Real-Time Implementation for Secure monitoring of Wastewater Treatment Plants using Internet of Things

J.S. Prasath, S. Jayakumar, K. Karthikeyan

Abstract: ***The scarcity and demand of water increases rapidly. The varieties of wastewater treatment techniques are adopted to produce the quality water and recycling. Wastewater treatment is the process of removing the contaminants present and to produce it suitable for reuse as well as to save the environment. Water utility systems are susceptible to a variety of natural, infrastructure and man-made hazards. These threats result in contaminating the drinking water and affect the human health as well as environment. It is essential to ensure the smooth functioning of wastewater treatment process and to protect the water utility systems from security attacks. This proposed work is the real-time implementation of embedded system for secure monitoring of wastewater treatment process through the internet. The measure of Dissolved Oxygen (DO) content present in water is essential for marine organisms and fish to breathe. The measure of pH value indicates that the amount of chemicals dissolved in the water and whether organisms are affected by them. The High value of acidity can be deadly to fish and other marine organisms. In this proposed work, the presence of DO content and pH value is detected and sent to the embedded system. The content of dissolved oxygen and pH value is encrypted using embedded system and transmitted across wireless networks. The cipher text is decrypted at the receiver using embedded system. It protects the water security system from unauthorized access and modification of process parameters. It ensures good quality water produced and protects the environment as well as public health.***

Keywords: Encryption; Decryption; Industrial IoT; Embedded Systems; Wastewater Treatment.

I. INTRODUCTION

The water utility systems are used for municipal, industrial, agricultural, and household needs. The major sources of water are dams, reservoirs, sea, lakes, ground and surface. These waters are untreated and it is not suitable for usage. The sources of wastewater are industries, commercials, residents, sewage etc. It is necessary to recycle the wastewater by using suitable treatment process and to produce the good quality water.

The water security is a major issue in the wastewater treatment process. It is necessary to ensure the outcome of water treatment operation should be toxic free to save the environment. He was attempting to use the system to distribute malware. The possibility of terrorist attack takes place in these systems. The attack against water security system results in loss of environment, reduction in water quality etc. The water security issues are highlighted in terms of quality and quantity of water supply, and society requirements [1]. The requirements of water treatment process towards quality, quantity and society makes it more complexity in real-time implementation. Due to the continuous demand and scarcity of quality water supply, desalination technologies are adopted in various countries which make use of seawater and inland brackish waters.

Wastewater contains toxic substances, effluent from household, commercials, industries, institutions, hospitals etc. Sewage is a type of wastewater originating from kitchen sinks, cleaners, bathing, toilet and bathroom fixtures, laundry, public places etc. The security attacks in water utility systems are disrupting normal water treatment operations, attacks on process equipments, pumping stations, control systems etc. The chemical attacks would cause serious threat to output of entire plant. The contaminants and toxic chemicals may be added by the attacker which results in hazardous to public health and poisonous environment. The serious threat occurs due to the wastewater discharge into the environment.

Drinking water systems are susceptible to chemical and biological attacks. The intruders mix the toxic chemicals in the drinking water supply systems which are very harmful to human being. The drinking water also affected by the conditions surrounding the environment.

The internet is widely used in various industries for process monitoring and control functions. Internet of Things (IoT) is a growing technology in which a large number of objects which has ability to communicate information without manual operation. The control action has to be taken based on the sensor data and the command is given to implement these decisions. The security mechanisms to be focused for IoT are authentication and access control protocols. The advanced network protocols are essential to achieve the dynamics of IoT topology. The security concern need to be addressed for constrained and various network environment. Smart sensors used in Industrial Internet of Things (IIoT) enable precise control and monitoring of complicated processes. The IIoT has the potential for substantial improvements in manufacturing productivity. IIoT provides improvement in efficiency of operation through predictive maintenance and remote management. The various energy efficient mechanisms are addressed in IoT security services [2]. The energy saving mechanisms is applied to the deployment environment and the target

Revised Manuscript Received on October 15, 2019.

