International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 14, Issue 6 [June. 2025] PP: 115-120

Development of Novel Cryptography for Information Security

Dr. J.S.Prasath[1], Ms. Sushmitha G S[2], Ms. Swathi R[3]
[1]*Professor, Department of CSE, Sapthagiri NPS University, Bengaluru, India*
[2,3]*CSE Student, Department of CSE, Sapthagiri NPS University, Bengaluru, India*

ABSTRACT
Cryptography is essential to secure the sensitive information and to protect the confidential data from the unauthorized access. Data security is most important in information technology field, bank online transactions, industrial process, and to ensure privacy. This proposed work is the development of novel cryptography algorithm suitable for encryption of text messages. This proposed security algorithm is easy to implement and produces the cipher text in binary values. The benefit of this proposed algorithm is it produces large number of bits as cipher text during encryption for a smaller text input. The cipher text can be transmitted across internet to ensure data confidentiality. The decryption is performed at the receiver to obtain the original text. The benefit of this proposed novel cryptography is simple, easy to understand, and it ensures data confidentiality over internet. This proposed novel cryptography can perform string encryption, numerical data encryption, floating point encryption, binary data encryption, octal data encryption, hexadecimal data encryption, and special characters encryption. This proposed security algorithm can be used for encryption of password, industrial process information, money transaction details, electronic mail messages, medical data, and text messages.
Keywords: *Cryptography, Encryption, Decryption, Data Security, String*

Date of submission: 01-06-2025 Date of acceptance: 10-06-2025

I. INTRODUCTION

Data security is essential during transmission and monitoring across internet. Due to the internet is an open nature, any parties can access the sensitive process data, modify the data and re-transmit to the destination. This leads to abnormal plant operations and results in failure of process devices. The security algorithms are essential to protect the plant information and to safeguard the process equipment against unauthorized access and modification. Cryptography is the widely used technology in securing the plant parameters. The continuous varying process data can be converted into unreadable cipher text before transmission over internet. This conversion of process data into cipher text is performed through encryption. The cipher text ensures data confidentiality across internet. The cipher text at the receiver is converted back into original process data through decryption. Cryptography involves sequence of operations to convert input raw data into unreadable cipher text. Cryptographic algorithms are utilized to assure confidentiality, and authentication of sensitive process data. The key is essential to perform encryption and decryption. The number of keys required depends on the types of cryptography. Symmetric Cryptography utilizes single key to perform both encryption and decryption. Asymmetric Cryptography uses public key for data encryption and private key for data decryption. The objectives, concerns and solutions for industrial Wireless Sensor Networks (WSN) are presented [8]. The present standards and protocols are discussed. The various constraints in WSN limit the performance in industrial operations.

Industrial Internet of Things (IIoT) has the potential for usage in the production industries. IIoT is highly accurate and efficient in performing plant operations through predictive maintenance and collecting the status of continuous varying process parameters. The various energy efficient techniques to ensure data security over internet is discussed [9]. The security issues in IoT devices and simulation techniques are used for vulnerability assessment of cyber security. The various needs of IoT configuration for cyber security is proposed [10]. The security of smart home is evaluated using Small World platform. Attackers target the network by monitoring or altering the plant data. The hardware device is implemented that can detect the Denial of Service (DoS) attack by monitoring the electrical signals in the circuit [7]. The issues and future research areas of Intrusion Detection System (IDS) across internet is addressed [11]. The study on research is related to different IDS mechanisms for internet based data transmission, to raise the limit of attack detection, to address several IoT technologies, to improve evaluation methods, to produce communication traffic warning system and to enhance the security management.The one-way security gateway system is proposed to guarantee the security and reliability of transmitted information[17]. The security problems should be considered in order to protect the process data from unauthorized access. A location privacy preservation technique is proposed that satisfies differential privacy issue

