure monitoring of plant information in real-time applications. It combines the asymmetric encryption and hash algorithm which provides data confidentiality and integrity. The large key size of 4096-bits is generated using asymmetric encryption which is not exists in the previous work and it enables secure transmission and monitoring of process information through the internet.

5. Proposed compound cryptography algorithm

The temperature and gas process data is secured by performing hybrid cryptographic algorithm which includes modified asymmetric encryption and hash algorithm. The public and private keys are generated in the asymmetric algorithm to perform data encryption and decryption in order to ensure data confidentiality.

5.1 Key generation

5.1.1 Modified asymmetric algorithm

Asymmetric algorithm involves usage of public key and private key. The public key is used for encryption of process data and the private key is used for decryption of process data. It enhances the security level of sensitive plant information due to the usage of two keys.

The various steps involved in asymmetric algorithm are given below. These include

- Generation of public and private keys
- Encryption
- Decryption

5.1.1.1 Algorithm steps

- Select two different prime numbers: i and j
- Calculate s = i*j
- Calculate g (s) = (i-1) (j-1)
- Select integer 'd' such that gcd(g(s)) = 1; 1 < d < g(s)
- Calculate e, e = d^{-1}(mod(g(s))
- Public key, PU = (d,s)
- Private key, PR = (e,s)

5.1.2 Encryption

After generation of public and private keys, encryption is performed to convert the raw input data into cipher text that is., unreadable format. The encryption of plant information is performed at the transmitter. The encrypted data is transmitted across internet.

Assume that the original input is denoted by 'T'. The cipher text is obtained by the formula given below.

- Original text: T
- Cipher text: C = T^d mod s

  where d – Public key.

5.1.3 Decryption

The cipher text is obtained at the receiver and performs decryption. It converts process data in unreadable format to original plain text. The original plain text is obtained by the formula given below.

- Original text: $T = C^e \bmod s$
  where e – Private key.

The large key size of 4096-bit is generated in this proposed modified asymmetric algorithm. The hash algorithm is proposed which generates different hash value in order to ensure data integrity. The SHA (Secure Hash Algorithm)-512 generates intermediate hash value using the message block as key. The block size is 1024-bits, the word size is 64-bits and the number of rounds is 80. The SHA-512 algorithm is highly secured as compared to the MD5 (Message Digest) algorithm.

5.2 Secure hash algorithm (SHA-512)

The SHA hash function converts input value of approximate to a constant length. The hash is smaller than the input data and it is a tiny representation of a big data which is referred to as digest. The hashing algorithm involves processing of hash function and each block size varies depending on the algorithm. The capacity of the block varies from 128-bits to 512-bits. It involves round function in which each round takes an input of a uniform size, typically merging of the latest information block and the result of the last round. The modified SHA1 algorithm is developed which expands the hash value from 160-bits to 1280-bits [25]. It is achieved by allocating four buffer registers in each round inside the compression function for eight times. This hash value was not hacked against brute force attack. The hash algorithm protects the password storage and it is used to check the data integrity.

5.2.1 Description of SHA-512

The input message is padded first to obtain the block size of 1024-bits. The message schedule is generated to process the 1024-bit block size of the input message. It consists of eighty 64-bit words. The first 16 words are directly obtained from the 1024-bit message block. The remaining words are generated by performing permutation and mixing functions to the previously generated words. The modified asymmetric and hash algorithm is proposed that generates large key size of 4096-bit and 512-bit respectively [26]. It provides authentication and integrity of process information across internet. Authentication is essential to ensure the plant information is accessed and controlled by the authorized users.

The message block consists of two inputs which are 512-bit hash buffer and the 1024-bit message block. The hash buffer contents are processed along with the input which is called round function. The round function is to be performed for each block of 1024-bit input message. The eighty rounds are to be carried out for each message block. The eightieth round output is added to the hash buffer contents at the starting of the round process. This addition is performed for each 64-bit word of the output. The message digest is obtained from the content of hash buffer which is the processing of all N-message blocks. The key generation and encryption algorithm is proposed for ensuring privacy in Mobile Ad-Hoc Networks [27]. This key generation algorithm adds scrambling factors to generate random key sequences with essential length but incurred low execution overhead, whereas the encryption/decryption algorithm utilizes the One Time Pad (OTP) system by

adding scrambling factors for data confidentiality which satisfies the randomness, diffusion, and confusion tests.