J.S. Prasath, Department of Electronics and Instrumentation Engineering, KCG College of Technology, Chennai, Tamilnadu, India.(Email: prasath.ei@kcgcollege.com)

Dr. S. Jayakumar, Department of Electronics and Instrumentation Engineering, KCG College of Technology, Chennai, Tamilnadu, India. Email: jayakumar.ei@kcgcollege.com).

K. Karthikeyan, Department of Electronics and Instrumentation Engineering, KCG College of Technology, Chennai, Tamilnadu, India.(Email: Karthikeyan.eee@kcgcollege.com).

protocol. The energy efficient services can be provided by low power security protocols. IIoT performs machine-to-machine communication and it ensures manufacturing of quality products. The major challenges in IIoT are security, adaptability, scalability, maintenance and flexibility.

The attackers can disturb the network by monitoring or altering the information of the process by intrusion. The intrusion detection system (IDS) can be utilized to supervise the vicious traffic in certain node and network to protect information systems. The trends, issues and future research of IDS for IoT are addressed [3]. The focus on research towards IoT is to investigate various sensing methods and strategy, to enhance the range of attack detection, to notify additional IoT technologies, to enhance authorizing policies, to revamp security of alert traffic. The plant operators should be responsible to take remedial measures against physical security for all components of the water utility.

II. SECURITY THREATS IN WASTEWATER TREATMENT PROCESS

Wastewater contains lot of toxic chemicals generated from the municipal sources including gray water, black water and yellow water. The major sources of wastewater are institutions, schools, hospitals, restaurants, farms, floodwater, industries etc. This wastewater consists of hazardous dissolved chemicals, sediments and suspended particles with variety of size.

The water utility systems are vulnerable to variety of threats including natural disasters, man-made attacks, and infrastructure threats. The security issues need to be addressed in order to protect the sensitive plant information from unauthorized access. The processed data should ensure security for the received information transmitted by the authorized users. The authorized users only can perform monitoring and control of process parameters.

Natural Disasters

It occurs from the natural hazards at different times in varying magnitudes. It is unexpected and various disasters recorded around the globe. In the year 2014, Ebola epidemic disaster happened in West Africa, whereas in the year 2010, earthquake occurred in Haiti. In the year 2008, Sichuan earthquake occurred in China whereas in the year 2005, hurricane Katrina and earthquake occurred in US and Pakistan respectively. In the year 2004, Tsunami was recorded in the Sumatra Island. Approximately 218 million people per year between 1994 and 2013 lost their life due to Natural disasters. It also affects the water utility systems by extended periods of freezing temperatures, tornadoes, lightning strikes, snow and ice storms, severe windstorms, and droughts.

Man-made Incidents

The malicious activities occur due to the intruder attack on the water utility systems and disturb the normal functioning of water treatment plant. The security threats due to man-made are cyber threats, chemical contamination threats and physical threats. The risk assessment strategy is essential to analyse the risk factors in different areas of water treatment systems.

Internal Threats

It occurs due to the employees, vendors, contractors working inside the organization. Insiders attack takes place on water systems causes serious threats to utilities. They have enough knowledge about the operation of wastewater treatment process. It is very difficult to identify the insider who initiates attack on water utility systems.

External Threats

It includes contamination of water distribution systems, contamination of wastewater, theft of components and equipments, physical attacks etc. Intruder targets the SCADA system and capture the process information, damage the operating system, access the on-line process data, and modifies the value of set point.

Cyber Threats

The urban water systems are susceptible to a variety of man-made and natural disasters. The main focus of water industry is cyber security. The cyber-attacks are the growing issue and the risk assessment should be made to protect the entire plant. Most of the water treatment plant operators are not familiar with SCADA and Information technology. The plant sensitive information may be modified by the unauthorized party to target the entire system operations. The periodical assessment is necessary to ensure the smooth functioning of water treatment process. The security mechanisms are considered depending upon the type of work performed by the IoT. The communication security in IoT can be achieved by incorporating lightweight security protocols for constrained environments. The cryptographic algorithm is used to protect the plant information from the attackers.

