International Journal of Electrical and Computer Engineering (IJECE)
Vol.10, No.1, February 2020, pp. 387~395
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp387-395

A reliable next generation cyber security architecture for industrial internet of things environment

C. Vijayakumaran[1], B. Muthusenthil[2], B. Manickavasagam[3]
[1,3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, India
[2]Department of Computer Science and Engineering, Valliammai Engineering College, India

Article Info

Article history:

Received Feb 17, 2019
Revised Aug 29, 2019
Accepted Aug 30, 2019

Keywords:

Cyber-defense authentication mechanism
Cyber security architecture
Industrial IoT
Industry 4.0
Internet of things
Real-time critical information
Virtual gateway system

ABSTRACT

Architectural changes are happening in the modern industries due to the adaption and the deployment of 'Internet of Things (IoT)' for monitoring and controlling various devices remotely from the external world. The most predominant place where the IoT technology makes the most sense is the industrial automation processes in smart industries (Industry 4.0). In this paper, a reliable 'Next Generation Cyber Security Architecture (NCSA)' is presented for Industrial IoT (IIoT) environment that detects and thwarts cybersecurity threats and vulnerabilities. It helps to automate the processes of exchanging real-time critical information between devices without any human intervention. It proposes an analytical framework that can be used to protect entities and network traffics involved in the IIoT wireless communication. It incorporates an automated cyber-defense authentication mechanism that detects and prevents security attacks when a network session has been established. The defense mechanism accomplishes the required level of security protection in the network by generating an identity token which is cryptographically encrypted and verified by a virtual gateway system. The proposed NCSA improves security in the IIoT environment and reduces operational management cost.

Corresponding Author:

C. Vijayakumaran,
Department of Computer Science and Engineering,
SRM Institute of Science and Technology,
SRM Nagar, Kattankuluthur, Kanchipuram District, Tamilnadu, 6020, India.
Email: kumar1612@yahoo.com

1. INTRODUCTION

The proliferation of embedded devices in the modern industrial sector has provided many kinds of solutions for the industrial automation processes. The emergence of the Internet of Things (IoT) technology paves a way to connect these devices wirelessly with the internet [1]. The most prevalent place in which the IoT technology makes the most sense is the industry automation in smart industries (Industry 4.0) and it is also called as Industrial IoT (IIoT) [2, 3]. It is expected that nearly 45 billion IoT devices will be in use in 2023 [4]. The smart industries use thousands of smart sensors and devices in their automation processes which control different aspects of the manufacturing process ranging from automation of production line to protection and safety of the operating environment. The legacy devices have been upgraded with smart sensors which provide more functionality, intelligence, and connectedness between devices. By enabling industries with IoT technology, the manufacturers can considerably reduce the operating and maintenance cost of their industrial equipment. It also helpsto reduce errors, improve safety and efficiency in the manufacturing process. However, security attacks make failures in the automation processes. Industries can use cyber-physical systems to monitor their physical processes through different administrative divisions and make critical decisions from the collected data. Data collected and stored in the central repository are

more susceptible to various security attacks and can choke the entire automation processes. For instance, data interception in the communication channel can exploit the data integrity of the system.

The characteristics of a smart industry include interoperability, data integrity, transparency in information sharing, technical assistance and decentralized decision making. In order to provide secure access to industrial automation processes, the Supervisory Control and Data Acquisition (SCADA) system [5] is mainly used as an Industrial Control System (ICS) in the IIoT environment. The main role of the SCADA system is to feed the real-time system performance data into higher level IT support systems for decision-making processes. The general architecture of the SCADA system is shown in Figure 1. It provides instant access to real-time information for making data-driven decisions in order to improve efficiency, performance, customer experience and control industrial processes remotely. However, strategic plans for securing the IoT devices have not been kept up with the rapid development and innovations happening in IIoT sectors which enables many new challenges in the cybersecurity landscape [6]. The integration of IoT with the existing SCADA system in the industry environment can introduce many kinds of security risks to the system.

