AUTOMATION OF INDUSTRIAL (IOT) AND CYBER SECURITY

Santi Priyanka Prem [1], V.V.S.S.S.Balaram[2], Sunil Bhutada [3]

[1]Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, Email: priyankapremsanti@gmail.com
[2]Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, Email: vadrevu_kinnera@yahoo.com
[3]Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, Email: sunilb@sreenidhi.edu.in

Abstract: In our everyday lives, it could be easy to gain personal information or know the information of the individual business network community in order to allow cyber security attacks in our country to collapse and lose control. Cyber attacks are limitless in the IT field or in companies of the network. As a matter of fact, many business industries use IoT that is used to link and pass data from one computer to another that is called MACHINE TO MACHINE communication while the transfer of data cyber security threats are transferred so that the attacker can access and track the data. We have suggested industrial automation using IoT by including cyber security in this article. The key aim of this paper is to allow data protection through the use of IoT in industries and to share or transfer protected messages.

Keywords: Internet of things, Cyber Security, communication links, M2M

I. INTRODUCTION

As we see, technology has been quickly evolving and is being used by companies to safeguard and protect information or data. Cyber security plays an important role in the structure of industrial automation and control. The destruction of companies or any company would be vast if the cyber intruder hacks the device. The industrial automation and control system is an environment in which the IoT is known to each other for the sharing of knowledge to minimize manual labour, i.e. the internet of things that has various aids in the current technologies that supports processes and management of self-governing coordination among the systems. The real-time data is gathered as the vast volume of these unifiedcorporeal hardware units could be recycled for new intellectual technologies to develop. Several challenges will emerge as modern intellectual applications are processed to include security and data safety, and usability and functionality to satisfy the new technology environment for particular sector specifications of industrial automation and control systems.

Constantly mesmerizing is factory robotics. The modern intellectual infrastructure has transformed the world of the internet, the programming and solutions used by the industrial control system to run cloud-based systems by involving the internet unswerving or circuitously. Many customer centred online websites are transitioning to cloud-centric technologies. The network of the Industrial Control System results in tremendous robberies, there are several industries using data storage and transfer computing that can be exploited and many tragedies that can have a personal and professional effect. The protection offered by the Industrial Control System is used to protect the data against misfortunes or deliberate risk. The security monitoring over the Industrial Control System is restricted such that the information is lost and that the hacker or the attackers may use the data inappropriately to use the property or private data. The relation loss mechanisms of the native devices would become a risk for information disruption, interruptions in the production and manufacturing phase, circulation failure and harmful effects of the associated units. In this project, we provide data protection and secure data sharing from one gateway to another that takes place from the server to the client.

II. LITERATURE REVIEW

In this section of the article, the key reviews in the industrial control system arena and the protection offered for industrial automation are reviewed and analyzed. Earlier computers were built to perform various tasks [2]. For automation purposes, every industry in the world uses machines to minimize the workload that is performed manually, the applications are managed and supervised by humans. Industrial automation is achieved in the past by intellectual technology such as Bluetooth and radio frequency, which are used only for short distance to communicate and monitor the data [6] [10]. With the aid of sensors and cameras, the circumstances encountered by industrial automation is tracked to minimize the workload

for human adoption of the Internet of Things in factories to track and advise the responsible authority to take the necessary steps that could take some time to damage the assets and it is a time-taken process [5][9].

Industrial automation was then further upgraded to the IoT, but companies are facing several security issues [3]. The Industrial Control System cyberprotection sequence reveals that security accidents during device contact are more likely to be vulnerable to data exploitation [7]. Monitoring and security of the movement of data or information from one computer to another machine are the key features of this paper [8]. Safety is an important consideration for the data analytics and computation of Information Management Systems [1]. It could trigger great price to subordinate with the ruptures in real-time to provide protection. In industrial control systems, the complexity of modern malware threats without attacks has been difficult because of the avoidance and detection of cyber attacks [4]. We will address the problems posed in the next portion of the paper and how to include the security and transmission of data.

III. CHALLENGES IN THE INDUSTRIAL AUTOMATION

Excess types of industrial control systems are covered by industrial automation. Industrial automation is carried out for the implementation of the application information in several different domains, (i) the construction of the commodity that is carried out in a step-by-step phase i.e. stage by stage, e.g., food processing industries, pharmaceutical industries, etc. (ii) the continuous production process carried out without any interruption, e.g. (iii) different forms of manufacturing existing in various fields, i.e. each particular component is produced in different units, e.g. automotive industries, etc.