The cryptography is used for transforming the information from the IoT into an unreadable format in order to protect the process data from unauthorized access. The cryptographic algorithm is based on key generation, encryption and decryption. The single key is only required for symmetric encryption. The public and private keys are required for asymmetric encryption. A lightweight encryption algorithm is proposed to secure IoT in which the 64-bit block cipher is used for data encryption [4]. The algorithm is a combination of uniform substitution-permutation and a feistel network. The development of lightweight security algorithm keeps the computational complexity at moderate level in IoT environment.

III. VULNERABILITIES OF WATER UTILITY SYSTEM

Water infrastructure includes both the drinking water and wastewater industries. Water systems are vulnerable to possible attack which leads to physical damage of components and equipment's, unsafe environment, various public health hazards etc. Physical attack results in interruption of water treatment process and economic loss to industries. Chemical attack leads to water contaminates and produces harmful environment. Traditional methodologies of water treatment are suitable for discarding most

biological contaminants from the wastewater. The existing water treatment techniques may not produce high quality water but it contains contaminants especially pharmaceuticals and chemicals. The real time monitoring system is necessary to secure against the contamination of water sources. The water distribution system from the pipelines, pumps and storage tanks are susceptible to severe attacks because it is relatively unsecured and isolated.

The susceptibility of water utility SCADA systems are filling or emptying water tanks, turning pump on or off and software attacks. The vulnerability assessment method is proposed in a Geographical Information System [11]. It is based on parameters identification that has an effect on the behaviour of pipelines. Each parameter having a coefficient that represents its influence on the behaviour of the system, the product of these parameters represents the seismic susceptibility. It is essential to establish physical and procedural controls to restrict access to water utility systems. The major security concern in drinking water system is water contamination. The early warning systems are essential for to detect contamination in drinking water system. The plant managers and operators should have the knowledge about disposal and recycling wastages.

IV. SECURITY CHALLENGES IN WASTEWATER TREATMENT PLANTS

The major security challenges are to detect the presence of contaminants, testing of water quality, water turbidity, to detect the physical attacks etc. The risk assessment is the process of identifying, estimating and prioritizing risks to assets and operations. The existing risk assessment provides information about threats, attack probabilities, potential impacts etc. The current risk assessment approaches are ineffective for highly dynamic systems. The major challenge in the IoT is to ensure security and privacy in the constrained environment.

Confidentiality

The process information must be secured during transmission over wireless networks. Attackers can easily capture the information which is transmitted through the internet. The stored data inside the IoT device should be protected from the unauthorized access. The security algorithm is essential to protect the data and to avoid failure of process equipment's. The cryptographic algorithm can be used to convert the process data into unreadable format. The key size, security level, energy and time needed for execution of cryptographic algorithm is to be considered while used for secure process monitoring applications.

Integrity

The integrity ensures that the sensor data has not been modified or dropped during transmission over wireless networks. It is essential to secure the plant information and to safe the process equipment's from the attackers. The hash algorithm can be used to ensure the data integrity.

Availability

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

Authentication

The process information transmitted through the internet should be authenticated. The process data should be monitored and controlled only by the authorized users. It is associated with the place, mechanisms and elements that can be used to confirm the identification of the authorized parties.

Authorization

It is the mechanism of verifying that the plant operator has the authority to access the sensitive process information. The devices connected to the IoT must only be reprogrammed by the authorized users. The various solutions related to access control in IoT are highlighted [5]. The commonly used internet protocols cannot suit for constrained environments. The effective access control system should satisfy the security properties such as integrity, availability and confidentiality. It involves specifying the standard security practice, choosing model for access control and enforcing the access control protocols.

V. KEY MANAGEMENT SYSTEM

The key management is an important mechanism which protects the process data from the attackers. It is the process of managing the process information throughout the transmission from the sensor to the internet. The IoT data should be encrypted using suitable cryptographic algorithm to obtain the original data into unreadable format. The number of keys depending on the type of security algorithm used for securing IoT communications.

The algorithm used for protecting IoT data should be strong so as to ensure confidentiality and integrity. The security algorithm is proposed which provide end to end privacy for sharing the data [6]. The size of the key is increased to prevent the information from brute force attack. The constraints in the hybrid algorithm are cost, power and performance. This hybrid algorithm can be improved to provide higher security level between performance and memory usage.