to protect location data privacy and extends the usage of data and algorithm in Industrial IoT[5]. The difficult work is the protection of data from unauthorized access and security of communication medium. A public key encryption called Cramer–Shoup encryption technique is proposed with shorter ciphertexts[15]. The security is based on plain decisional Diffie–Hellman (DDH) assumption.It is necessary to propose strong security algorithm and key management schemes. The different security threats and vulnerabilities of IoTare addressed [12]. The universal IoT security architecture can be implemented to ensure security in IoT applications. The energy efficient security architecture is proposed for wireless based industrial automation systems [20]. The packet protection based on encryption consumes energy in the case of battery powered devices. The architecture level attacks include physical, software, side channel, logical, timing and power analysis. A self-organizing approach is proposed which detects the abnormal behavior of program [21]. The malicious code can be introduced remotelythrough the network in the code injection attacks. A cost effective method is proposed for protecting embedded software against passive side channel attacks [23]. The protocols are vulnerable to software attacks and could result in a malevolent behavior such as unknown destination, packet replay or deadlock. The attacks on IoT include hardware, software, and networks. The lightweight hash function is proposed which reduce complication in terms of hardware implementation and standard security can be achieved [16]. The lightweight hash function is essential for constrained devices include wireless sensors and embedded systems. The various access control solutions in IoT are highlighted [14]. The commonly used internet protocols cannot suit for constrained environments. A key management mechanism is proposed that combines the random seed distribution with transitory master key mechanisms [24]. The nodes are unable to establish new keys after the specific time period and it is suitable for static networks. The key management mechanisms 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[22]. The key size is increased to prevent the information from brute force attack. The challenges related to the need of energy efficiency, real-time performance, coexistence, interoperability, and security and privacy are addressed [6]. The symmetric algorithm is capable to provide a lightweight solution for IIoT devices. The routing algorithms and protocols are necessary to ensure the secure transmission of messages. The protocols and mechanisms related to secure routing in IoT are analyzed [19]. The standard secure routing algorithm is essential for IoT devices. The hardware security mechanism is proposed along with the hybrid cryptography algorithm which provides authentication and data confidentiality of process information [2]. It is the cost-effective method and achieves high level of security in monitoring the sensitive plant information across internet. The IoT networks have the ability to self-organize and serve without manual operations. The features and challenges of the distributed approach of the IoT are analyzed [25]. The distributed approach increases the complexity of security mechanisms. IoT utilizes wireless communications which is susceptible to variety of attacks including Denial of Service (DoS), man-in-middle, eavesdropping, masquerading, and saturation. A fast and accurate intrusion detection mechanism is designed to detect the distributed denial-of-service (DDoS) attacks [1]. An enhanced ResNet architecture is proposed for feature extraction which brings out deeper features from given traffic traces. The composite security algorithm is proposed and implemented in real-time to ensure process data security [3]. It utilizes 128-bit key size to perform encryption along with the hash algorithm to assure data integrity.

The major security issues in IIoT are physical devices attacks, eavesdropping of process information by the intruders, illegitimate monitoring of plant parameters, and refusing of process information to authorized users. The various existing protocols for ensuring security and communications in IoT are addressed [18]. The protocols utilized for IoT are IEEE 802.15.4 which is low-energy communications used at the physical layer and Medium Access Control (MAC) layer, 6LoWPAN adaptation layer which allows transmission of IPv6 packets over IEEE 802.15.4, IPv6 Network routing and Constrained Application Protocol (CoAP), which supports communications at the application layer. The network related issues in IoT are scalability, bandwidth, security and privacy. The security issues for distributed industrial control systems are addressed [26]. The various security features considered are architecture level, terminal level for security validation in order to attain high level of security in IoT systems. A multi-dimensional analysis scheme is developed for cryptographic algorithms in terms of speed, power, and unit energy cost [27]. The experimental result and analysis predict that the plain text size is not linear with the energy consumptions and time overheads of cryptographic algorithms. The problems in secure integration of sensor nodes with the internet are addressed with the focus on industrial environment [28]. The number of security challenges related to threats and vulnerabilities rises due to the combination of internet in automation and control devices. The issues related to the distributed approach of the IoT are analyzed [29]. It improves the security schemes such as authentication, identity, access rights, security protocol etc. The general security framework is essential with consideration of majority of attacks and to ensure secure process data transmission and provides safety to plant equipment.

The advanced form of block cipher encryption is proposed, which is Cipher Block Chaining (CBC) mode that gives extra complexity to the encrypted data. The countermeasure technique is proposed which are based on fault space transformation to protect AES-128 bits against biased fault attacks [13]. The fault collision based

attacks are prevented. Each block of plain text is XORed with the previous cipher text block prior to encryption and then the result is encrypted with the key. The advantage of CBC mode is it generates different cipher text for identical input data by modifying the initialization vector. The combination of symmetric and secure hash algorithm is proposed for monitoring the process data in the wastewater treatment plants using IoT [4]. The dissolved oxygen and the pH value is encrypted and monitored through IoT.

