INDUSTRIAL (IOT) AUTOMATION AND CYBER SECURITY

Santi Priyanka Prem
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad

V.V.S.S.S.BALARAM
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad

Sunil Bhutada
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad

Abstract- In our day to day life we read about the new techniques of cybersecurity attacks happening in the our country it may be to obtain the private information or to know about the information of specified group of industries network to cause them fall and lose power. Cyber-attacks in the IT sector or companies are unlimited. As a matter of fact many corporate industries are using IOT which is used to connect and for the transfer of data from device to another which is called as MACHINE TO MACHINE communication while transferring of the data cybersecurity attacks are occurring so that the attacker can control and monitor the information. In this paper we have proposed the Industrial automation using IOT by providing cybersecurity. The main purpose in this paper is to use IOT in Industries by enabling data security and exchanging or transfer secured messages.

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

I. INTRODUCTION

As we see the technology has been growing hastily and is used by industries to protect and secure the information or the data .Cyber security acts as an important role in Industrial automation and control system. If the cyber attacker hacks the system the loss of the industries or any organisation will be vast. The industrial automation and control system is a field in which the Iot i.e., the internet of things which has numerous aids in the present technology which supports processes and upkeep of self-governing cooperation amid the devices are known to each other for information interchange to decrease manual work. The real-time information is collected as of the huge amount of these unified corporeal hardware units could be recycled for evolving new intellectual applications. Many problems will occur while processing new intellectual applications in providing security and protecting the data, and the accessibility and dependability to fulfil the new framework of technology, for specific field needs in Industrial automation and the control system.

Industrial automation is constantly mesmerizing. The new intellectual technology has been changing the world of internet, the computing and solutions are which used by the industrial control system to operate the applications through cloud by involving unswervingly or by circuitously to the internet. Many online internet sites of customer centric solutions are converting to cloud centric solutions. The Industrial Control System network results in enormous crimes, there are many industries which uses computing for data storage and transfer which can be hacked and several tragedies takes place which will impact personally and professionally. The security provided through Industrial Control System is used to secure the data in contradiction of misfortunes or purposeful jeopardy. The security control over the Industrial Control System is limited so the information will be lost and that data can be used illegally by the hacker or the attackers to right to use the properties or the private data. The mechanisms of the native devices with the connection loss will become a hazard for damage of the information, interruptions in the manufacturing and fabrication procedure, circulation fault and damagingly effect related units. In this project we are providing the encryption of the data and secure exchange of the data takes place from one gateway to another that from the sever to the client.

Ⅱ.Literature Review

In this part of the paper we discuss and examine the foremost reviews in the arena of industrial control system and the security provided for the industrial automation. Earlier computers were designed; to accomplish numerous tasks[2]. Every Industry in the world are using computers for automation purpose to reduce the work load which is manually done, the applications are controlled and monitored by the humans. The Industrial automation is done through the intellectual technologies in the past such as Bluetooth and radio frequency which are used to communicate and control the data only for short distance[6][10]. The situations which are faced through the industrial automation was monitored with the help of and cameras to reduce the workload for humans implementation of Internet of things in the industries to monitor and inform the liable authority to take the right measures it may take some time which will harm the properties and it’s a time takin process[5][9]. Industrial automation then further updated to the IOT but there are many security issues that are faced by the industries[3]. The series of cyber security in Industrial Control System shows the security incidents during the communication through software are more likely susceptible for the exploitation of the data[7]. The main characteristics of this paper are to monitor and protect the transfer of the data or the information from one machine to another machine[8]. The data analytics and computing of Information Control Systems, the safety is quiet important concern[1]. To provide security it might cause great price to subordinate with the ruptures in the real-time. The complexity of new malware attacks in the Industrial control systems, with no attacks, due to which prevention and the detection of the cyber-attacks has become difficult[4]. In next section of the paper we will discuss about the challenges that are faced and how to provide the protection and transfer of the data.