VI. SECURITY CHALLENGES IN IOT

The security is an important concern in exchanging information between IoT devices. The major challenge in securing IoT is to identify theft, to secure the information, to authenticate the information and to secure the end devices. Data management is a major concern while routing the information form source to the destination. The large amount of information should be transferred from one place to another place in IoT. The routing challenges in IoT are dynamic routing topology, limited resource, scalability etc. The routing protocols should be flexible to deal with the

dynamics of IoT topology. The analysis of routing scheme and structure is performed to protect routing communications in IoT [7]. The security hazards in IoT are segregated into generic security hazards in IoT networks and specific security hazards. The standard secure routing algorithm is essential for IoT devices. The IoT networks have the ability to self-organize and serve without manual operations. The traditional IoT routing protocols lack appropriate security implementations.

The drawback of IoT is its limitation in resources such as processing power, energy supply, memory capacities, wireless communication range and bandwidth. The IoT will be large in scale in terms of number of nodes and geographically. IoT should have the ability to adapt to the modifications in the surroundings and to meet the future needs. IoT should have the provisions to increase the capacity of existing hardware or software be adding more resources to it.

The security mechanisms are essential to protect the devices which are internet enabled industrial wireless networks. The security algorithm is necessary to protect the resources that are used in IoT applications. The industrial IoT requires suitable cryptography to strengthen the sensitive plant data. The performance of cryptographic algorithms is assessed for various devices that can be used in IoT [8]. It is easy to implement the security algorithms such as symmetric ciphers and hash functions into the IoT services. These algorithms require only few milliseconds and can run on microcontrollers with RAM less than 1 Kilo-Byte. The symmetric algorithm can be used for end nodes to achieve end-to-end security.

The security risks in IoT can be reduced by choosing suitable encryption algorithm. The challenges in secure combination of sensor nodes with the internet are addressed with the focus on industrial environment [9]. The number of security issues related to threats and vulnerabilities increases due to the integration of internet in automation and control devices. The amount of energy consumption by the security algorithm is an important factor for battery-powered devices. The encrypted message from the transmitter will be sent to the receiver in secret and safely.

The challenges related to the distributed approach of the IoT are analysed [10]. It enhances the security mechanisms such as authentication, identity, access rights, security protocol etc. The IoT uses wireless communications which is vulnerable to number of attacks including Denial of Service (DoS), eavesdropping, masquerading, and saturation. The network related challenges in IoT are scalability, bandwidth, security and privacy. The modelling of security and technologies of securing IoT is addressed [12]. The various levels of security mechanism should be considered are system, communication, privacy, architecture, circuit, process and evaluation to reach higher security level in IoT systems. The number of security issues and privacy increases due to the wide usage of IoT in various environments.

VII. PROPOSED SECURITY ALGORITHM

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

Flowchart

The flowchart for the proposed security algorithm is shown in figure 1. The temperature and gas sensor data is taken as input. The key is essential to encrypt the sensor data. The symmetric encryption is performed to get cipher text for the sensor data. The hash algorithm (SHA 256) is used in this work to generate hash value for a given key. The key cannot be modified by the attackers during transmission and it ensures integrity of process information. The IP address is necessary to view the cipher text and key in hash form.

The proposed decryption algorithm is shown in figure 2. The cipher text is obtained by entering the IP address at the receiver. The symmetric decryption is performed for the received cipher text to obtain the sensor value in original plain data.