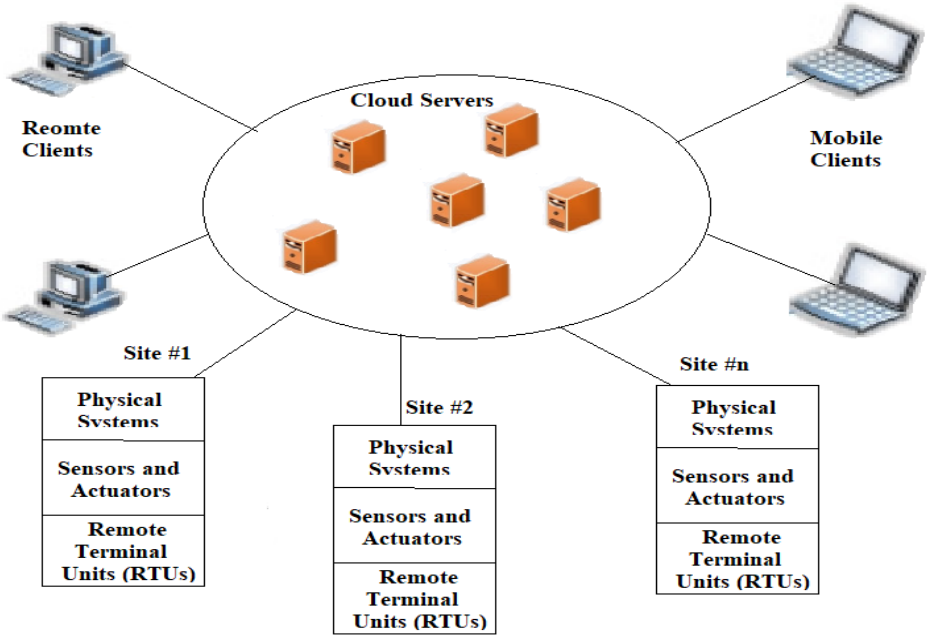


Figure 1. The architecture of the SCADA system in the Industrial IoT (IIoT) environment

The IIoT environment needs low-cost smart sensors that should be reliable, easily deployable and configurable. It should exhibit application-level interoperability and fault tolerance capabilities under communication impairments. It should also provide scalability, security and privacy requirements to its users. In order to provide effective security control mechanism in the IIoT landscape, many authentication mechanisms have been proposed [7, 8]. However, the limited computational power of devices and low bandwidth of communication channels prevents those mechanisms directly applied to the IIoT sector. In this paper, a reliable next-generation cyber security architecture is proposed to authenticate entities involved in wireless communication. It ensures the integrity of the real-time critical information exchanged between those entities in the IIoT network.

a. Cyber security challenges in the IIoT landscape

There is a multitude of cybersecurity threats emerging in the information era that are mainly targeting organizations and industries at large. The IIoT network environment is shown in Figure 2. Many cybersecurity challenges [9] and solutions [10, 11] have been addressed in this environment to mitigate security vulnerabilities and threats. Without having a well-designed security infrastructure for any IIoT deployments, an organization should encounter a considerable amount of damages to its assets and reputation over time. This section discusses different kinds of security attacks and major cybersecurity challenges needed to envisage a security framework for the IIoT environment [12].

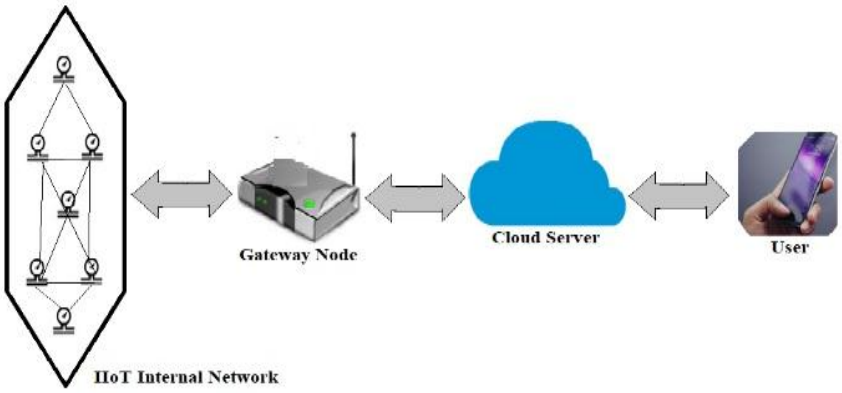


Figure 2. The IIoT network environment

b. Different security attacks in IIoT network

Most of the critical infrastructure is vulnerable to security attacks. The classification of different security attacks in the IIoT network landscape are categorized as follows:

Attacks on Physical Components: Attacks on physical components of IIoT require unauthorized access to sensing devices, control systems and actuators [13]. Hackers have various options at their disposal to intercept the radio signals and clone it to extract the security credentials which cause significant damage to critical infrastructure in the industrial control systems.