II. Proposed Cryptography

Proposed Encryption Algorithm

Step 1: Get the input string
Step 2: Find the equivalent ASCII value for the given string
Step 3: Convert the given ASCII value to Gray code
Step 4: Find the 2's complement from the resultant Gray code
Step 5: Divide the resultant 2's complement by 2
Step 6: Square the quotient value to obtain the cipher text

The flowchart of the proposed encryption algorithm is shown in figure 1. The input is the string which is converted into cipher text. This input string is converted into equivalent ASCII value. The gray code is computed from the ASCII value. The 2's complement value is to be computed from the obtained gray code. This resultant 2's complement output is divided by two. After the division, the quotient is to be squared to obtain the cipher text.

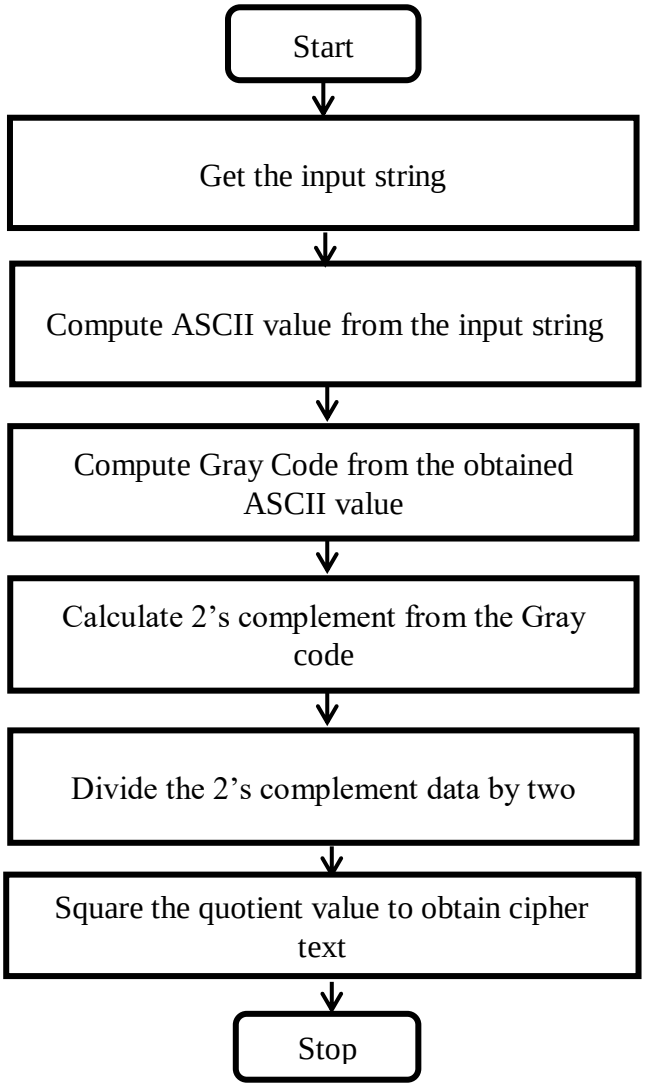

Figure 1 Flowchart of the proposed Encryption algorithm

Proposed Decryption Algorithm
Step 1: Convert the cipher text into equivalent decimal value
Step 2: Find square root of decimal value
Step 3: Multiply the resultant value by 2
Step 4: Find the 2's complement of the product
Step 5: Find equivalent Gray code from the resultant 2's complement
Step 6: Convert Gray code to equivalent ASCII value
Step 7: Convert the ASCII value to equivalent string to obtain the original text

The flowchart of the proposed decryption algorithm is shown in figure 2. The cipher text obtained at the receiver is converted into equivalent decimal value. Compute the square root of this decimal value. The result obtained from the square root is multiplied by two. Compute the 2's complement of the product and the gray code is to be generated from the resultant 2's complement. Then the equivalent ASCII value is computed from the obtained gray code. The original text is obtained by converting the ASCII value into equivalent alphabets.