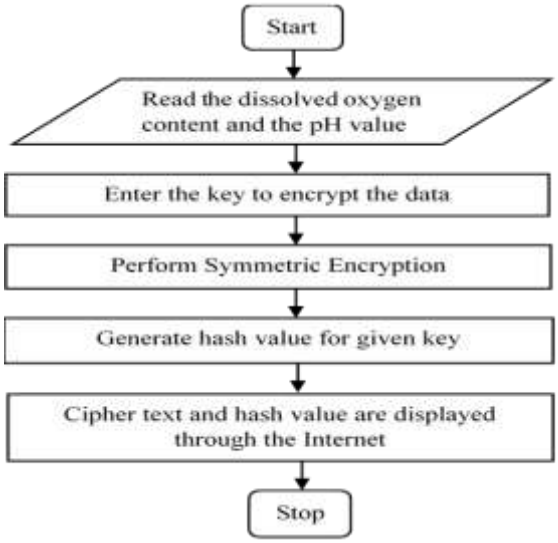

Fig. 1 Flowchart for proposed Encryption algorithm

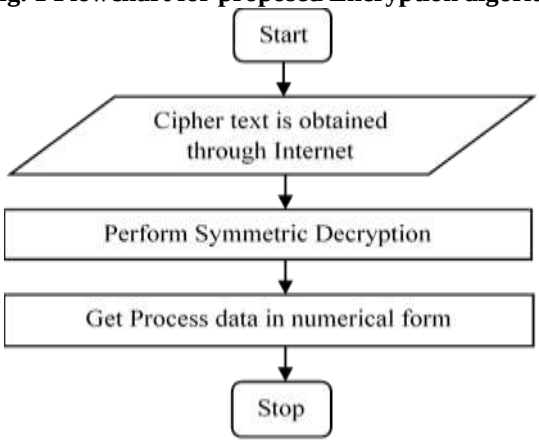

Fig. 2 Flowchart for proposed decryption algorithm

VIII. HARDWARE IMPLEMENTATION OF PROPOSED SECURITY ALGORITHM

This proposed security algorithm is implemented in embedded hardware with wireless transmission. The process data can be monitored through the internet both at the transmitter and at the receiver. The raspberry pi is used to perform encryption and decryption of proposed cryptographic algorithm. It has built-in Wi-Fi facility which enables wireless transmission of sensor data. The two nodes are used in which encryption is performed at the transmitter node and the decryption is performed at the receiver node.

The Dissolved Oxygen (DO) sensor is used to measure the contents of oxygen present in the wastewater. This measure of oxygen content is essential for aquatic organisms and fish to breathe. The quality water contains high level of DO content. The factors that affect the DO content in water includes temperature, water flow speed, plants and algae that produce oxygen, water pollution, the composition of stream present in the bottom etc.

The pH sensor provides the hydrogen ion concentration in the water. The value of pH indicates that it is acidic, alkaline or neutral. The value of pH varies from 0 to 14 and it indicates the acidic, basic or neutral solution. The potential is generated on the surface glass membrane by the pH electrode immersed in the solution. The pH value can be measured using electrochemical sensors which consist of a measuring and reference electrodes. The MCP3008 is a low cost eight channel 10-bit ADC. It is connected to the Raspberry Pi using a SPI serial connection. It reads the value of pH and DO content in analog form and converts it into equivalent digital form.

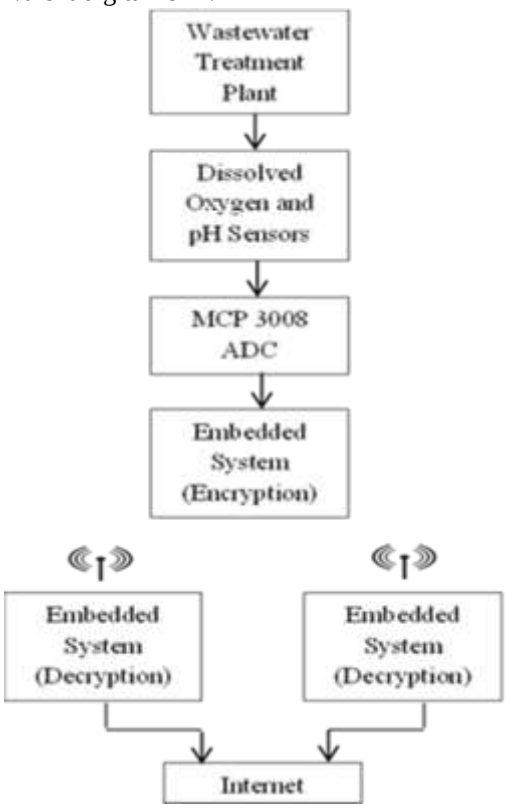

Fig. 3 Block Diagram of Embedded based secure monitoring of Chemical process using IoT

The transmitter node is a raspberry pi in which the encryption algorithm is written using python code. It produces the cipher text for the sensor data. The encrypted data is transmitted through Wi-Fi to the receiver node. The secure hash algorithm (SHA-256) is used to generate 256-bits hash value for a given key. The hash algorithm ensures data integrity while transmitting sensor data over wireless networks. The receiver node is another raspberry pi in which the decryption algorithm is performed to get the original sensor data from the encrypted data. The IP address is essential to monitor the sensor data in both transmitter and receiver side through the internet.