Ⅲ Challenges in the Industrial Automation

Industrial automation extents in excess types of Industrial control systems. Industrial automation is done in many different domains for the execution of the information of the applications, (i) the creation of the product which is done in a step by step process i.e., stage by stage e.g., food production industries, pharma industries etc. (ii) the process of continuous production done without any disruption e.g. Glass industries, paper industries etc. (iii)different types of production happening in different sectors i.e., every single product is manufactured in different units e.g., automobile industries etc.

The main purpose of the industrial automation:

1) It is to reduce the work load of the man power by episodic or physical inspection.
2) To increase in the production in short span of time.
3) Due to which there won’t be more energy or the power used cost of the productivity decreases.
4) The quality of the product which the manual manufacturing may not be good to automation will be helpful in the improvement of production
5) Increase the Suppleness
6) It will be easily operated and it also increases the safety for the user.

Industrial sensors and applications have over all endured secure in arrears to their relative isolation from enterprise IT, this is no more the case. Cybersecurity investors comprehend the conservative IT security performs of network segmentation, firewalls and Security Information and Event Managers (SIEMs) must be accompanied with technologies that bring real-time visibility and threat analysis to OT segments.

Three core capabilities that every operations manager and cybersecurity investor necessities to consider when emerging an IT/OT cybersecurity approach. These capabilities comprise Real-time Perceptibility, Detection and Remediation of the Threats.

IV.Project design setup and execution

Securing the data:

In the field of Internet of Things (IoT) Millions of devices will be connected to internet through high capability gateways which have the capability of Machine-to-Machine (M2M) communication with these legacy devices. However, for the communication between these distinct devices and the gateway a protocol is necessary. As the scale of deployment increases the data transferred by the legacy devices can be used in critical application. These devices may be primitive and would not be having any security capabilities of their own to protect their data from theft while it's i.e. being transmitted. Hence there is need to give capability to the gateway device to secure the data during transmission.

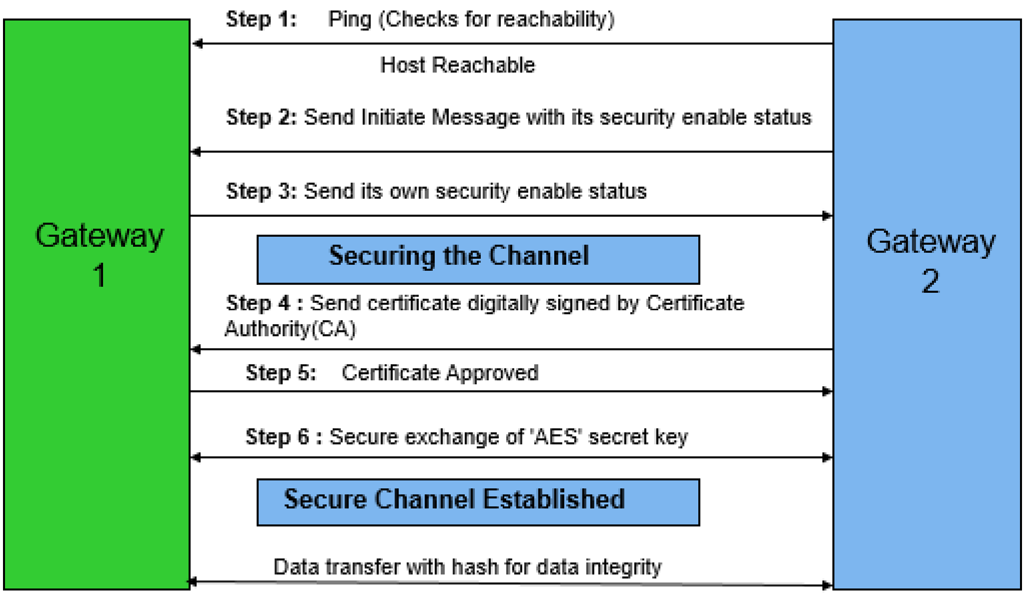
So, proposal is implement proof of the concepts in creating Trusted known environment between two devices or two IoT gateways by following means

a. Secure Channel
b. Data Security
c. Data Integrity

First the security must be established by using from Gateway1 to Gateway2 by using the algorithm by securing and establishing the channel.

