TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

Modified Asymmetric and Hash Algorithms for InternetEnabled Industrial Automation

J.S. Prasath1, Dr. U. Ramachandraiah2
1. Department of EIE, KCG College of Technology, Chennai
2. Department of EEE, Hindustan Institute of Technology and Science, Chennai
Email: jsprasath@gmail.com

Article Info
Volume 83
Page Number: 7431 - 7444
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 18 May 2020*

Abstract:

Industrial automation systems are specially designed for monitoring, controlling and smooth plant operations. Automation systems use the internet for monitoring and control of process parameters. The security threats increases due to the internet is an open environment. Automation devices are not built with security mechanisms preferably for the internet enables process equipment. This proposed work is the implementation ofsecure monitoring of plant information through the Supervisory Control and Data Acquisition (SCADA) system. This modified asymmetric and hash algorithm is proposed which generates the large key size of 2048-bit and 512-bit respectively. This proposed algorithm is implemented using the ARM Cortex A53 processor which performs data encryption and decryption. The ARM Cortex processor used in this proposed work is low-cost, 1.2 GHz quad-core, 1 GB RAM, 802.11n wireless standard, inbuilt High Definition Multi-media Interface, Ethernet and four USB ports. It offers low latency in generating the encrypted process data. This encrypted unreadable information is transmitted across the internet. The process data is decrypted using embedded system at the receiver and the original process data is received through the SCADA system. 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.

Keywords: *Security, Industrial Networks, SCADA, Encryption, Decryption*

I. INTRODUCTION

The industrial automation system plays a major role in real-time data acquisition and control applications. Modern industries depend on vastly more automation and intercommunication. Industrial process equipments are automated to perform 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. Industrial automation devices does not have inbuilt security mechanisms. The suitable security algorithm is essential to protect the process equipments 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 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 in order to maintain the steady state of process. SCADA systems include Master Terminal Unit (MTU), Remote Terminal Unit (RTU), Network devices and SCADA software. SCADA

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

alerts operators by alarm when conditions become hazardous. The field devices of SCADA system includes RTU, Programmable Logic Controllers (PLCs) which collect data from end-point devices like actuators, pumps, or other sensors and control ongoing processes at a specific field site. The process sensitive information is transmitted between MTU and RTU which is unsafe plant operations. The process data can be accessed and modified by the attackers. The security mechanisms are required to ensure safety for SCADA system.

Programmable Logic Controllers (PLCs) are used to control the process parameters and for smooth plant operation. PLCs and SCADA system are 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, RTUs 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. The decryption algorithm is to be used at the receiver to obtain the process data in original plain text. The security policies and security mechanisms are essential for internet enabled industrial automation system.

II. 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.

III. 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 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-

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

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. 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 [1]. 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 [2]. 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 [3]. 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 [4]. 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 [5]. The encryption is performed using RSA and Elliptic Curve Cryptography (ECC). The data is encoded along with receiver identification. The identity and the keyword is encrypted using Proxy Re Encryption. It achieves efficiency and assures the security of user message.

The Intrusion Detection System (IDS) is essential to preserve the SCADA system from internet attacks. IDS monitors the network activities and host to detect the security threats. The clustering based IDS is proposed [6] to detect the attacks on SCADA systems. 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 [7]. 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 [8]. 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 [9]. 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 [10]. In this work, external malicious attack is identified by a SCADA-specific IDS technique. A cyber security

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

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 [11]. 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 [12]. 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 [13]. 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 [14]. 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 [15]. 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 [16]. 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 [17]. 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 [18]. 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 [19]. 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 estimationschemeis proposed to estimate the susceptibility of SCADA systems in terms of access points [20]. The proposed 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.

IV. Overview of Existing Security Mechanisms

The security is a major concern for industrial operations. The industrial process information should be protected from unauthorized access. The

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

existing security mechanisms are adopted for intrusion detection, cyber-attacks, risk management, data 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.