Attacks on Software Components: Attackers injects various kinds of malware such as Viruses, Trojans, and Worms to see how they react in the system. The distributed denial of service (DDoS) attacks can disturb the regular operation of the systems under control. For an instance, in IIoT sector, attack on the safety-critical information such as warning of a broken gas pipeline can be done through the DDoS attacks [14] to suppress the warning messages that can go unnoticed. Each update of the software must be signed (verified) before flashing into a device to accomplish authenticity.

Attacks on Network Components: Wireless connectivity between devices facilitates remote access. However, it is also the biggest vulnerable point in the IIoT network from which the attackers can exploit the whole network components remotely. Intruders can initiate possible attacks on the nodes connected to the wireless network. In fact, a cloud infrastructure could be used to control the networked IoT devices connected through a gateway [15]. Thus, if the gateway node has been compromised by an attacker, the whole IIoT system can be down and becomes critical. Each end-to-end session can be encrypted at the end-points to avoid security threats in the network. The lack of well-established business processes, mature technologies, and proliferation of different device standards create complexities in the IIoT sector which in turn, makes it difficult to tackle all kinds of security attacks [16]. Thus a well-established cybersecurity solution is essential to secure the IIoT landscape.

c. Security requirements for IIoT landscape

Any framework envisaged for IIoT environment should meet the following security requirements:

1. Security: It provides assurance to the user of a system that all components used in the system are well protected and remain secure from outside threats and attacks that try to compromise the system. It also assures that the confidentiality and integrity of the system will remain intact and the information will not be disclosed at any cost to any unauthorized entity. It assures the availability of the system to its authorized user and enables instantaneous access to the information.
2. Privacy: It is the ability of the system under control that provides controlled access to its information flow within the organizational setup.
3. Reliability: It is the ability of a system that should perform its required functions under stated conditions within the specified period
4. Safety: It is the most important requirement for any IIoT sectors that provides an amicable working condition at which the user of the system should not pose any potential threat of danger. It should safeguard both people and physical assets in the working environment.
5. Resilience: It provides fault-tolerance capabilities to the system when a failure occurs. The system should accomplish its functions through meaningful alternative ways when it encounters some failures. If a single component of the system has encountered a failure, it would not affect other parts. The system should automatically overcome with that failure

The nodes of the network in the IIoT landscape are interfaced with a cloud-based management system (integration of SCADA with web-based cloud system through a gateway) for performing various analytics and decisions making processes. The communication entities use TCP/IP protocol stack for wireless transmission of data between them which is much more susceptible to security threats than its wired counterpart. The security breach impacts on data loss and it can extend into the areas of human and physical risks. Thus, it is essential to have a security solution that should address the various issues related to the security and privacy of the data shared between entities involved in the IIoT sectors [17, 18].

The main objective of this research paper is to present a scalable and reliable security system architecture named as "NextGen Cyber Security Architecture (NCSA) for IIoT Applications" that protects the real-time data traffics generated from various IoT devices and to the data stored in the cloud server system. It provides the required level of security to the system by enabling a suitable authentication mechanism and by enforcing necessary policy management in the proposed security framework. The proposed framework tries to address the following key questions:

a. Does the existing configuration of cloud infrastructure of the IIoT application intact? In general, redundancy in device deployment is followed in the IIoT sector. The system hence collects redundant, dynamic and heterogeneous data and stores them in its cloud. The collected raw data should be cleaned and formatted for performing various analytical processes. Thus, the proposed framework ensures the data integrity and privacy requirements of the organization through a suitable authentication mechanism.
b. Is it scalable for new devices introduced in the existing network environment? Scalability is essential in the IIoT environment, either new devices are introduced at any time to the existing network or failure devices can be removed for diagnosing a fault. The proposed cybersecurity framework supports scalability by means of device identity tag.
c. What are the security and privacy policies enforced when the cloud infrastructure was hacked? Data confidentiality should be maintained within the IIoT network. Privacy-preserving policies are used and employed in the proposed scheme to address these security issues in the cloud infrastructure of IIoT.
d. Are the legacy technologies sufficient? If not, do we need any further enhancement to meet the additional requirements of new applications? The proposed NCSA describes well-defined key capabilities of IIoT security platform that includes various aspects of integrating cybersecurity schemes in the existing infrastructure without affecting the operational characteristics of the legacy systems to avoid various kinds of cybersecurity threats.

The rest of the paper is organized as follows. The proposed NextGen Cyber Security Architecture (NCSA) is described in Section 2. The security analysis for the proposed NCSA is given in Section 3 and the performance analysis of the NCSA is given in Section 4. Finally, Section 5 concludes this research work.

2. THE NEXTGEN CYBER SECURITY ARCHITECTURE (NCSA) FOR IIoT ENVIRONMENT

Many efforts have been taken by researchers in the field of IIoT to provide protection mechanisms and cybersecurity frameworks for IIoT applications. In this section, the system level security framework for IIoT landscape is presented.

a. The system architecture

The daunting task in wireless network communication environment is to detect and thwart security-related threats. The security frameworks designed for mitigating security vulnerabilities in IIoT sectors is neither automated nor integrated. For instance, it is difficult to automate the updating of signatures in signature-based security solutions to detect polymorphic attacks. A better solution can be achieved through an automated cyber defense mechanism that can provide necessary protection approaches for various threats in a wireless environment. The components of the proposed NextGen cyber security architecture (NCSA) is shown in Figure 3.

It has two perceptible features that enhance the existing cyber defense mechanism and network security. At first, it provides scalability that the system can scale from a few nodes to a large volume of data nodes in the IIoT communication network. A new client node can become a member by generating an authentication token which is cryptographically signed. The identity of the token (client) is verified by an administrator node. The gateway node authenticates each session established between the IoT devices and the cloud server. It allows only authenticated traffic in the network through a table look-up mechanism which reduces computational overheads occurred in complex network control packets. A dynamic and adaptive trust mechanism can be easily integrated with existing security solutions to provide cyber defense solutions that scale well. The trust mechanism enforces a well-established business rule (Policy Management) to protect the network resources.

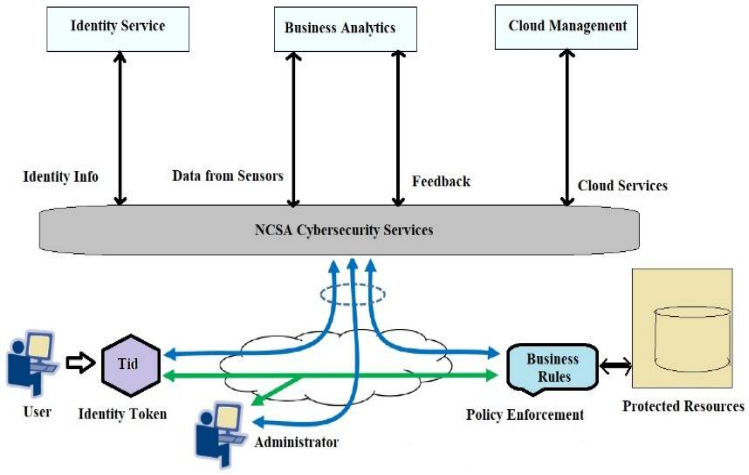


Figure 3. The nextgen cyber security architecture (NCSA) for an IIoT landscape

The second major capability of the proposed system is to provide a real-time detection and prevention mechanism for system security that addresses different kinds of security attacks induced when a session is established. An access control (AC) mechanism preloaded in the administrator authenticates a network packet at each session establishment process in advance so that only legitimate node will be allowed to transfer packets with other entities in the wireless environment. The attackers outside of the network cannot see the protected resources since the access control mechanism restricts the unauthenticated requests from the outside world. The access controller achieves this restricted access to data traffic through an encrypted security token that can be inserted in each session.