Figure 1 shows the generation of message digests of SHA 512 algorithm. The input message is first divided into block of 1024-bits long. The messages of each 1024-bit block are denoted by M (1), M (2)...M (N). The message blocks are processed one at a time, starting with a fixed initial value H(0), sequentially compute

$$H(i) = H(i-1) + C_M(i)\left(H(i-1)\right)$$

where C – Compression function.

Figure 2 shows the processing of single 1024-bit block. The message schedule array has eighty 64-bit words. Each 1024-bit block is performed with 80 rounds to generate hash value.

Figure 3 shows round function of SHA-512 hash algorithm. The intermediate output is generated which is equivalent to the addition of modulo 2^32 sum of.

The following quantities are performed logical XOR operation.

- Rotation of block towards right by 14 places
- Rotation of word towards right by 18 places
- Rotation of word towards right by 41 places

The additional quantities are also appended with the eighth word in the block modulo 2^64:

The following quantities are performed with logical XOR operation.

- Rotation of the first word in the block towards right by 28 bits

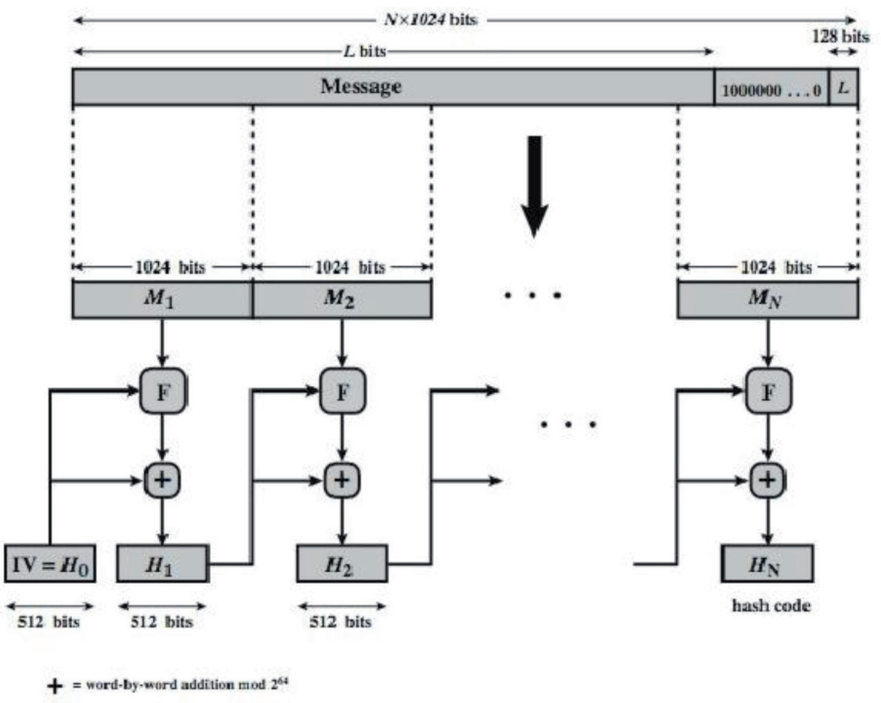

Figure 1.
SHA-512 for generation of message digest.

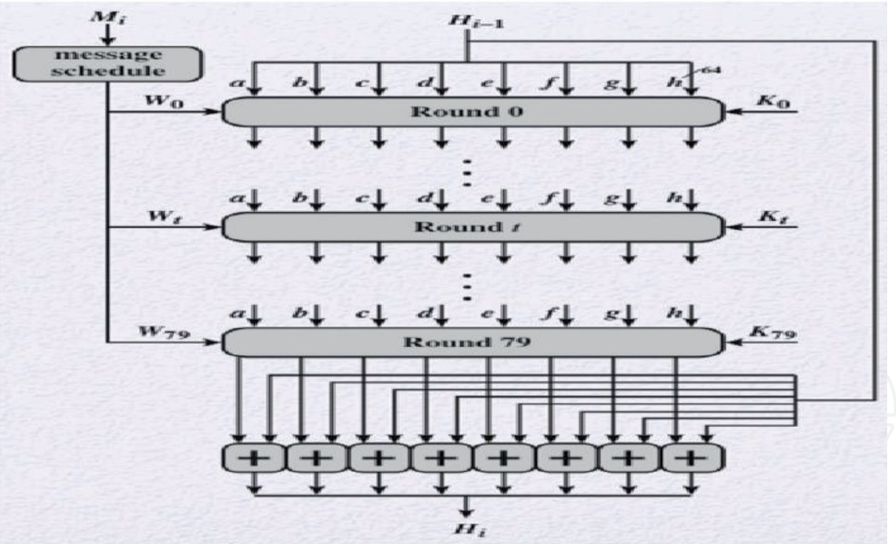

Figure 2.
Processing of SHA-512 single 1024-bit block.