TABLE I COMPARISON OF EXISTING SECURITY MECHANISMS

S.No.	Authors	Techniques	Advantage	Drawback/ Future Work
1	Vikas K. Soman et. al., [1]	AES and SHA-256 algorithms	Enhanced data security in cloud system	To perform comparison and efficiency analysis of various hybrid cryptographic algorithms
2	Adviti Chauhan et. al., [2]	MD5 and Blowfish algorithms	Execution time is less as compared to hybrid RSA-MD5 algorithm.	Combination of various security algorithms can be proposed to achieve higher level of integrity and security
3	M. Hariniet. al., [3]	AES, RSA and MD5 algorithms	It increases the level of security by incorporating AES with RSA algorithms along with the MD5 hashing	Image files need to be encrypted and decrypted
4	Anushka Gaur et. al., [4]	Blowfish and MD5 algorithms	The time taken to perform encryption and decryption is very less time and requires less storage space	Augmentation technique can be adopted with hybrid approach to make it as excellent, and adequate security
5	PrabuKanna et. al., [5]	RSA and ECC algorithms	The security of user message and efficiency is achieved	The various hybrid algorithm can be incorporated to secure the outsourced data
6	Abdul Mohsen Almalawi et. al., [6]	Clustering-based IDS	Determining the general and critical states for an end system Criticality degree of a target system is monitored	Development of incremental model to address the frequent changes in the system specifications
7	Yichi Zhang et. al., [7]	Bayesian attack models	Intrusions are estimated in various paths	Increase in victorious intrusion on the physical systems

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

				and the ability levels of intruders results in less reliability of power system
8	Riccardo Muradore et. al., [8]	Energy-efficient security-aware architecture	Energy consumption is reduced by Packet-based selective encryption technique	Measurements and commands corrupted by deception attacks
9	Wei Jiang et. al., [9]	Dynamic Security Risk Management mechanism	Time and energy utilization of security algorithms is measured	Critical challenge in achieving high level security
10	Yang et. al., [10]	Reducing various cyber-attack hazards	The multi-attribute IDS is behavior-based concept which provides higher level of security to SCADA cyber systems	Smart-grid SCADA systems are vulnerable to large number of cyber security issues, which could threaten digital substations
11	Abdalhossein Rezai et. al., [11]	Key management scheme	The efficiency and security of SCADA communication is enhanced and the desired speed is supported in the MODBUS	RTUs and IEDs have finite processing resources as compared to Master station
12	Wei Jiang et. al., [12]	Performance analysis of security algorithm	Multi-dimensional analysis of cryptographic algorithms in terms of power, speed and energy cost	To propose real-time scheduling with security concern for energy and time-sensitive applications
13	Manuel Cheminod et. al., [13]	Security analysis in Industrial Automation and Control System (IACS)	The analysis related to satisfactory degree of security for a distributed industrial process	The efficient security management decisions will become complex due to the complexity and size of IACS. Modern techniques need to be proposed to enhance IACS security
14	Igor Nai Fovino et. al., [14]	Attack detection Attacks by filtering systems design approach	Firewall detects complex attacks	New security issues arise due to the linkage of enterprise network to the public network. ICT security cannot achieve complete system protection
15	Carcano et. al., [15]	Intrusion detection by Critical State Analysis and State Proximity	A multidimensional metric provides a measure of length	Traditional ICT security countermeasures

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

		technique	between a given state and the set of critical states.	failed in giving an entire security to SCADA systems
16	Kang et. al., [16]	Addressed the problems in SCADA based electric power systems and its security environment	Maximizes the network performance and security by optimal key distribution period based on the Quality of Service (QoS) function	SCADA network integration with Information Technology (IT) networks becomes vulnerable and it increases cyber attacks
17	Gregory M. Coates et. al., [17]	Active security test performed by software	Trust system is flexible and Secure network can be established for power grid	Digital certificates and digital signatures methods should be used to protect the RTU's, PLC's, and IED's from prevent unauthorized users
18	Donghyun Choi et. al., [18]	Key-management architecture	It supports information broadcasting and protects communications. Computational cost and the number of keys to be stored reduces in a Remote Terminal Unit (RTU).	Multi-cast communication process is less efficient
19	Igor Nai Fovino et. al., [19]	Analyzed the impact of conventional ICT malware on SCADA systems	Delivery of gas, oil or water in a pipeline can be block or reduced in case of hazard on SCADA system	The suggestion is to propose ad-hoc filtering and network monitoring with encryption and authentication to detect and mitigate anomalous behavior
20	Ten et. al., [20]	Attacks evaluation	System vulnerability measurement is quantified	Lack of information related to attack towards the power infrastructure

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.

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. It combines the asymmetric encryption and hash algorithm which provides data confidentiality and integrity. The large key size of 2048-bits is generated using asymmetric encryption which is not exists in the

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

previous work and it enables secure transmission and monitoring of process information through the internet.