For Example, if gateway1 needs to direct delicate information to gateway2, and needs to be certain that only gateway2 may be capable to recite it, gateway1 will encode the information with gateway2's Public Key.

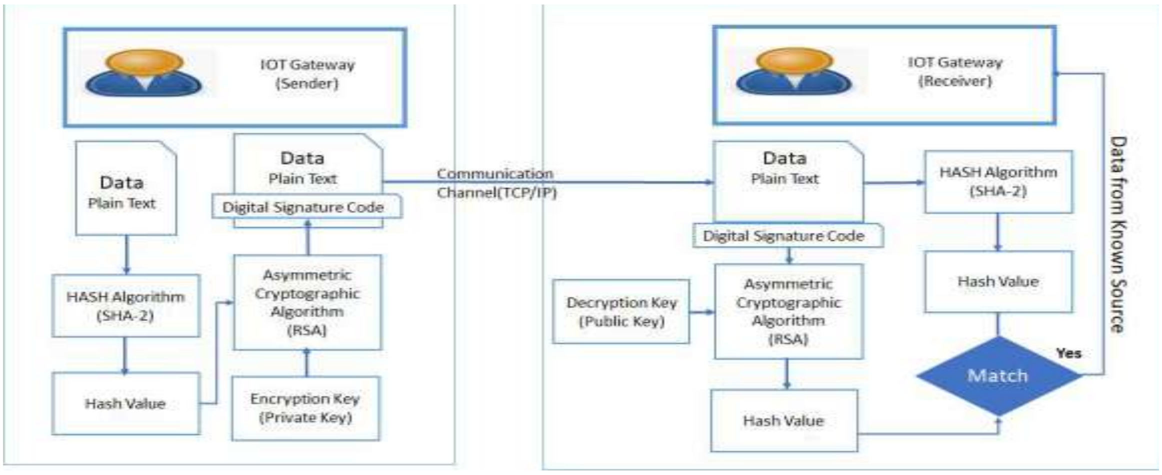
Only gateway2 has right to use to the matching Private Key and as a consequence the individual with the ability of decoding the encoded information to its actual form.As only gateway2 has right to use to the Private Key, it is conceivable that only gateway2 can decode the encoded information. Even if unauthorised advances the right to use to the encoded information, it will endure trustworthy as they would not have the right to use to gateway2's Private Key.


Gateway 1
Gateway 2
Step 1: Ping (Checks for reachability)
Host Reachable
Step 2: Send Initiate Message with its security enable status
Step 3: Send its own security enable status
Securing the Channel
Step 4 : Send certificate digitally signed by Certificate Authority(CA)
Step 5: Certificate Approved
Step 6 : Secure exchange of 'AES' secret key
Secure Channel Established
Data transfer with hash for data integrity

Note:- If either one sides' security status is 'disabled', skip step 4-6.

Bootstrapping with the multiple keys is done to create a trustworthy environment to transfer the data from one gateway to another gateway. Enabling to secure the communication channel for data integrity by using data encryption and decryption. Then by securing the authentication to identify the right to use management to provide the security and protecting of the data.

Securing the data by using RSA and AES algorithms by the digital signature. Digital Signature is a procedure that gives assurances that the matters of a communication have not been transformed during the transportation. A digital signature provides the client a motive to trust that the communication was produced and directed by the requested server. As it provides digital signature, the server cannot reject obligating the directed communication. The Digital signature guarantees that the communication was not transformed during the transportation.