b. Data-level security in the NCSA

Each device is assigned with a unique identity (n_i) in the pre-deployment phase. A public key (K_r) and a secret key (K_a) is also assigned for each node in the IIoT network. A shared session key (K_s) is generated during a network session established between neighboring nodes which ensures the security in the data exchanged between those neighbors. Hence, the attacker cannot eavesdrop security information in the data transmission process. Similarly, the intruders cannot perform node forgery attack by introducing some malicious nodes in the network. Because they cannot generate a session key with the required level of identities for the malicious node. For instance, let us consider a node in the IIoT network sends the monitored information in the form of data packets to the central repository (Cloud Servers) system. A malicious node in the communication path unable to decipher the content of the packet, since it was encrypted by the negotiated session key along with the public and secret keys of that node. A public key encryption algorithm such as RSA is used to encrypt the packet transmitted between a source node and a destination node. Only the intended recipient can decipher the received packets. An efficient key-management protocol [19-21] is used to generate and manage the keys in the proposed system. There are many challenges exist in the cyber security management for IIoT [22].

In the cloud server side, the proposed framework enforces the secure information storage policies in order to preserve the integrity of stored data [23-25]. The data are stored in the encrypted format and cannot be decrypted without knowing the secret key of the end user. As per the pre-defined rules given in the policy, the received packets can be decrypted using the same algorithm used for encrypting the packets. In addition to these capabilities, NCSA provides necessary APIs required to identify network management processes, privacy-preserving policies, and various interfaces needed for smooth operation of the whole network in a controlled manner. With the integration of all the mechanisms, a reliable automated cyber security architecture can be envisaged in an IIoT landscape.

c. Securing the network traffic through IIoT gateway node

The most valuable entity in the IIoT network is the smart sensors that have different calibration capabilities within the specific level of tolerance to provide a required data fidelity. They generate different kinds of information with the varying degree of tolerance, however, the receiving end may use a data analytics system that can apply a pre-defined tolerance level (threshold) to each sensor measurements in order to provide real-time responses to the user. When such sensors are deployed in time bounded IIoT

landscape, they must be physically secured to prevent unnecessary relocation or deletion from the network. Each sensor has a unique identity that can be encrypted and verified for authentication purpose.

The basic capability of the gateway system is to bridge all devices in the internal network to the external world (Internet) through a wireless local network interface. It monitors all the network traffic and controls them to identify unexpected and unwanted content in network communication. It can achieve the required level of defense using several methods such as:

1) By effectively isolating unauthorized external network traffic from reaching the IIoT devices, the gateway prevents the external threats that are aimed to manipulate the device behavior
2) Compromised devices are prevented from being used to attack other entities in either internal or external network. For example, a DDoS attack or transmission of sensitive data to other internet-based systems.

The next major function of the gateway system is to identify and authenticate each device in the internal network. Only authorized devices with enact integrity can participate in network operations. The gateway should promptly identify, authorize and authenticate devices connected in the network and it should also verify the integrity of the software installed or updated in the devices.Finally, the applications and gateway interfaces must also be well secured through a virtual private network (VPN) which prevents manipulation of system messages, eavesdropping, network error, and data corruption.

3. SECURITY ANALYSIS

This section analyzes the security of the proposed authentication mechanism as follows:

a. Proposition 1. The identity of the IIoT devices is secured by the proposed authentication mechanism

Proof: The identity of the devices used in the IIoT network is protected by generating a unique authentication token which is cryptographically encrypted using a strong public key cryptographic algorithm such as SHA. Therefore, the attacker cannot obtain the identity of the devices without compromising the security keys generated during the encryption and decryption processes.

b. Proportion 2. It preserves the confidentiality of the information exchanged in the IIoT landscape

Proof: The confidentiality of the information is secured by using a hash value of a random number generated when s session has been established in the communication process. Therefore, the adversary cannot intercept a communication session without knowing the randomly generated hash value of the identity token.

c. Proportion 3. Mutual authentication between devices and gateway involved in the communication is achieved through the proposed authentication mechanism