V. Proposed Modified Asymmetric and Hash Algorithms

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. The large key size of 2048-bit is generated in the modified asymmetric algorithm. The hash algorithm is used which generates different hash value in order to ensure data integrity. The SHA (Secure Hash Algorithm)-512 generatesintermediate hash value using the message block as key.The block size is 1024-bits and the word size is 64-bits. The number of rounds is 80. The SHA-512 algorithm is highly secured than the MD5 algorithm.

5.1 Key Generation

5.1.1 Modified Asymmetric Algorithm

- Select two different prime numbers: m and n
- Calculate p=m*n
- Calculate r (p) = (m-1) (n-1)
- Select integer ‘f’ such that gcd(r(p)) = 1; 1< f < r(p)
- Calculate g, $g=f^{-1}(\mathrm{mod}(r(p))$
- Public key, PU = (f,p)
- Private key, PR = (g,p)

5.1.2 Encryption

- Original text: T
- Cipher text: $C=T^f \bmod p$

5.1.3 Decryption

- Original text: $T = C^g \bmod p$
  where f – Public key, g – Private key

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. Thehashing algorithm involves processing of hash function. 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. This task is continued for as more rounds as are required to hash the complete message. The hash algorithm protects the password storage and it is used to check the data integrity.

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 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 inputs which is called roundfunction. 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.

Fig. 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

$$H(i) = H(i-1)+C_M^{(i)} (H^{(i-1)})$$

Where C – Compression function

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

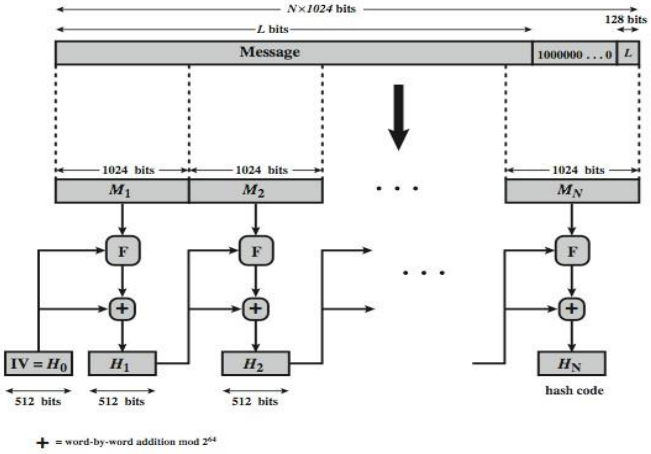

Fig. 1 SHA-512 for generation of Message Digest

Fig. 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.

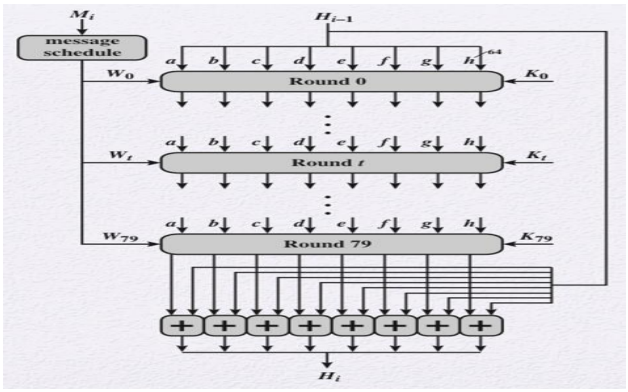

Fig. 2 Processing of SHA-512 Single 1024-bit Block

Fig. 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

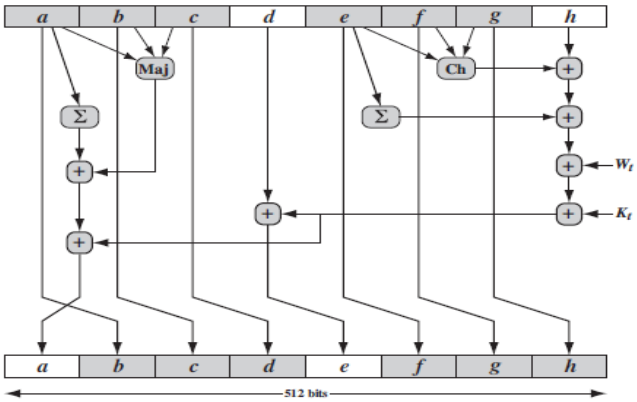

Fig. 3 SHA-512 Round Function

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
  - 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.