IX. RESULTS AND DISCUSSION

The symmetric algorithm used in this work produces the encrypted data for a given input data. It is performed with a fixed block size of 128-bits. It involves the sequence of operations which includes substitution of bytes, shifting of rows, mixing of columns and Add round key. The input data is encrypted through the 10 rounds of encryption. In addition, the SHA-256 hash algorithm is used in this proposed work which produces a digest length of 256 bits. It does not require key because it is not used for encryption. It generates hash value for a given input data. The symmetric and hash algorithms provide confidentiality, authentication and data integrity.

Pre-Processing

Padding

The padded data 'D' is to be created first and L its length in bits where L < 264, which is data D plus a right padding. An input data is processed with the block size of 512 bits and individual block performs 64 rounds of operations. The input data of up to 264 bit are transformed into digests of size 256 bits. The original data can be obtained by reading the last 64 for bits for length, and then fetching the message from left to right, of length L.

Blocks

The data D is parsed into N blocks of size 512 bits, D^1 to D^N, and each block is expressed as 16 input blocks of size 32 bits, D_0 to D_{15}.

The binary words of size 64 given by the 32 starting bits of the segmental parts of the cube roots of the first 64 prime numbers:

0x582A4F46 0x26845152 0x2B5C43DB 0x7A482E6C
0x84B4F39E 0x72B51C9C 0x71DF95A7 0x2B836D3F
0x6F4C394B 0x371F95B1 0x724D86A3 0x619FE47A
0x6D37C4A8 0x573F6B94 0x37856A7B 0xD63A7B4E
0x8F4B735D 0x7E549A3B 0x468D2B9E 0x93A7D526
0x5D8A4E9B 0x7B3976D4 0x38BE642A 0x489265E3
0x572E3B7C 0x37D3B57F 0x5D3B9A2F 0x4F3B8E43
0xc6e00bf3 0xC827A261 0x83F7A5C9 0x7136F5C2
0x6A3F94B1 0x7D3A9C6E 0x4D2AB574 0x7A6C48E3
0x37D2C364 0x72945D6A 0x4AB7F823 0x78246FA3
0xF581C6D4 0xC63F81E7 0xD4872A9B 0x8D5AC734
0x84D7A2B6 0x95A7F23D 0x7C34723A 0x5D3C638F

0x4C7234A6 0x825FAE62 0x629D5C83 0x48E28A5C 0x3F72D9B6 0x26D18A6B 0x2765F5AC 0x2F5D63A8 0x8E472D8F 0x4B376C2A 0x619FE47A 0xC6392B7E 0xF62C83D4 0xE847A5D2 0xD57A395E 0x6F3B2A84

Hash initialization

The initial hash value N0 of length 256 bits is set by considering the first 32 bits of the segmental parts of the square roots of the beginning eight prime numbers:

N0 = 7A09C778, N1 = CC67AD75, N2 = 7C4EB282, N3= 9D372A52, N4= 4C7629E4, N5 = 8F32B675A, N6 = 38B6825A, N7 = 5A62C8E2

This proposed hybrid security algorithm produces the cipher text and hash value to ensure confidentiality and data integrity across wireless networks. It protects the process parameters used for monitoring the operations of wastewater treatment plant. This proposed security algorithm is implemented in embedded system and monitoring the DO content and pH value through the internet. It enables process data transmitted across wireless medium and allows secure monitoring of plant operations in remote areas.

X. CONCLUSION

The water security is an important concern to ensure safe environment and drinking water purity. This proposed work is the real-time implementation of embedded security system for wastewater treatment plant. The amount of DO content and the pH value from the wastewater treatment process is encrypted using embedded system. This encrypted data is transmitted across the internet. The decryption is performed at the receiver using embedded system and the process data is monitored through the internet. This proposed security algorithm ensures confidentiality and integrity of process data during transmission over wireless networks. It allows secure monitoring of wastewater treatment process data through the internet. It provides cost-effective solutions in protecting the industrial equipment and authentic security for any industrial process to secure the sensitive plant information.