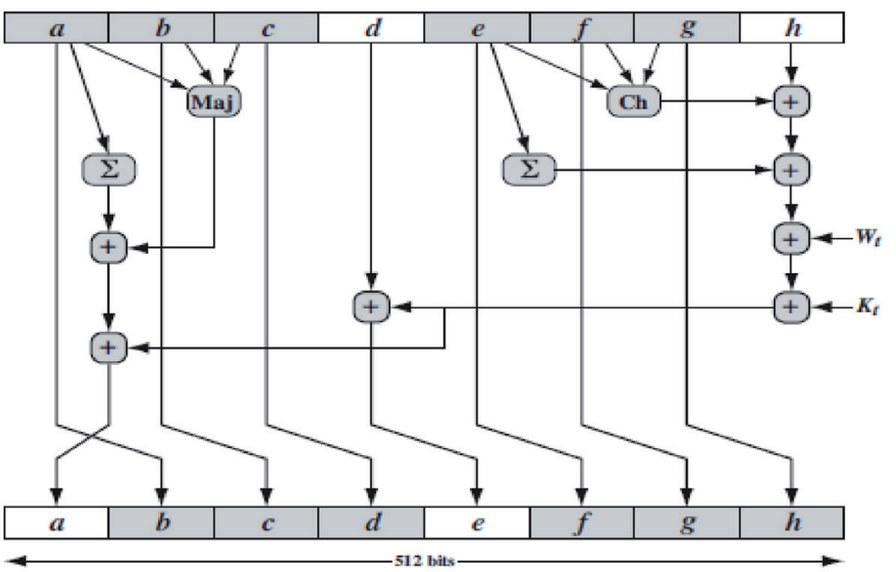

Figure 3.
SHA-512 round function.

- Rotation of word towards right by 34 bits
- Rotation of word towards right by 39 bits

Finally, each of the eight words of the block that will ultimately become the hash is moved to the position of the next word in the block, with the first word in the block being replaced by the modified eighth word in the block.

The first step is to perform modified asymmetric encryption using public key. The SHA-512-bit block cipher algorithm is performed to generate hash value. The hash algorithm ensures IP security and data integrity. The process data in cipher text is transmitted across the internet.

This proposed work uses large key size of 4096-bit in the modified asymmetric algorithm and the number of rounds can be varied. It performs data encryption at very high speed. This proposed hybrid cryptographic algorithm achieves higher level of data security. It can be applicable for securing the

Authors	Algorithm	Key size	Block size	Rounds	Security
Vikas K.Soman [2017]	AES, ECDSA, SHA-256	128, 256 bits	128 bits	10, 12, 14	Medium Security
Adviti Chauhan [2017]	Blowfish, MD5	32–448 bits	64 bits	16	Medium Security
M. Harini [2017]	AES, RSA, MD5	128, 1024 bits	128 bits	10	Medium Security
Anushka Gaur [2017]	Blowfish, MD5	332–448 bits	64 bits	16	Medium Security
Prabukanna [2016]	RSA, ECC	1024 bits, 256 bits	128 bits	—	Highly Secure
Proposed Modified Compound Cryptography algorithm	RSA and SHA	4096-bits and 512-bits	470 bytes, 1024 bits	80	Highly Secure

Table 2.
Comparison between existing and proposed cryptography algorithms.

sensitive plant information in industrial applications. The cipher text is received through the internet. The modified asymmetric decryption is performed using 4096-bits private key at the receiver. The key length is a major factor in securing the sensitive process data. The larger key size ensures that the brute force attack is infeasible. The process data in original numerical form is monitored through the SCADA system.

Table 1 shows the comparison between standard and proposed cryptographic algorithms. As compared to standard algorithms, the large key size as well as block size is generated in the proposed security algorithm. The proposed asymmetric algorithm produces the large key size of 4096-bits that strengthens the security to higher level. The number of rounds used in SHA-512 is 80 for each message block. The size of each message block is 1024-bits long. It achieves high speed of encryption. This proposed algorithm strengthens the level of security. It is suitable for securing highly sensitive plant information in industrial operations.