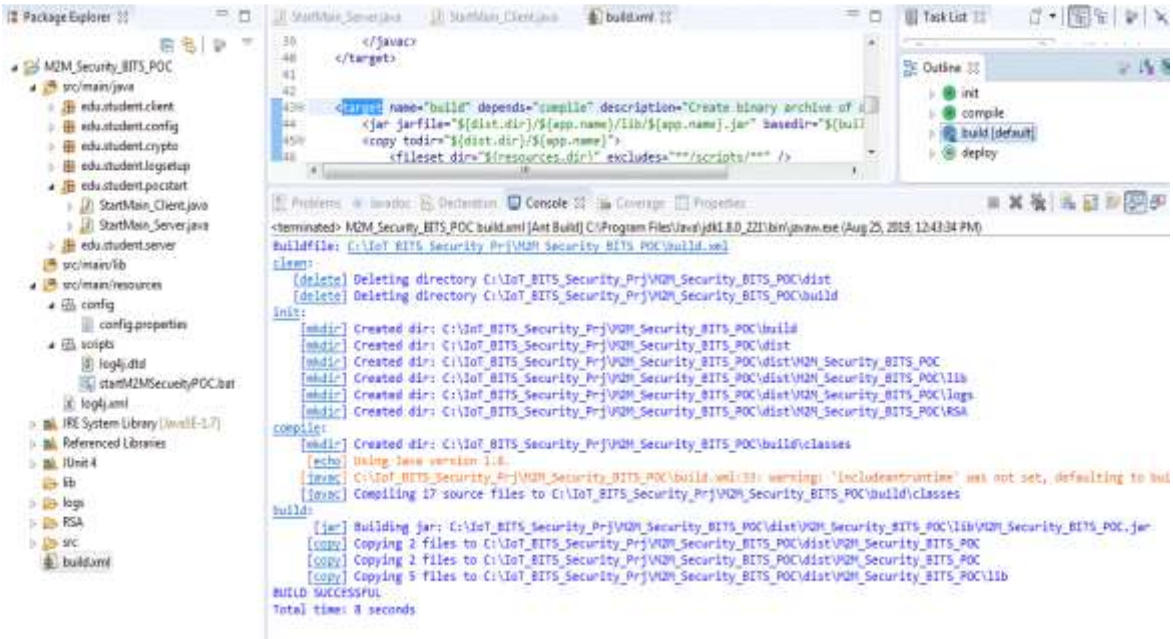


Sensitive data transfer using digital signature

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.



```
        </javac>
    </target>


    <target name="build" depends="compile" description="Create binary archive of a
        <jar jarfile="${dist.dir}/${app.name}/lib/${app.name}.jar" basedir="${buil
        <copy todir="${dist.dir}/${app.name}">
            <fileset dir="${resources.dir}" excludes="**/scripts/**" />
```

```
<terminated> M2M_Security_BITS_POC build.xml [Ant Build] C:\Program Files\Java\jdk1.8.0_221\bin\javaw.exe (Aug 25, 2019, 12:43:34 PM)
Buildfile: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\build.xml
clean:
   [delete] Deleting directory C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist
   [delete] Deleting directory C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\build
init:
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\build
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC\lib
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC\logs
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC\RSA
compile:
    [mkdir] Created dir: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\build\classes
     [echo] Using Java version 1.8.
    [javac] C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\build.xml:33: warning: 'includeantruntime' was not set, defaulting to bui
    [javac] Compiling 17 source files to C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\build\classes
build:
      [jar] Building jar: C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC\lib\M2M_Security_BITS_POC.jar
     [copy] Copying 2 files to C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC
     [copy] Copying 2 files to C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC
     [copy] Copying 5 files to C:\IoT_BITS_Security_Prj\M2M_Security_BITS_POC\dist\M2M_Security_BITS_POC\lib
BUILD SUCCESSFUL
Total time: 8 seconds
```