REFERENCES

1. Hess T.G.D., Hornberger, G.M., and Worland, S. (2019) 'Water Security in Practice: The quantity-quality-society nexus', Water Security, Vol. 6, pp. 1-6.
2. Hellaoui, H., Koudil M., and Bouabdallah, A. (2017) 'Energy-Efficient mechanisms in security of the Internet of Things: A Survey', Computer Networks, Vol. 127, pp. 173-189.
3. Zarpelao, B.B., Miani, R.S., Kawakani C.T., and Carlisto de Alvarenga, S. (2017) 'A Survey of Intrusion detection in Internet of Things', Journal of Network and Computer Applications, Vol. 84, pp. 25-37.
4. Usman, M., Ahmed, I., Aslam, M.I., Khan S., and Shah, U.A. (2017) 'SIT: A Lightweight Encryption Algorithm for Secure Internet of Things', International Journal of Advanced Computer Science and Applications, Vol. 8, pp. 1-10.
5. Ouaddah, A., Mousannif, H., Elkalama A.A., and Ouahman, A.A. (2017) 'Access control in the Internet of Things: Big challenges and new opportunities', Computer Networks, Vol. 112, pp. 237-262.
6. D. Aakash and P. Shanthi, (2016) 'Lightweight Security Algorithm for Wireless Node Connected with IoT', Indian Journal of Science and Technology, Vol. 9, pp. 1-8.
7. Airehrour, D., Gutierrez J., and Ray, S.K. (2016) 'Secure routing for Internet of Things: A Survey', Journal of Network and Computer Applications, Vol. 66, pp. 198-213.
8. Malina, L., Hajny, J., Fujdiak R., and Hosek, J. (2016) 'On perspective of Security and Privacy-preserving Solutions in the Internet of Things', Computer Networks, Vol. 102, pp. 83-95.
9. Alcaraz, C., Roman, R., Najera P., and Lopez, J. (2013) 'Security of Industrial Sensor Network-based remote substations in the context of the Internet of Things', Ad-Hoc Networks, Vol. 11, pp. 1091-1104.
10. Roman, R., Zhou J., and Lopez, J. (2013) 'On the features and challenges of Security and Privacy in distributed Internet of Things', Computer Networks, Vol. 57, pp. 2266-2279.
11. Zohraa, H.F., Mahmouda, B.,and Luc, D. (2012) 'Vulnerability Assessment of Water Supply Network', Energy Procedia, Vol. 18, pp. 772-783.
12. Jin-cui, Y.,and Bin-xing, F. (2011) 'Security model and Key technologies for the Internet of Things', The Journal of China Universities of Posts and Telecommunications, Vol. 18, pp. 109-112.

AUTHORS PROFILE

Mr. J S Prasath received M.E degree in Process Control and Instrumentation Engineering from Annamalai University, Chidambaram and pursuing Ph.D. in Wireless Sensor Networks for Industrial Security at Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as Assistant Professor in the Dept. of Electronics and Instrumentation Engineering at KCG College of Technology, Chennai, India. He is an interdisciplinary and guiding many Research projects at under graduate and post graduate level. Earlier he served as Assistant Professor in SRM University. His research interests are Embedded Systems, Wireless Sensor Networks, Process Control and Industrial Automation.

Dr. S. Jayakumar received the Ph.D degree in Information and communication engineering from Anna University, India in 2018. Currently he is working as Assistant Professor in the Dept. of Electronics and Instrumentation Engineering at KCG College of Technology, Chennai, India. His research includes VLSI design, Embedded Systems, Wireless Sensor Networks, Biomedical Engineering and Industrial Automation. He is the life member of IEI.

K. Karthikeyan received the M E. degree from Madras University in Applied electronics. Currently he is pursuing his PhD in Anna University. He is working in the area of Renewable energy optimization. His research interests include power electronics, DC-DC converters, Special Electrical Machines. He is the life member of ISTE.