Table 2 shows the comparison between existing and proposed cryptographic algorithms. The asymmetric algorithm used in the proposed work generates large key size and provides authentication. The hash algorithm is also used which ensures data integrity. The key size of the existing security algorithms is low and the key size is increased in this work. The number of rounds also increased during the process of encryption. This proposed work uses one key for encryption and another key for decryption.

6. Implementation of embedded based secure process monitoring through SCADA system

Figure 4 shows the transmission of temperature and gas process data in cipher text. The temperature and gas process data is sensed by the sensor and it is transmitted to the embedded system. This process data is encrypted using the embedded system. The hybrid encryption algorithm is proposed which combines the asymmetric encryption and hash algorithm. The encrypted data is transmitted over the internet.

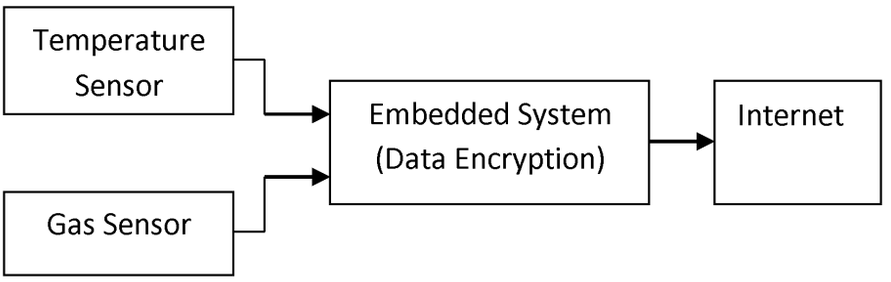

Figure 4.
Transmission of process data using embedded system with internet.

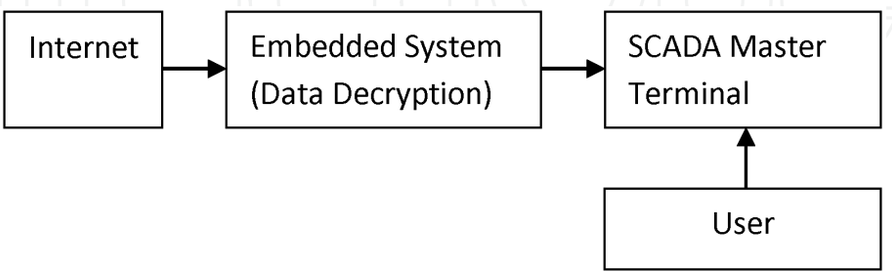

Figure 5.
Reception of process data using SCADA system with internet.

Figure 5 shows the reception of process data in cipher text through internet. The decryption is performed using embedded system and the original data in numerical form is monitored through SCADA master terminal unit.

7. Results and discussion

This proposed modified compound cryptography algorithm is performed using python. This modified asymmetric algorithm generates large key size of 4096-bit and the modified hash function of 512-bitmessage digest is generated which ensures data integrity over wireless networks. The private key is used only by the receiver to decrypt the process data. The public key is used by the sender to encrypt the process information.

7.1 Generation of private key and public key

The large key size of 4096-bit private key is generated from the modified asymmetric encryption which strengthens the security of sensitive process data. The private key and public key generated from the proposed modified asymmetric algorithm is given below.

-----BEGIN RSA PRIVATE KEY-----.

MIIEpAIBAAKCAQEAms7TPybmkXuzbEGcfQsBuHu2SigegjXbzlrS94ktXN
evH40cpjEGEfUYxX3qoUwJXhTSNb9TnoTRNdL6cgwhdByly07dEM7 + sfK1Jw/
lvLjsZQmYuoIWfJJAmNey55rD/oqkFV6wnpG5O97JJEHjCEDqpqbcUoqmbPBBAUs-
P5yZcvAhKJorhicPajBnN8ZOoYm6pv/1KmVBtNxY/edSKQFUsekbbMvjgkpWcqaB-
bGsR62NWPErK58jUReJrPYI39u + 97yGEEu3Wm2zOXjAqmTX2 + 6Jb1cXC7lMzdZ/
UOQRz9Fw + BdHCIeJRMUktdjdQD4BNq5kub4tTAcqU2h6AyUQIDAQABAoIBAG
Pd5P0qdTeJG3hM40zvWs7OUAyK0ROi9weqI8q4XeE06q5p8/9qRMY03SQaVNB1It
3khK9Tm/f5KpWUYyhLlxE2oeYEHCyJvFjDgAWRBd23VhjgFfzLiwIVv0Jac/lhJ + r/