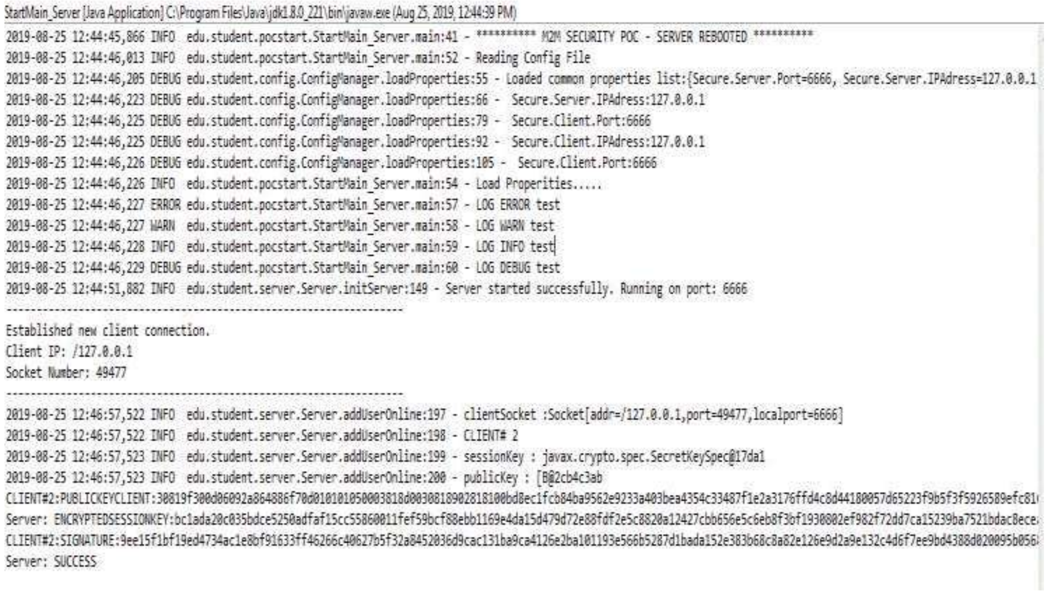
The logging mechanism system activities must be enabled which can be audited to find the state of the system and it also helps in debugging the issues which are found during the development or during the run-time environment.