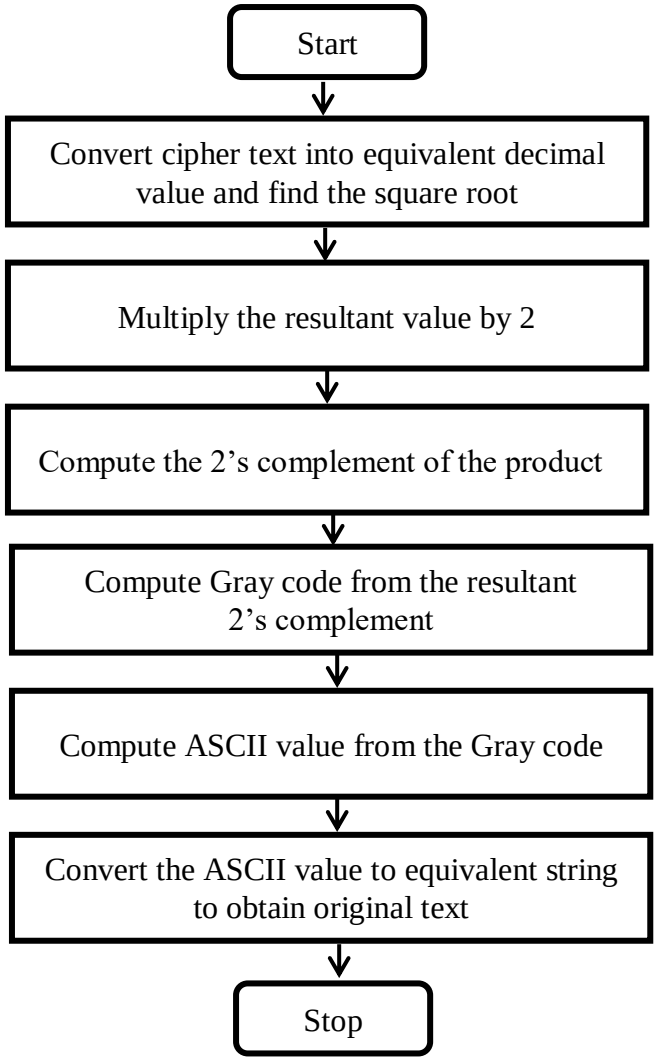

Figure 2 Flowchart of the proposed Decryption algorithm

III. Results and Discussion

This proposed cryptography takes the input string and converts it into cipher text. This proposed novel cryptography is encrypted and decrypted using Python code. Figure 3 shows the Python output that reads the input string "cryptography" and generates the cipher text. This cipher text is decrypted and produced the original string. This cipher text can be transmitted across internet to ensure data

confidentiality. The decryption is performed at the receiver to obtain the original string from the cipher text.

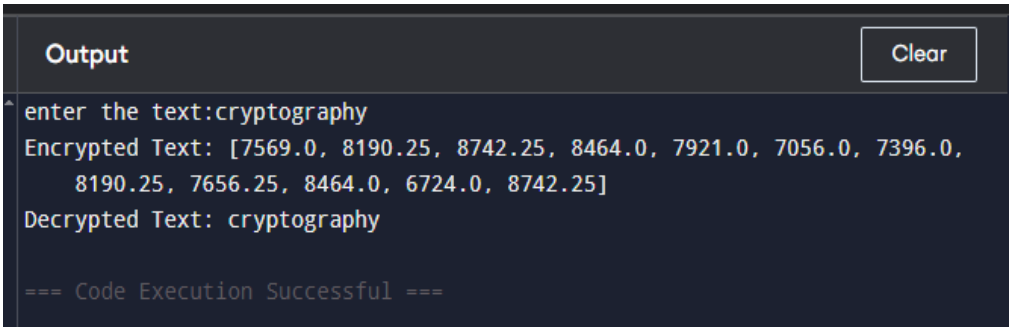

Figure 3 Python Output for the Proposed String Encryption

This proposed novel cryptography is simple and suitable for string encryption. This work can be used to secure the text messages, email messages, whatsapp messages, and official confidential information. Figure 4 shows the Python output that reads the input numerical data and produces the cipher text. This cipher text is decrypted and obtained the original numerical data.

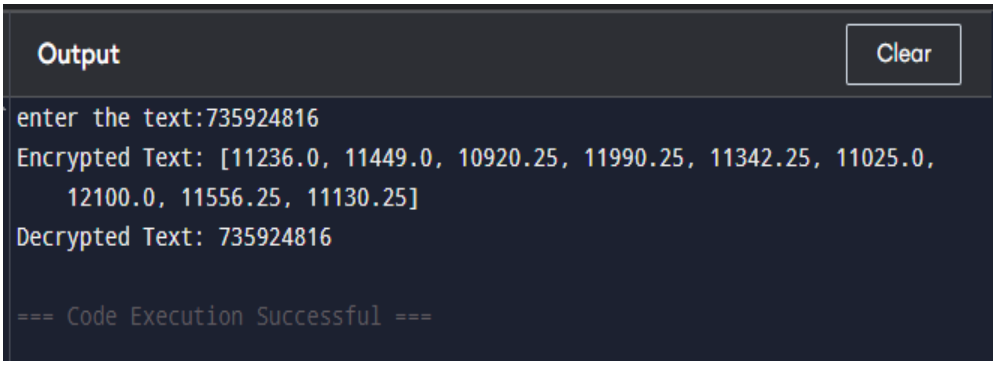

Figure 4 Python Output for the Proposed Numerical Data Encryption and Decryption

This proposed novel cryptography is suitable for string encryption, numerical data encryption, floating point encryption, binary data encryption, octal data encryption, hexadecimal data encryption, and special characters encryption.