OVbn3PyOeXacBBo1vuZGKpoTrrI465//ZZAWAk5Uukb9h9CzHCiSQofbx68qXMK/
bXuiWFFGRWSdOSN53eX3j/gm8 + wvWRwYBnahIhgoLIQd8mVwzSoimg-
4sQnAenep7y6a + 0znATQNU1boANn2vDyUHtKLIbLBI9fHAycWg3 + nKQ
AUBTFsxvPSBulAFalfHbSqLGGsuUW+pk1HiCKECgYEAxcXyor8Flys1Gd/
lOGJPdsOitnlvecQgTZjKks+Hqfferxketdvb0mG7Hiimmz75QN + 8D6yHR/
rl4rlKERTGMqm/5K6C + HQ5qUOHmneyWefRV + gKu1Zt1YcLSSY0D-
pbn2LUqW6YHueBjJLPkBM7IyZGNtcn9niQPjda8MvcP32UCgYEAyGK-
bNrdrP4U8RlJIz6vbyo4F0viQh1ydNY6PgX/038y19dey + mPk8MQh3nZFw-
vN0rpsSgcOqjSj/1avXETmlGNMhFM2IfR5jnGW0oQMD8nRXfe0qheB2sEeV
xlQlITIhP2WAxDOelKff0iq4yJlC5Y0utpzIC5Xq8Rq8RcA4xn0
CgYEAiFggHzyr4PyjnhPx1b5I5CqZOU1cocipMHW + ahnyg-
CXm+jXKKzvIPzCrLG5/9ZUjhyr3XqLlnKUG6RguTLpSrUjDhyccGacevWdVzBLq/
PpJI15QT7iU/dkc2bAhwVEdwxOagRZkSyu7jekKsJnSaMwUsxfu5aAcrP82Pbh/09
UCgYEAtyAGILb2uBIWx10jVUYFktK/19F4o3ur3 + nsk7hQHMaD86uv0MvByZY-
0LY2Aq2y50We + PgCGuIIjay2jWgaILmuj69L5TP6coa0AqbSLwuM3ock/9yDu1qJU
6e60D + Y0JC + qwaM65TeVgAey3v/Q9t9TNWeKGaxkDPsV29iTCjECgYA0cNjdb/
ifHRL0QMy3oJJjn3HAFDwbpO1UN0CQ2SoVfob1Cy7byq2NTnf-
PjHjheeVmLW6e3zMxHfezAJ42y3SNLHH5vVJkauecorZZMnVC8iVla8v0D/
Yvti8bkigt4YcQGWSpTE8Trdjfdr6gNOgrvJrVHWvD4R78ftZS7O + 5A=
=7fEnw52DyQMSF4U35duRJfs/g3HsNGDyhLlxE2oeBRDGrtKWdgDVR-
5ghes4xf63jkhueijvzdfhuucTG8jtjdihdbnhnxndflkldd VhjgFfzLiwIVv0Jac/lhJ + r/
OVbn3PyOeXacBBo1vuZGKpoTrrI465//ZZAWAk5Uukb9h9CzHCiSQofbx68qXMK/
bXuiWFFGRWSdOSN53eX3j/gm8 + wvWRwYBnahIhgoLIQd8mVwzSoimg-
4sQnAenep7y6a + 0znATQNU1boANn2vDyUHtKLIbLBI9fHAycWg3 + nKQ
AUBTFsxvPSBulAFalfHbSqLGGsuUW+pk1HiCKECgYEAxcXyor8Flys1Gd/
lOGJPdsOitnlvecQgTZjKks+Hqfferxketdvb0mG7Hiimmz75QN + 8D6yHR/
rl4rlKERTGMqm/5K6C + HQ5qUOHmneyWefRV + gKu1Zt1YcLSSY0Dpbn-
2LUqW6YHueBjJLPkB7IyZGNtcn9niQPjda8MvcP32UCgYEAyGKbNrdrP4U8RlJIz-
6vbyo4F0vih1.