Proof: While receiving a join request message from a new device or messages to be sent to devices, the gateway node checks the identity token, hash value and the random number generated for the device. The message is considered to be genuine only when equality holds good. The same verification process is carried out in the device side to authenticate the gateway node when it received a message from the gateway node. Hence, the aim of an attacker to fake a device or the gateway node is prevented since he needs to generate the valid combination of the authentication token which is very difficult to achieve. Moreover, he cannot assume the random number generated in the mutual authentication process.

d. Proportion 4.Impersonation attack is prevented in the network by the proposed authentication mechanism

Proof: The proposed authentication mechanism guarantees the user that a packet transmitted between nodes cannot be modified by the attacker without knowing the hash values used in the mutual authentication process involved in the establishment of a secure communication session. The tampered message send by the attacker can easily be detected by checking the hash values at the node itself. Hence, the impersonation attack can be prevented in the network.

4. PERFORMANCE ANALYSIS

The performance of the proposed NCSA is analyzed in this section. The performance of NCSA is evaluated through a simulation experimental setup as given in Table 1. A prototype of the NCSA is created and deployed to monitor certain parameters (like temperature and pressure) in the IIoT landscape. The performance of the prototype is tested in terms of the amount of data securely transmitted, time-synchronization, data retrieval capability and volume of storage required in the server side.

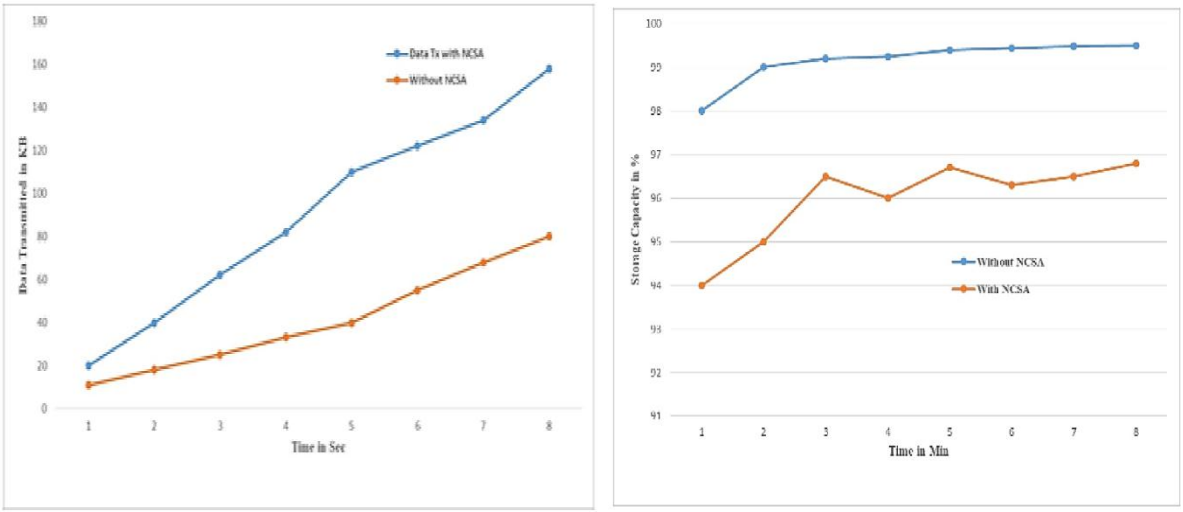
Table 1. Experimental setup

Sl. No	Parameters	Values
1	No. of nodes (devices)	9
2	Wireless communication	ZigBee and WirelessLAN
3	Connection to Cloud Server	Internet
4	Cloud Server	An Intel desktop server with 8GB RAM and 1TB storage capacity
5	Data fusion	Indirect, decentralized
6	Sensing Time Interval	100ms
7	Monitoring parameters	Temperature and Pressure
8	Gateway Node	A laptop with 4GB RAM and 500 MB storage capacity

The wireless communication between nodes in the IIoT network is achieved through the ZigBee (IEEE 802.15.4) technology. The temperature and pressure sensors are mounted in the internal nodes. The external cloud server is responsible for collecting, storing and processing the data received from these nodes. The nodes are transmitting the sensed data to the cloud server through an intermediate gateway node. It is assumed that the temperature and pressure values are measured every 100ms and these values are directly sent to the gateway node. It collects this information from those 9 devices and performs an estimation of local temperature and pressure at the deployed location in the IIoT environment. The estimated information is sent to the cloud server every 10 min for further processing. As presented in Figure 4, the proposed NCSA considerably reduces both the data transmission overheads and storage space occupied by the data in the cloud storage system external to the IIoT network.