VI. FLOWCHART

The fig. 4 shows the flowchart of proposed encryption of process data. 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.

The fig. 5 shows the flowchart of proposed decryption of process data. The cipher text is received through the internet. The modified asymmetric decryption is performed using 2048-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.

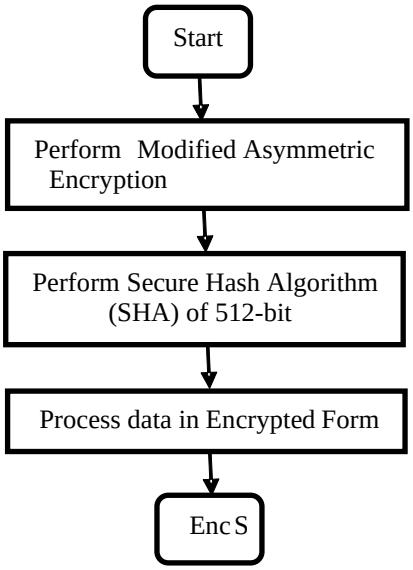

Fig. 4 Flowchart for Hybrid Encryption of Process data

This proposed work uses large key size of 2048-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 sensitive plant information in industrial applications.

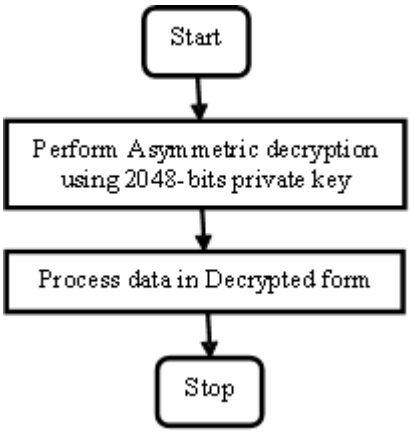

Fig. 5 Flowchart for Hybrid Decryption of Process data

Table 2 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 key size of 2048-bits. 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 3 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.

TABLE II COMPARISON BETWEEN STANDARD AND PROPOSED CRYPTOGRAPHIC ALGORITHMS

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

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)	2048-bits and 512-bits	214 bytes, 1024 bits	80	Fast	Highly Secure

TABLE III COMPARISON BETWEEN EXISTING AND PROPOSED CRYPTOGRAPHIC ALGORITHMS

Authors	Algorithm	Key size	Block size	Rounds	Security
VikasK.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 Asymmetric and Hash algorithm	RSA and SHA	2048-bits and 512-bits	214 bytes, 1024 bits	80	Highly Secure

VII. IMPLEMENTATION OF EMBEDDED BASED SECURE PROCESS MONITORING THROUGH SCADA SYSTEM

Fig. 6 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.

Fig. 7 shows the reception of process data in cipher text through internet. The decryption is

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

performed using embedded system and the original data in numerical form is monitored through SCADA master terminal unit.

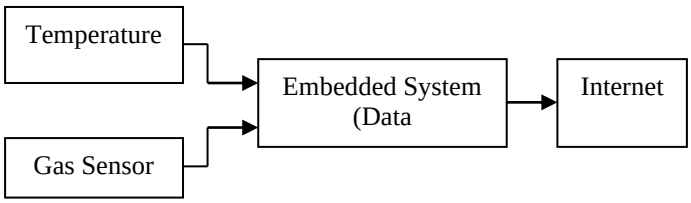

Fig.6 Transmission of Process data using Embedded System with Internet

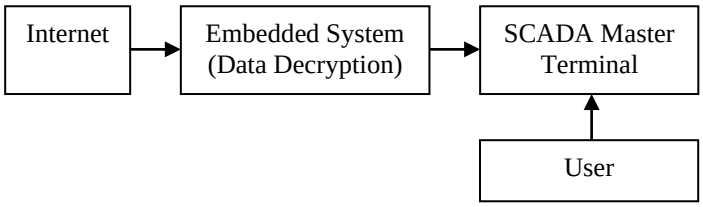

Fig. 7 Reception of Process data using SCADA System with Internet

VIII. Results and Discussion

This proposed modified asymmetric and a hash algorithm is performed using python. The modified asymmetric algorithm generates large key size of 2048-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.