ydNY6PgX/038y19dey + mk8MQh3nZFwvN0r-
psSgcOqjSj/1avXETmlGDZiAy5w7cvgjhhRTdxujNh-
j2gbdrrbcsxgnhhsvdDVGgtsrWAxDOelKff0iq4yJlC5Y0utpzIC5Xq8Kvdyij8dpsufjk3-
etundfDGTyhu4HYVsuiv7MRC4JTNEVthr6JFB8xnfmshJRMC7fklnuihvduhsuih-
HBGdbvhdn4hjbh9hjbhBVH3Jbvkj4shrh/rTNKJnbuir4bhjsbvBGHH9uhuiHgfsdv/
gubSJ5ohybvj8afhvuIBJKugibv.

-----END RSA PRIVATE KEY-----.

-----BEGIN PUBLIC KEY-----.

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAms7TPybmk
XuzbEGcfQsBuHu2SigegjXbzlrS94ktXNevH40cpjEGEfUYxX3qoUwJXhTSN
b9TnoTRNdL6cgwhdByly07dEM7 + sfK1Jw/lvLjsZQmYuoIWfJJAmNey55rD/
oqkFV6wnpG5O97JJEHjCEDqpqbcUoqmbPBBAUsP5yZcvAhKJorhicPa-
jBnN8ZOoYm6pv/1KmVBtNxY/edSKQFUsekbbMvjgkpWcqaBbGsR62N-
WPErK58jUReJrPYI39u + 97yGEEu3Wm2zOXjAqmTX2 + 6Jb1cXC7lMzdZ/UOQRz
9Fw + BdHCIeJRMUktdjdQD4BNq5kub4tTAcqU2h6AyUQIDAQAB.

-----END PUBLIC KEY-----.

The modified hash algorithm of 512-bit message digest is proposed which operates on eight 64-bit words. Each block is considered as sixteen 64-bit words, eighty 64-bit words are produced.

The initial input value to SHA-512 is hexadecimal and is given below.

7D03A66713842D93 1F83D9ABFB41BD6.
3C6EF372FE94F82B A54FF53A5F1D36F1.
5BE0CD19137E2179B05688C2B3E6C1F.
2BF549C5158E2A72510E527FADE682D1.

Each of the eight words in a block becomes the hash which is shifted to the position of the next word in the block. The first word in the block is being replaced by the modified eighth word in the block. The constant words of length 80 used in SHA-512, obtained from the fraction of cube roots of the first eighty primes, which are:

766A0ABB3C77B2A8A831C66D2DB43210240CA1CC77AC9C6E2748774CD
F8E5D353380D139D95B3DF4CC5D4BECB3E42B6923F82A4AF194F9B
CA273ECEEA26619391C0CB3C5C95A63243185BE4EE4B28C550C7DC3
D5FFB4E2983E5152EE66DFAB72BE5D74F27B896F80DEB1FE3B1696B19BDC06A7
25C71235 C19BF174CF692694C 92722C851482353B6EFBE4786384.

F25E3AB5C0FBCFEC4D3B2 A0FC19DC68B8CD5B00327C898FB213FEAD.

A7DD6CDE0EB165CB0A9DCBD41FB D876F988DA83115312835B01457.

06FBE2DE92C6F592B0275BF597FC7BEEF0EE47137449123EF65CD2J
L7C6E00BF33DA88FC2D5A79147930AA72559F111F1B605D019142929670A0E6E7
03GU281C2C92E47EDAEE62E1B21385C26C92619 A4C116B8D 2D0C8
4D2C6DFC5AC42AE50A73548BAF63DE428A2F98D728AE22E49
B69C19EF14AD227B70A8546D22FFCN6KVC24B8B70D0F89791A4506CEB
DE82BDE9C76C51A30654BE308CC702081A6439EC4A7484AA6EA6
E483 5FCB6FAB3AD6FAECA2BFE8A14CF1036 CF40E35855771202E9B5DBA581.

89DBBC3956C25BF348B538F57D4F7FEE6ED178 4B0BCB5E19B48AD807.

AA98A30302426C44198C4A4758174C9EBE0A15C9BEBC90BEFFFA23631
E2597F299CFC657E2AC67178F2E372532B106AA07032BBD1B884C87814.

A1F0AB72C28DB77F523047D841B710B35131C471B78A5636F43172F604
2CAAB7B40C72493D7AB1C5ED5DA6D81181E376C085141AB5D186B8C.