Therefore, the cloud server has to occupy more storage space to store data in the cloud storage system without the NCSA framework. The data transmission overhead occurs within the internal networks in the IIoT environment due to the header portion of data packets. There is always a trade-off between the data transmission time and the data processing time in any wireless network environment. Time efficiency can be achieved through suitable time synchronization mechanism. In the case of NCSA, time-stamp mechanism is used to achieve the synchronization between various network elements during the data transmission process.

To secure IIoT environment, more research works are needed in the future. Because the security frameworks for IIoT integrated with cloud computing are at the early stages of development. More attention is needed in preventing cybersecurity-related attacks on the IIoT environment. Cloud-based solutions provide a more efficient and optimized usage of computing resources. The future landscape may utilize data science and big data frameworks that are expected to have a large impact on the IIoT sector.



(a) (b)

Figure 4. (a) The size of data transmitted to the cloud, (b) The percentage of storage space allotted for data

5. CONCLUSION

The paper presents anext-generation cyber security architecture for Industrial IoT (IIoT) environment. The paper has highlighted the importance of critical infrastructure in industrial systems such as SCADA and various cybersecurity-related attacks. The proposed system provides a reliable, automated, cybersecurity framework for Industrial IoT that can monitors and controls its overall operation remotely.

It provides authentication to all devices used in the system and achieves the same by using cryptographically secured keys. An automated cyber-defense mechanism integrated with the authentication system is presented to achieve the required level of security and reduces operational and maintenance cost considerably. The gateway acts as a defense point between the external internet and internal network in the IIoT network. It filters unwanted traffics thereby it prevents various security threats entering into the IIoT landscape. The performance analysis of the proposed system showed that there is a considerable amount of reduction in the storage space required in the cloud server and transmission overheads in the IIoT network environment.

ACKNOWLEDGMENTS

This research was supported by the management of SRM Institute of Science and Technology. We thank our Director and Head of the department, Computer Science and Engineering from SRMIST who provided insight and expertise that greatly assisted us to successfully complete this research paper.