Industrial automation's primary purpose:

1) Through episodic or physical examination, it is to reduce the job load of the man's strength.

2) To maximize demand within a limited period of time.

3) So there would not be more energy or reductions in the expense of productivity of the electricity used.

(4) The consistency of a commodity that might not be good for automation through manual manufacturing would be helpful in improving efficiency.

5) Increase flexibility

6) It is easy to operate and it also enhances the user's safety.

In the event of their relative isolation from enterprise IT, industrial sensors and applications have overall endured stability; this is no longer the case. Investors in cyber security must consider the conservative IT protection efficiency of network segmentation, firewalls, and Security Information and Event Managers (SIEMs) with applications that provide OT segments with real-time insight and hazard analysis.

Three key skills that need to be addressed by any operations manager and investor in cyber security as an IT/OT cyber security strategy arises. These capabilities include perceptibility, detection and remediation of threats in real-time.

IV. PROJECT DESIGN SETUP AND EXECUTION

Securing the data:

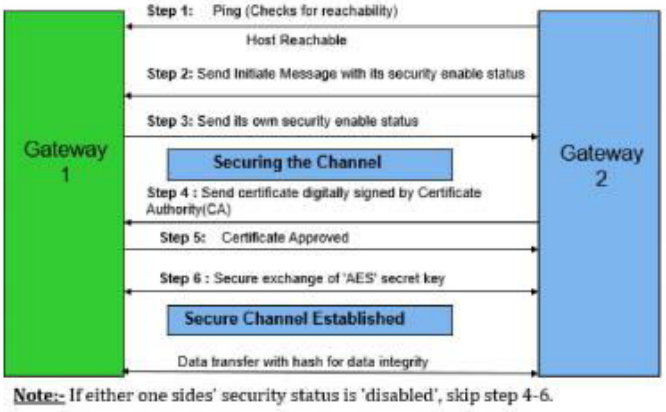
Millions of devices will be connected to the internet in the area of the Internet of Things (IoT) by high-capacity gateways that have the potential to interface with these legacy devices through Machine-to-Machine (M2M). However a protocol is required for communication between these different devices and the gateway. The data transferred from legacy systems can be used in sensitive applications as the size of implementation grows. Such systems may be primitive and do not have their own encryption capability to safeguard their data against manipulation as it is being transmitted. There is also a need to grant the gateway system the opportunity to protect data during transmission.

Therefore the proposal provides evidence of the principles of creating a trusted known environment between two devices or two IoT gateways by following means. a. Secure Channel

b. Data Security
c. Data Integrity

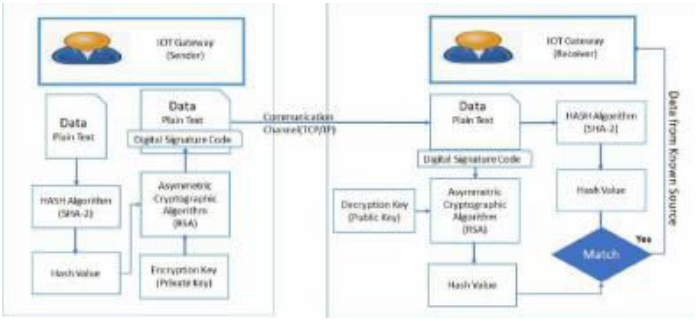
First, protection must be defined by the use of the algorithm by securing and setting up the channel from Gateway1 to Gateway2. For example, if gateway1 needs to direct confidential information to gateway2, and needs to make sure that it

can only be recited by gateway2, gateway1 can encrypt the data with the public key of gateway2. Only gateway2 is allowed to use the corresponding private key and as a result, the user with the power to decipher the encoded data to its original form. As only gateway2 is allowed to use the private key, it is possible that the encoded information will only be decoded by gateway2. And if the right to use the encoded information is advanced without permission, it would remain trustworthy since they will not have the right to use the private key of gateway2.



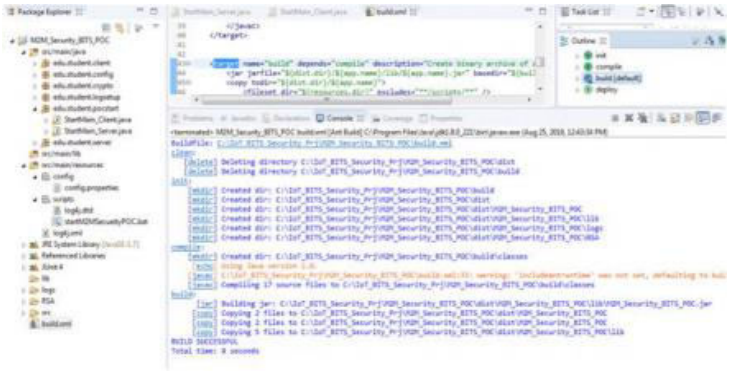
Bootstrapping is performed to create a trustworthy environment with several keys to transfer data from one gateway to another gateway. Enabling, using data encryption and decryption, to protect the contact channel for data integrity. Then by ensuring authentication, the right to use management to provide data access and privacy is established.