721C0C207 6D192E819D6EF521806F067AA72176FBA0A637DC5A2C898.

A6113F9804BEF90DAE A81A664BBC423001682E6FF3D6B2B8A3BEF9A3.

F7B2C67915431D67C49C100D4C5B9CCA4F7763E373Y4N06CA6351E003.

826F748F82EE5DEFB2FC4ED8AA4AE3418ACB D69906245565A910.

The above hash value changes when the input value applied to the modified hash algorithm is changed. It ensures data integrity during transmission over wireless networks. The combination of modified asymmetric and hash algorithms ensures secure monitoring of plant information and protects the sensitive process data from unauthorized access. It also ensures smooth functioning of plant equipments which deals with data monitoring and control applications. Asymmetric algorithm is complex and it achieves higher level of security than the symmetric algorithm. Hash function provides protection of password and ensures data integrity. It is necessary to propose the security algorithm that ensures end-to-end secure plant operations, low latency and high speed.

8. Conclusion

This proposed work is the implementation of modified asymmetric and hash algorithms using embedded system with process monitoring through internet. The temperature and gas process data is read through the sensor and encrypted using the embedded system. The strength of the proposed modified asymmetric encryption is it generates large key size of 4096-bit and the 512-bit message digest to ensure confidentiality and integrity. This proposed modified asymmetric algorithm

provides authentication and modified hash algorithm provides data integrity as well as Internet Protocol (IP) security. This encrypted data is transmitted across the internet. The cipher text is received through the internet by providing the correct IP address. The decryption algorithm is executed at the embedded system to obtain the plain text. The original process data is monitored through the SCADA master terminal. This proposed work achieves data integrity as well as data confidentiality. It offers low latency and achieves higher efficiency of more than 95 percent in securing the sensitive plant information. It allows secure monitoring of plant information through the SCADA system. This proposed work can be applicable for securing sensitive process information in any industrial applications. It provides the cost-effective solutions in protecting the expensive industrial devices from unauthorized attacks and ensures workers safety.

Author details

J.S. Prasath
KCG College of Technology, Chennai, India

*Address all correspondence to: jsprasath@gmail.com; prasath.ei@kcgcollege.com

References

[1] J. S. Prasath, U. Ramachandraiah, G. Muthukumaran, "Modified Hardware Security Algorithms for Process Industries Using Internet of Things," Taylor and Francis Journal of Applied Security Research, Article in Press, pp. 1-14, 2020.

[2] Amiruddin, Anak Agung Putri Ratna, Riri Fitri Sari, "New Key Generation and Encryption Algorithms for Privacy Preservation in Mobile Ad Hoc Networks," International Journal of Communication Networks and Information Security, Vol. 9, No. 3, pp. 376-385, 2017.

[3] Vikas K.Soman, Natarajan V, "An Enhanced Hybrid Data Security Algorithm for Cloud," IEEE International Conference on Networks and Advances in Computational Technologies, Trivandrum, India, pp. 416-419, 2017.

[4] Adviti Chauhan, Jyoti Gupta, "A Novel Technique of Cloud Security Based on Hybrid Encryption by Blowfish and MD5," IEEE International Conference on Signal Processing, Computing and Control, Solan, India, pp. 349-355, 2017.

[5] M. Harini, K. PushpaGowri, C. Pavithra, M. Pradhiba Selvarani, "A Novel Security Mechanism Using Hybrid Cryptography Algorithms," IEEE International Conference on Electrical, Instrumentation and Communication Engineering, Karur, India, pp. 1-4, 2017.

[6] Anushka Gaur, Anurag Jain, "Analyzing Storage and Time Delay by Hybrid Blowfish-MD5 Technique," IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing, Chennai, India, pp. 2985-2990, 2017.

[7] G. Prabu Kanna ; V. Vasudevan, "Enhancing The Security Of User Data Using The Keyword Encryption And Hybrid Cryptographic Algorithm In Cloud," IEEE International Conference on Electrical, Electronics, and Optimization Techniques, Chennai, India, pp. 3688-3693, 2016.

[8] 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.

[9] Abdul Mohsen Almalawi, Adil Fahad, ZahirTari, Abdullah Alamri, Rayed AlGhamdi, Albert Y. Zomaya, "An Efficient Data-Driven Clustering Technique to Detect Attacks in SCADA Systems," IEEE Transactions on Information Forensics and Security, Vol. 11, pp. 893-906, 2016.