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

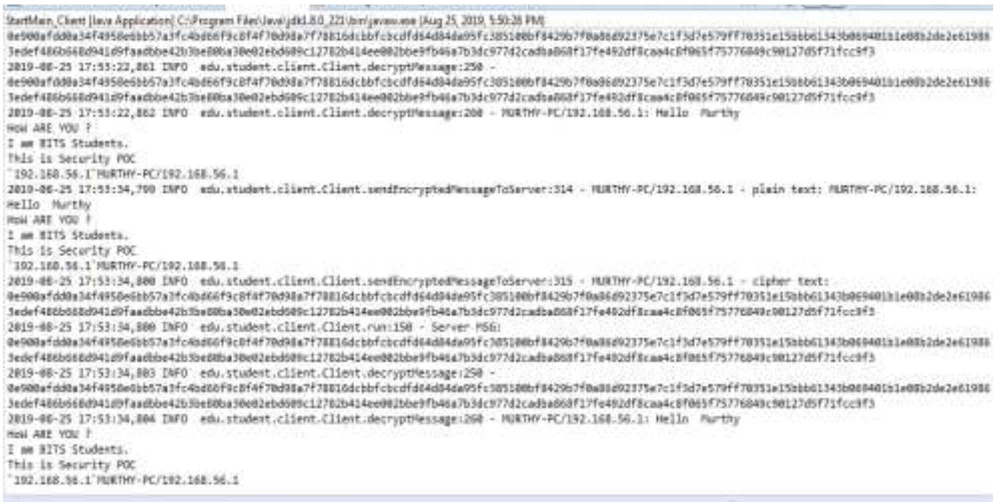
Now the establishment of the secure channel is done from the server to the client communication. In which with the help of the port numbers the data will be secured in which the key exchange happens from server to client which will be the encrypted information.



```
StartMain_Server [Java Application] C:\Program Files\Java\jdk1.8.0_221\bin\javaw.exe (Aug 25, 2019, 12:44:39 PM)
2019-08-25 12:44:45,866 INFO  edu.student.pocstart.StartMain_Server.main:41 - ********** M2M SECURITY POC - SERVER REBOOTED **********
2019-08-25 12:44:46,013 INFO  edu.student.pocstart.StartMain_Server.main:52 - Reading Config File
2019-08-25 12:44:46,205 DEBUG edu.student.config.ConfigManager.loadProperties:55 - Loaded common properties list:{Secure.Server.Port=6666, Secure.Server.IPAdress=127.0.0.1
2019-08-25 12:44:46,223 DEBUG edu.student.config.ConfigManager.loadProperties:66 -  Secure.Server.IPAdress:127.0.0.1
2019-08-25 12:44:46,225 DEBUG edu.student.config.ConfigManager.loadProperties:79 -  Secure.Client.Port:6666
2019-08-25 12:44:46,225 DEBUG edu.student.config.ConfigManager.loadProperties:92 -  Secure.Client.IPAdress:127.0.0.1
2019-08-25 12:44:46,226 DEBUG edu.student.config.ConfigManager.loadProperties:105 -  Secure.Client.Port:6666
2019-08-25 12:44:46,226 INFO  edu.student.pocstart.StartMain_Server.main:54 - Load Properities.....
2019-08-25 12:44:46,227 ERROR edu.student.pocstart.StartMain_Server.main:57 - LOG ERROR test
2019-08-25 12:44:46,227 WARN  edu.student.pocstart.StartMain_Server.main:58 - LOG WARN test
2019-08-25 12:44:46,228 INFO  edu.student.pocstart.StartMain_Server.main:59 - LOG INFO test
2019-08-25 12:44:46,229 DEBUG edu.student.pocstart.StartMain_Server.main:60 - LOG DEBUG test
2019-08-25 12:44:51,882 INFO  edu.student.server.Server.initServer:149 - Server started successfully. Running on port: 6666
-----------------------------------------------------------------
Established new client connection.
Client IP: /127.0.0.1
Socket Number: 49477
-----------------------------------------------------------------
2019-08-25 12:46:57,522 INFO  edu.student.server.Server.addUserOnline:197 - clientSocket :Socket[addr=/127.0.0.1,port=49477,localport=6666]
2019-08-25 12:46:57,522 INFO  edu.student.server.Server.addUserOnline:198 - CLIENT# 2
2019-08-25 12:46:57,523 INFO  edu.student.server.Server.addUserOnline:199 - sessionKey : javax.crypto.spec.SecretKeySpec@17da1
2019-08-25 12:46:57,523 INFO  edu.student.server.Server.addUserOnline:200 - publicKey : [B@2cb4c3ab
CLIENT#2:PUBLICKEYCLIENT:30819f300d06092a864886f70d010101050003818d0030818902818100bd8ec1fcb84ba9562e9233a403bea4354c33487f1e2a3176ffd4c8d44180057d65223f9b5f3f5926589efc81
Server: ENCRYPTEDSESSIONKEY:bc1ada20c035bdce5250adfaf15cc55860011fef59bcf88ebb1169e4da15d479d72e88fdf2e5c8820a12427cbb656e5c6eb8f3bf1930802ef982f72dd7ca15239ba7521bdac8ece
CLIENT#2:SIGNATURE:9ee15f1bf19ed4734ac1e8bf91633ff46266c40627b5f32a8452036d9cac131ba9ca4126e2ba101193e566b5287d1bada152e383b68c8a82e126e9d2a9e132c4d6f7ee9bd4388d020095b056
Server: SUCCESS
```