Generation of Private Key and Public Key

The large key size of 2048-bit private key is generated from the modified asymmetric encryption whichstrengthens 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-----
MIIEpAIBAAKCAQEAms7TPybmkXuzbEGcfQsBuHu
2SigegjXbzlrS94ktXNevH40cpjEGEfUYxX3qoUwJXh
TSNb9TnoTRNdL6cgwhdByly07dEM7+sfK1Jw/lvLjsZ
QmYuoIWfJJAmNey55rD/oqkFV6wnpG5O97JJEHjCE
DqpqbcUoqmbPBBAUsP5yZcvAhK
JorhicPajBnN8ZOoYm6pv/1KmVBtNxY/edSKQFUsek
bbMvjgkpWcqaBbGsR62NWPErK58jUReJrPYI39u+97
yGEEu3Wm2zOXjAqmTX2+6Jb1cXC7lMzdZ/UOQRz
9Fw+BdHCIeJRMUktdjdQD4BNq5kub4tTAcqU2h6Ay
UQIDAQABAoIBAGPd5P0qdTeJG3hM
40zvWs7OUAyK0ROi9weqI8q4XeE06q5p8/9qRMY03
SQaVNB1It3khK9Tm/f5KpWUYyhLlxE2oeYEHCyJvF
jDgAWRBd23VhjgFfzLiwIVv0Jac/lhJ+r/OVbn3PyOeX
acBBo1vuZGKpoTrrI465//ZZAWAk5Uukb9h9CzHCiS
Qofbx68qXMK/bXuiWFFGRWSdOSN53eX3j/gm8+wv
WRwYBnahIhgoLIQd8mVwzSoimg4sQnAenep7y6a+0
znATQNU1boANn2vDyUHtKLIbLBI9fHAycWg3+nK
QAUBTFsxvPSBulAFalfHbSqLGGsuUW+pk1HiCKEC
gYEAxcXyor8Flys1Gd/lOGJPdsOitnlvecQgTZjKks+Hq
fferxketdvb0mG7Hiimmz75QN+8D6yHR/rl4rlKERTG
Mqm/5K6C+HQ5qUOHmneyWefRV+gKu1Zt1YcLSS
Y0Dpbn2LUqW6YHueBjJLPkBM7IyZGNtcn9niQPjda
8MvcP32UCgYEAyGKb
NrdrP4U8RlJIz6vbyo4F0viQh1ydNY6PgX/038y19dey+
mPk8MQh3nZFwvN0rpsSgcOqjSj/1avXETmlGNMhF
M2IfR5jnGW0oQMD8nRXfe0qheB2sEeVxlQlITIhP2
WAxDOelKff0iq4yJlC5Y0utpzIC5Xq8Rq8RcA4xn0Cg
YEAiFggHzyr4PyjnhPx1b5I5CqZOU1cocipMHW+ahn
ygCXm+jXKKzvIPzCrLG5/9ZUjhyr3XqLlnKUG6Rgu
TLpSrUjDhyccGacevWdVzBLq/PpJI15QT7iU/dkc2bA
hwVEdwxOagRZkSyu7jekKsJnSaMwUsxfu5aAcrP82P
bh/09UCgYEAtyAGILb2uBIWx10jVUYFktK/19F4o3u
r3+nsk7hQHMaD86uv0MvByZY0LY2Aq2y50We+PgC
GuIIjay2jWgaILmuj69L5TP6coa0AqbSLwuM3ock/9yD
u1qJU6e60D+Y0JC+qwaM65TeVgAey3v/Q9t9TNWeK
GaxkDPsV29iTCjECgYA0cNjdb/ifHRL0QMy3oJJjn3H
AFDwbpO1UN0CQ2SoVfob1Cy7byq2NTnfPjHjheeVm
LW6e3zMxHfezAJ42y3SNLHH5vVJkauecorZZMnVC
8iVla8v0D/Yv
ti8bkigt4YcQGWSpTE8Trdjfdr6gNOgrvVJrVHWvD4R
78ftZS7O+5A==

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

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

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
KCAQEAms7TPybmkXuzbEGcfQsBuHu2SigegjXbzlrS
94ktXNevH40cpjEGEfUYxX3qoUwJXhTSNb9TnoTR
NdL6cgwhdByly07dEM7+sfK1Jw/lvLjsZQmYuoIWfJJ
AmNey55rD/oqkFV6wnpG5O97JJEHjCEDqpqbcUoqm
bPBBAUsP5yZcvAhKJorhicPajBnN8ZOoYm6pv/1Km
VBtNxY/edSKQFUsekbbMvjgkpWcqaBbGsR62NWPE
rK58jUReJrPYI39u+97yGEEu3Wm2zOXjAqmTX2+6J
b1cXC7lMzdZ/UOQRz9Fw+BdHCIeJRMUktdjdQD4B
Nq5kub4tTAcqU2h6AyUQIDAQAB