IV. Conclusion

The novel cryptography is developed in this work for text encryption. This proposed security algorithm reads the input string, performs series of operations to get the cipher text. The cipher text produces in binary values for the input string. The number of bits produced in cipher text is large for a smaller string. When the input string contains more number of characters, then the cipher text produced from this proposed cryptography becomes thousands of bits. This large number of bits produced as cipher text strengthening the level of security. The decryption is the reverse operation of encryption performed to obtain the original string from the cipher text. This proposed security algorithm is simple procedure, easy to implement, and used for securing the password, process data, bank account holder information, online transactions, and border information.

References

[1]. J.S.Prasath, V.Irine Shyja, P.Chandrakanth, B. Kiran Kumar, A. Raja Basha, "An optimal secure defense mechanism for DDoS attack in IoT network using feature optimization and intrusion detection system," *Journal of Intelligent & Fuzzy Systems*, vol. 46, no. 3, pp. 6517-6534, 2024.

[2]. J.S.Prasath, U.Ramachandraiah, G.Muthukumaran, "Modified Hardware Security Algorithms for Process Industries using Internet of Things," *Journal of Applied Security Research*, vol. 16, No. 1, pp. 127-140, 2020.

[3]. 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.

[4]. J.S.Prasath, S. Jayakumar, K.Karthikeyan, "Real-Time Implementation for Secure monitoring of Wastewater Treatment Plants usingInternet of Things," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 2997-3002,