REFERENCES

[1] L. Atzori, *et al*., "The Internet of Things: A survey,"*Computer Networks*, vol. 54, pp. 2787-2805, 2010.
[2] S. Mumtaz, *et al*., "Massive internet of things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," *IEEE Industrial Electronics Magazine*, vol. 11, pp. 28-33, 2017.
[3] L. D. Xu, *et al*., "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, pp. 2233-2243, 2014.
[4] V. Gandhi, "Security Essentials for IoT Deployments and in Connected Spaces," *White Paper from Frost and Sullivan*, 2017.
[5] K. Stouffer, *et al*., "Guide to Industrial Control System (ICS) Security," *NIST Special Publication*, Revision 2, U.S. Department of Commerce, 2015.
[6] A. Kott, *et al*., "Six Potential Game-Changers in Cyber Security," *NATO Symposium on Cyber Security Science and Engineering*, vol. 47, pp. 104-106, 2014.
[7] X. Yao, *et al*., "A lightweight multi-cast authentication mechanism for small scale IoT applications," *IEEE Sensors Journal*, vol. 13, pp. 3693-3701, 2013.
[8] W. L. Chin, *et al*., "A framework of Machine-to-Machine authentication in smart grid: A two-layer approach," *IEEE Communications Magazine*, vol. 54, pp. 102-107, 2016.
[9] K. Alexander, "Towards fundamental science of cybersecurity,"*Springer Journal on Network Science and Cybersecurity*, pp. 1-13, 2013.
[10] A. Patcha and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *IEEE transaction on Computer Networks*, vol. 51, pp. 3448-3470, 2007.
[11] Hitachi Ltd., "An anomaly detection system for advanced maintenance," *Hitachi Review*, vol. 63, 2014.
[12] World Economic Forum, "Industrial Internet of Things Safety and Security Digital Protocol Network," *Center for the Fourth Industrial Revolution*, 2016.
[13] D. Welch and S. Lathrop, "Wireless security threat taxonomy," *Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society*, pp. 76-83, 2003.
[14] C. Kolias, *et al*., "DDoS in IoT: Mirai and Other Botnets,"*IEEE Journal on Computer*,vol.50, pp. 80-84, 2017.
[15] M. Henze, *et al*., "A comprehensive approach to privacy in the cloud-based Internet of Things,"*Future Generation Computer Systems*, vol. 56, pp. 701- 718, 2016.
[16] H. Kawai, *et al*., "Access Authentication – Providing Flexible and Secure Network Access," *NEC Technical Journal*, vol. 8, 2014.
[17] K. Alexopoulos, *et al*., "Architecture and development of an Industrial Internet of Things framework for realizing services in Industrial Product Service Systems," *CIRP Conference on Manufacturing Systems*, pp. 880-885, 2018.
[18] R. Chetan and R. Shahabadka, "A Comprehensive Survey on Exiting Solution Approaches towards Security and Privacy Requirements of IoT," *International Journal of Electrical and Computer Engineering (IJECE)*, vol.8, pp. 2319-2326,2018.
[19] Y. BenSlimane and K. Ben Ahmed, "Efficient End-to-End Secure Key Management Protocol for Internet of Things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol.7, pp. 3622-361, 2017.
[20] J. Metan and K.N. N. Murthy, "FSDA: Framework for Secure Data Aggregation in Wireless Sensor Network for Enhancing Key Management,"*International Journal of Electrical and Computer Engineering (IJECE)*, vol.8, pp. 4684-4692,2018.
[21] S.V. Manikanthan and T.Padmapriya, "A Secured Multi-Level Key Management Technique for Intensified Wireless Sensor Network,"*International Journal of Recent Technology and Engineering*, vol. 7, 2019.
[22] Maximilian L*, Markl E and Mohamed A. "Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities," *Journal of Information Technology & Software Engineering*, vol. 8, 2018.
[23] Sahmim S, and Gharsellaoui H,"Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review,"*Procedia Computer Science*, Vol. 112, pp.1516-1522, 2017.
[24] HughBoyes, BilHallaq, JoeCunningham and TimWatson,"The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, Vol. 101, pp.1-12, 2018.

[25] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, and T. Eschert,"Industrial internet of things and cyber manufacturing systems," *Industrial Internet of Things, Springer*, pp. 3-19, 2017.

BIOGRAPHIES OF AUTHORS

Chellavelu Vijayakumaran is currently working as an Associate Professor in the department of Computer Science and Engineering at SRM Institute of Science and Technology, KTR Campus. He has completed his B.E degree in Computer Science &Engineering from Madras University, M.Tech. Degree from SRM IST (Deemed University) and P.hD from AISECT University, Bhopal. His research interests include Network Security, Mobile Adhoc Networks (MANETs), Artificial Intelligent, Virtual Reality, Data Science and Big Data Analytics. He has serverd as invited reviewer for many conferences and journals. He was invited as guest speaker in a foreign university. Further details can be found at http://www.srmuniv.ac.in/engineering/computer-science/faculty/dr-vijayakumaran-c.

Muthusenthil Balasubramanian received his B.E degree in Electronics & Communication Engineering from Madras University, in 1996 Masters Degree from Satyabama University in 2007, Doctorate from Anna University, Chennai 2016. He was working as a Research Scientist in Wookyoung Information technology, Daegu, Southkorea. Now, he is working as an Associate Professor at Valliammai Engineering College, Chennai. His interests are in mobile ad-hoc networks, network security, video security, network attacks, privacy preservation, trust evaluation and cloud computing. He is affiliated with scientific publications, he has served as invited reviewer. Further info on his homepage: http://www.srmvalliammai.ac.in

Manickavasagam Balasubramanian, a member of IEEE. He got his Diploma in Computer Technology in 2008 from Pattukkottai Polytechnic College, bachelor of Engineering from Apollo engineering College, affliated to Anna University, and Master of Technology from SRM University. Currently, he is pursuing Doctor of Philosophy, in the domain of Software Defined Wireless Body Area Network. His research interests are Software Defined Network, Network Security, Sensor Networks, and Internet Of Things. Mail ID: bmanickavasagam90@gmail.com