[10] Yichi Zhang, Lingfeng Wang, Yingmeng Xiang, Chee-Wooi Ten, "Power System Reliability Evaluation with SCADA Cyber Security Considerations," IEEE Transactions on Smart Grid, Vol. 6, pp. 1707-1721, 2015.

[11] Riccardo Muradore, DavideQuaglia, "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," IEEE Transactions on Industrial Informatics, Vol. 11, pp. 830-840, 2015.

[12] Wei Jiang, Yue Ma, Nan Sang, ZiguoZhong, "Dynamic Security management for real-time embedded applications in Industrial Networks," Elsevier Journal of Computers and Electrical Engineering, Vol. 41, pp. 86-101, 2015.

[13] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, H. F. Wang, "Multi-attribute SCADA-Specific Intrusion Detection System for Power

Networks," IEEE Transactions on Power Delivery, Vol. 29, pp. 1092-1102, 2014.

[14] AbdalhosseinRezai, ParvizKeshavarzi, Zahra Moravej, "Secure SCADA communication by using a Modified Key Management scheme," Elsevier Journal of ISA Transactions, Vol. 52, pp. 517-524, 2013.

[15] Wei Jiang, ZhenlinGuo, Yue Ma, Nan Sang, "Measurement-based research on Cryptographic algorithms for Embedded Real-time Systems," Elsevier Journal of Systems Architecture, Vol. 59, pp. 1394-1404, 2013.

[16] Manuel Cheminod, Luca Durante, Adriano Valenzano, "Review of Security Issues in Industrial Networks," IEEE Transactions on Industrial Informatics, Vol. 9, pp. 277-293.

[17] Igor NaiFovino, AlessioColetta, Andrea Carcano, Marcelo Masera. 2012. Critical State-BasedFiltering System for Securing SCADA Network Protocols. IEEE Transactions on Industrial Electronics, Vol. 59, No.10, 3943-3950.

[18] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. NaiFovino, and A. Trombetta, "A Multi-Dimensional Critical State Analysis for Detecting Intrusions in SCADA Systems," IEEE Transactions on Industrial Informatics, Vol. 7, pp. 179-186, 2011.

[19] D.J. Kang, J.J. Lee, B.H. Kim, D. Hur, "Proposal strategies of Key management for Data encryption in SCADA network of Electric Power Systems," Elsevier Journal of Electrical Power and Energy Systems, Vol. 33, pp. 1521-1526, 2011.

[20] Gregory M. Coates, Kenneth M. Hopkinson, Scott R. Graham, Stuart H. Kurkowski, "A Trust System Architecture for SCADA Network Security," IEEE Transactions on Power Delivery, Vol. 25, pp. 158-169, 2010.

[21] Donghyun Choi, Sungjin Lee, Dongho Won, Seungjoo Kim, "Efficient Secure Group Communications for SCADA," IEEE Transactions on Power Delivery, Vol. 25, pp. 714-722, 2010.

[22] Igor NaiFovino, Andrea Carcano, Marcelo Masera, Alberto Trombetta, "An experimental investigation of malware attacks on SCADA systems," International Journal of Critical Infrastructure Protection, Vol. 2, pp. 139-145, 2009.

[23] C. Ten, C. Liu, G. Manimaran, "Vulnerability Assessment of Cyber Security for SCADA systems," IEEE Transactions on Power Systems, Vol. 23, pp. 1836-1846,2008.

[24] J.S. Prasath, S. Jayakumar, K. Karthikeyan, "Real-Time Implementation for Secure monitoring of Wastewater Treatment Plants using Internet of Things," International Journal of Innovative Technology and Exploring Engineering., Vol. 9, No. 1, 2997-3002, 2019.

[25] Esmael V. Maliberan, "Modified SHA1: A Hashing Solution to Secure Web Applications through Login Authentication," International Journal of Communication Networks and Information Security, Vol. 11, No. 1, pp. 36-41, 2019.

[26] 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.

[27] Amjad Y. Hendi, Majed O. Dwairi, Ziad A. Al-Qadi, Mohamed S. Soliman, "A Novel Simple and Highly Secure Method for Data Encryption-Decryption," International Journal of Communication Networks and Information Security, Vol. 11, No. 1, pp. 232-238, 2019.