2019.
[5]. Y. Chunyong,Jinwen Xi, Ruxia Sun, Jin Wang, "Location Privacy Protection based on Differential Privacy Strategy for Big Data in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 8, pp. 3628-3636, 2018.
[6]. S. Emiliano, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 11, pp. 4724-4734, 2018.
[7]. R. Jinnai, A. Inomata, I. Arai, K. Fujikawa, "Proposal of Hardware Device Model for IoT End Point Security and its Implementation," *IEEE International Conference on Pervasive Computing and Communications,* USA, 2017.
[8]. M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, N. Muhammad Khan, "A Critical Analysis of Research Potential, Challenges and Future Directives in Industrial Wireless Sensor Networks," *IEEE Communications Surveys and Tutorials,* vol. 20, no. 1, pp. 1-60, 2017.
[9]. H.Hellaoui,M.Koudi,A.Bouabdallah,"Energy-efficientmechanisms in security of the Internet of Things: A Survey," *Computer Networks,* vol. 127, pp 173-189, 2017.
[10]. A. Furfaro, L. Argento, A.Parise, A. Piccolo, "Using virtual environments for the assessment of cyber security issues in IoT scenarios," *Simulation Modeling Practice and Theory,* vol. 73, pp 43-54, 2017.
[11]. B. Bogaz Zarpelao, R. Sanches Miani, C. Toshio Kawakani, S. Carlisto de Alvarenga,"A Survey of Intrusion detection in Internet of Things," *Journal of Network and Computer Applications,* vol. 84, pp. 25-37, 2017.
[12]. F.Ayotunde Alaba, M.Othman, I. Abaker Targio Hashem, F.Alotaibi, "Internet of Things Security: A Survey," *Journal of Network and Computer Applications,* vol. 88, pp. 10-28, 2017.
[13]. Sikhar Patranabis, Abhishek Chakraborty, Debdeep Mukhopadhyay,P.P. Chakrabarti, "Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-like Block Ciphers," *IEEE Transactions on Information Forensics and Security,* vol. 12, no. 5, pp. 1-11, 2017.
[14]. A. Ouaddah,H. Mousannif, A. Abou Elkalam, A. Ait Ouahman, "Access control in the Internet of Things: Big challenges and New Opportunities," *Computer Networks,* vol. 112, pp. 237-262, 2017.
[15]. M.Abdalla, F.Benhamouda, D.Pointcheval, "Public-key Encryption indistinguishable under Plaintext-Checkable attacks," *IET Information Security,* vol. 10, no. 6, pp. 288-303, 2016.
[16]. P. Megha Mukundan, S. Manayankath, C. Srinivasan, M. Sethumadhavan, "Hash-One: A Lightweight Cryptographic Hash function," *IET Information Security,* vol. 10, no. 5, pp. 225-231, 2016.
[17]. Y. Heo, B. Kim, D.Kang, J.Na, "A Design of Unidirectional Security Gateway for Enforcement Reliability and Security of Transmission Data in Industrial Control Systems," *IEEE International Conference on Advanced Communications Technology,* South Korea, pp. 310-313, 2016.
[18]. D. Aakash, P.Shanthi, "Lightweight Security Algorithm for Wireless Node connected with IoT," *Indian Journal of Science and Technology,* vol. 9, pp. 1-8, 2016.
[19]. A. David, J. Gutierrez, S. Kumar Ray, "Secure routing for Internet of things: A Survey," *Journal of Network and Computer Applications,* vol. 66, pp. 198-213, 2016.
[20]. R. Muradore, D. Quaglia,"Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," *IEEE Transactions on Industrial Informatics,* vol. 11, pp. 830-840, 2015.
[21]. X.Zhai, K.Appiah, S.Ehsan, G.Howells, H.Hu, G.Dongbing, K.D. McDonald-Maier, "A Method for Detecting Abnormal Program Behavior on Embedded Devices," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 8, pp. 1692-1704, 2015.
[22]. J. Granjal, E.Monteiro, J. Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communication Surveys and Tutorials,* vol. 17, pp. 1294-1312, 2015.
[23]. G. Agosta, A. Barenghi, G. Pelosi, M.Scandale, "The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 34, no. 8, pp. 1320-1333, 2015.
[24]. F.Gandino, B.Montrucchio, M.Rebaudengo, "Key Management for Static Wireless Sensor Networks With Node Adding," *IEEE Transactions on Industrial Informatics,* vol. 10, no. 2, pp. 1133-1143, 2014.
[25]. R. Roman, J.Zhou, J.Lopez, "On the features and challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks,* vol. 57, pp. 2266-2279, 2013.
[26]. M.Cheminod, L.Durante, A.Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics,* vol. 9, no. 1, pp. 277–293, 2013.
[27]. W. Jiang, G.Zhenlin, M.Yue, N.Sang, "Measurement-based Research on Cryptographic Algorithms for Embedded Real-Time Systems," *Journal of Systems Architecture,* vol. 59, pp. 1394-1404, 2013.
[28]. C.Alcaraz, R.Roman, P.Najera, J.Lopez, "Security of Industrial Sensor Network-based Remote Substations in the Context of the Internet of Things," *Ad- Hoc Networks,* vol. 11, pp. 1091-1104, 2013.
[29]. R.Roman, Z. Jianying, J.Lopez, "On the features and challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks,* vol. 57, pp. 2266-2279, 2013.

AUTHOR BIOGRAPHY

Dr. J.S.Prasath received Master of Engineering degree in Process Control and Instrumentation Engineering from Annamalai University, Chidambaram and Doctor of Philosophy degree in Wireless Sensor Networks for Industrial Security from Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as Professor in the Department of Computer Science and Engineering, Sapthagiri NPS University, Bengaluru, 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, Hindustan University, KCG College of Technology and Narayana

Engineering College. His research interests are Embedded Systems, Wireless Sensor Networks, Internet of Things, Process Control and Industrial Automation. He has published twenty articles in International Journals, presented twenty papers in International Conference, published two patents, written two books and two book chapters.

Ms. Sushmitha G S is currently pursuing her Bachelor of Engineering degree in Computer Science and Engineering from Sapthagiri NPS University, Bengaluru, India. She is an aspiring researcher with a strong interest in Artificial Intelligence, the Internet of Things (IoT), and Web Technologies. She is committed to deepening her technical knowledge and actively engages in workshops and seminars to enhance her skills. Her goal is to contribute innovative solutions to real-world problems through her research in emerging technologies.

Ms. Swathi R is currently pursuing her Bachelor of Engineering degree in Computer Science and Engineering from Sapthagiri NPS University, Bengaluru, India. With a strong curiosity and enthusiasm for emerging technologies, She has developed a keen interest in areas such as Artificial Intelligence, Machine Learning, Web development, and the Internet of Things. Her academic journey is fuelled by continuous learning, experimentation, and a commitment to contribute meaningfully to the technology world. She looks forward to deepening her expertise and sharing more insightful contributions in the upcoming years.