-----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, obtainedfrom the fraction of cube roots of the first eighty primes, which are:

766A0ABB3C77B2A8A831C66D2DB43210
240CA1CC77AC9C6 E2748774CDF8E5D3
53380D139D95B3DF4CC5D4BECB3E42B6
923F82A4AF194F9B CA273ECEEA26619
391C0CB3C5C95A63243185BE4EE4B28C
550C7DC3D5FFB4E2983E5152EE66DFAB
72BE5D74F27B896F80DEB1FE3B1696B1
9BDC06A725C71235 C19BF174CF692694C
92722C851482353B6EFBE4786384F25E3A
B5C0FBCFEC4D3B2 A0FC19DC68B8CD5
B00327C898FB213FEADA7DD6CDE0EB165
CB0A9DCBD41FB D876F988DA831153
12835B0145706FBE2DE92C6F592B0275
BF597FC7BEEF0EE47137449123EF65CD2
C6E00BF33DA88FC2D5A79147930AA725
59F111F1B605D019 142929670A0E6E703
81C2C92E47EDAEE62E1B21385C26C926
19A4C116B8D2D0C8 4D2C6DFC5AC42AE
650A73548BAF63DE428A2F98D728AE22
E49B69C19EF14AD227B70A8546D22FFC
C24B8B70D0F89791A4506CEBDE82BDE9
C76C51A30654BE308CC702081A6439EC
4A7484AA6EA6E4835FCB6FAB3AD6FAE
CA2BFE8A14CF1036 CF40E35855771202
E9B5DBA58189DBBC3956C25BF348B538
F57D4F7FEE6ED178 4B0BCB5E19B48A
D807AA98A30302426C44198C4A475817
4C9EBE0A15C9BEBC 90BEFFFA23631E2
597F299CFC657E2AC67178F2E372532B
106AA07032BBD1B884C87814A1F0AB72C
28DB77F523047D841B710B35131C471B
78A5636F43172F604 2CAAB7B40C72493D7
AB1C5ED5DA6D81181E376C085141AB5
D186B8C721C0C207 6D192E819D6EF5218
06F067AA72176FBA0A637DC5A2C898A6
113F9804BEF90DAE A81A664BBC423001
682E6FF3D6B2B8A3BEF9A3F7B2C67915
431D67C49C100D4C5B9CCA4F7763E373
06CA6351E003826F748F82EE5DEFB2FC
4ED8AA4AE3418ACB 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.

IX. 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 2048-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

May – June 2020
ISSN: 0193-4120 Page No. 7431 - 7444

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 achieving process information security in any industrial applications.

REFERENCES

[1] VikasK.Soman, Natarajan V, "An Enhanced hybrid Data Security Algorithm for Cloud," IEEE International Conference on Networks and Advances in Computational Technologies, pp. 416-419, 2017.

[2] 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, pp. 349-355, 2017.

[3] M. Harini, K. PushpaGowri, C. Pavithra, M. PradhibaSelvarani, "A Novel Security Mechanism Using Hybrid Cryptography Algorithms," IEEE International Conference on Electrical, Instrumentation and Communication Engineering, 2017.

[4] 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, pp. 2985-2990, 2017.

[5] 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, pp. 3688-3693, 2016.

[6] Abdul mohsenAlmalawi, 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] AbdalhosseinRezai, ParvizKeshavarzi, Zahra Moravej, "Secure SCADA communication by using a Modified Key Management scheme," ISA Transactions, vol. 52, pp. 517-524, 2013.

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

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

[14] Igor NaiFovino, AlessioColetta, Andrea Carcano, Marcelo Masera. 2012. Critical State-BasedFiltering System for Securing SCADA Network Protocols. IEEE Transactions on Industrial Electronics, vol. 59(10), 3943-3950.

[15] 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.

[16] 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," Electrical Power and Energy Systems, vol. 33, pp. 1521-1526, 2011.

[17] 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.

[18] 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.

[19] 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.

[20] 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.