Securing the data with a digital signature using RSA and AES algorithms. Digital Signature is a mechanism that ensures that the problems of a correspondence have not been changed during the transport process. A digital signature offers a motive for the client to believe that the correspondence was produced and directed by the server requested. Since it offers digital signature, it is not feasible for the server to fail to force the guided contact. The digital signature ensures that during transport the communication has not been altered.



Sensitive data transfer using digital signature

Build Automation: First step for building the automation is to create the ANT based build environment to compile the program and create the field deployable software components. Then configuring the network such as the IP Address without rebuilding the application by the port numbers.



The logging mechanism system activities must be enabled which can be audited to find the state of the system and it also helps in debugging the issues which are found during the development or during the run-time environment.After the run-time that data security will be enabled and the transfer of the messages will be done securely. It has the capability to run the same application both in windows and Linux platforms.

IoT security Server and the client Instance

V. RESULT

Now the establishment of the secure channel is done from the server to the client communication. In which with the help of the port numbers the data will be secured in which the key exchange happens from server to client which will be the encrypted information.

Communication establishment between client and serverAbove is the screenshot of the Log Message screen depicting the communication established between client and Server and security keys has been exchanged successfullyhe transfer of the message from the server to client gateway and the data that is being transferred from the client to server or from server to the client has been encrypted.

Secure Exchange of messageThe above Log Message screen depicts the secure messages exchanging between client and Server and security keys have been exchanged successfully. The data that has been encrypted and is securely decrypted between the client and the server.

VI. CONCLUSION

It is to be inferred in this project that the paper guarantees cyber protection and provides a valuable definition of cyber-attacks in industrial automation through information management and surveillance. In order to minimize the difficulties that arise during contact between two gateways, the approach used in the paper is used. Using improved procedures and algorithms to guard essential contact networks and connections, the information will be analyzed.

VII. PROPOSED FUTURE SCOPE

1. Exploration of ETSI Security Standards.

2. Bootstrapping with Multiple Keys between Multi-Client and One-Server. 3. Exploration of Various security Algorithms

4. Profiling on each algorithm performance

5. CA Certification Integration

6. Encrypted Software download over secure channel

7. One M2M Open source gateway

REFERENCES

1) Li Da Zu" Internet of Things in Industries: A Survey" IEEE Transactions on Industrial Informatics, vol. 10, no. 4, November 2014.

2) Sadeque Reza Khan Professor Dr. M. S. Bhat "GUI Based Industrial Monitoring and Control System ``IEEE paper, 2014.

3) Ayman Sleman and Reinhard Moeller ``Integration of Wireless Sensor Network Services into other Home and Industrial networks "IEEE paper.

4) K. Suzuki, M. Inoue, Home network system with cloud computing and distributed autonomous control, IEEE 16th International Symposium on Consumer Electronics (ISCE), 2012.

5) IEEE 1686-2013, IEEE standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, [Online]. Available: http://standards.ieee.org/findstds/standard/1686-2007.html [Accessed September 2019]

6) W. Michael Sutton, P.E., Project Sales Engineer – SE Region, Phoenix Contact Co-Authors: DeraleeBowlin, Industry Manager – Electric Power, Phoenix Contact Dan Schaffer, Business Development Manager – Networking & Security, Phoenix Contact https://stevenengineering.com/Tech_Support/PDFs/67WHITEPAPER_CYBERSECURITY.pdf

7) Yiling Zheng, Song Zheng, Cyber Security Risk Assessment for Industrial Automation Platform, 2015 IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing

8) Hongyu Pei Breivold, Kristian Sandström, Internet of Things for Industrial Automation – Challenges and Technical Solutions, 2015 IEEE International Conference on Data Science and Data Intensive Systems

9) Prof.Niranjan M, IOT Based Industrial Automation, *National Conference On Advances In Computational Biology, Communication, And Data Analytics*

10) Deval Bhamare, MaedeZolanvari, AimanErbad, Cyber security for Industrial Control Systems: A Survey, https://www.researchgate.net/publication/337377177