Communication establishment between client and server

Above is the screen shot of Log Message screen depicts the communication established between client and Server and security keys has been exchanged successfully.The 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.



```
StartMain_Client [Java Application] C:\Program Files\Java\jdk1.8.0_221\bin\javaw.exe (Aug 25, 2019, 5:50:28 PM)
0e900afdd0a34f4950e6bb57a3fc4bd66f9c8f4f70d98a7f78816dcbbfcbcdfd64d84da95fc385100bf8429b7f0a86d92375e7c1f3d7e579ff70351e15bbb61343b069401b1e08b2de2e61986
3edef486b668d941d9faadbbe42b3be80ba30e02ebd609c12782b414ee002bbe9fb46a7b3dc977d2cadba868f17fe492df8caa4c8f065f75776849c90127d5f71fcc9f3
2019-08-25 17:53:22,861 INFO  edu.student.client.Client.decryptMessage:250 -
0e900afdd0a34f4950e6bb57a3fc4bd66f9c8f4f70d98a7f78816dcbbfcbcdfd64d84da95fc385100bf8429b7f0a86d92375e7c1f3d7e579ff70351e15bbb61343b069401b1e08b2de2e61986
3edef486b668d941d9faadbbe42b3be80ba30e02ebd609c12782b414ee002bbe9fb46a7b3dc977d2cadba868f17fe492df8caa4c8f065f75776849c90127d5f71fcc9f3
2019-08-25 17:53:22,862 INFO  edu.student.client.Client.decryptMessage:260 - MURTHY-PC/192.168.56.1: Hello  Murthy
HOW ARE YOU ?
I am BITS Students.
This is Security POC
`192.168.56.1`MURTHY-PC/192.168.56.1
2019-08-25 17:53:34,790 INFO  edu.student.client.Client.sendEncryptedMessageToServer:314 - MURTHY-PC/192.168.56.1 - plain text: MURTHY-PC/192.168.56.1:
Hello  Murthy
HOW ARE YOU ?
I am BITS Students.
This is Security POC
`192.168.56.1`MURTHY-PC/192.168.56.1
2019-08-25 17:53:34,800 INFO  edu.student.client.Client.sendEncryptedMessageToServer:315 - MURTHY-PC/192.168.56.1 - cipher text:
0e900afdd0a34f4950e6bb57a3fc4bd66f9c8f4f70d98a7f78816dcbbfcbcdfd64d84da95fc385100bf8429b7f0a86d92375e7c1f3d7e579ff70351e15bbb61343b069401b1e08b2de2e61986
3edef486b668d941d9faadbbe42b3be80ba30e02ebd609c12782b414ee002bbe9fb46a7b3dc977d2cadba868f17fe492df8caa4c8f065f75776849c90127d5f71fcc9f3
2019-08-25 17:53:34,800 INFO  edu.student.client.Client.run:150 - Server MSG:
0e900afdd0a34f4950e6bb57a3fc4bd66f9c8f4f70d98a7f78816dcbbfcbcdfd64d84da95fc385100bf8429b7f0a86d92375e7c1f3d7e579ff70351e15bbb61343b069401b1e08b2de2e61986
3edef486b668d941d9faadbbe42b3be80ba30e02ebd609c12782b414ee002bbe9fb46a7b3dc977d2cadba868f17fe492df8caa4c8f065f75776849c90127d5f71fcc9f3
2019-08-25 17:53:34,803 INFO  edu.student.client.Client.decryptMessage:250 -
0e900afdd0a34f4950e6bb57a3fc4bd66f9c8f4f70d98a7f78816dcbbfcbcdfd64d84da95fc385100bf8429b7f0a86d92375e7c1f3d7e579ff70351e15bbb61343b069401b1e08b2de2e61986
3edef486b668d941d9faadbbe42b3be80ba30e02ebd609c12782b414ee002bbe9fb46a7b3dc977d2cadba868f17fe492df8caa4c8f065f75776849c90127d5f71fcc9f3
2019-08-25 17:53:34,804 INFO  edu.student.client.Client.decryptMessage:260 - MURTHY-PC/192.168.56.1: Hello  Murthy
HOW ARE YOU ?
I am BITS Students.
This is Security POC
`192.168.56.1`MURTHY-PC/192.168.56.1
```

Secure Exchange of message

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

VI.Conclusion

In this project it is to conclude that the paper guarantees the cyber security and offer useful concept of the cyber-attacks in the industrial automation done by the controlling and monitoring of the information. The process that is used in the paper is used to reduce the problems that occur during the communication between two gateways. The information will be evaluated by using the enhanced procedures and algorithms for guarding the significant communication channels and the links.

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: Deralee Bowlin, Industry Manager – Electric Power, Phoenix Contact Dan Schaffer, Business Development Manager – Networking & Security, Phoenix Contact https://stevenengineering.com/Tech_Support/PDFs/67WHITE-PAPER_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 BhamareΩ, Maede Zolanvariφ, Aiman Erbad¥, Cybersecurity for Industrial Control Systems: A Survey, https://www.researchgate.net/publication/337377177