2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

Presenting IoT Security based on Cryptographic Practices in Data Link Layer in Power Generation Sector

Iqra Hussain
Amity Institute of Information Technology,
Amity University Uttar Pradesh, Noida
iqrahussain4@gmail.com

Nitin Pandey
Associate Professor
Amity Institute of Information Technology,
Amity University Uttar Pradesh, Noida
npandey@amity.edu

Ajay Vikram Singh
Associate Professor
Amity Institute of Information Technology,
Amity University Uttar Pradesh, Noida
avsingh1@amity

Mukesh Chandra Negi
Delivery Manager,
TechMahindra Ltd
A7, Sector 64, Noida
MN00330419@techmahindra.com

Ajay Rana
AIIT, Amity University Uttar Pradesh
Noida, India
ajay_rana@amity.edu

***Abstract*- With increasing improvements in different areas, Internet control has been making prominent impacts in almost all areas of technology that has resulted in reasonable advances in every discrete field and therefore the industries too are proceeding to the field of IoT (Internet of Things), in which the communication among heterogeneous equipments is via Internet broadly. So imparting these advances of technology in the Power Station Plant sectors i.e. the power plants will be remotely controlled additional to remote monitoring, with no corporal place as a factor for controlling or monitoring. But imparting this technology the security factor needs to be considered as a basic and such methods need to be put into practice that the communication in such networks or control systems is defended against any third party interventions while the data is being transferred from one device to the other device through the internet (Unrestricted Channel). The paper puts forward exercising RSA ,DES and AES encrypting schemes for the purpose of data encryption at the Data Link Layer i.e. before it is transmitted to the other device through Internet and as a result of this the security constraints are maintained. The records put to use have been supplied by NTPC, Dadri, India plus simulation part was executed employing MATLAB.**

Keywords: IoT, DCS, DDCMIS, PLC, SCADA, DES, AES, RSA, I/O, NTPC.

I. INTRODUCTION

The Internet of Things (IoT) is defined as ubiquitous and pervasive networks, enabling control and monitoring of physical settings by the investigation, collection and handling of data that is produced by smart devices and sensors [1]. IoT links different components of people's lives and so individual devices interact and communicate with each other for providing exclusive assistances. This intelligent behavior of objects lead to many things like Logistics, smart cities, home automation, smart agriculture health care, security, military surveillance etc [3].

Architectures that are based on Internet of Things comprise systems and devises that are linked transversely to networks that are heterogeneous in nature and employ various proprietary protocols and basic standards. Networks like these provide services that are powerful but even expose the systems to various threats like message falsification or eavesdropping the messages. Therefore for protection against such risks the Internet of Things devices or systems need to have proper communication security capacities. Therefore if we talk about the different layers of communication protocols, they too need to be defended against various security attacks and threats and similarly a breach in the Data Link Layer may end up disrupting the whole communication and compromise in terms of security. Data Link layer is subjected to the transfers of data coming in or out across a physical layer in the networks. It's the layer 2 in Open system Interconnects models for communication protocol. Data Link Layer is further divided into 2 sub layers:

- The Media Access Control Layer.
- The Logic Link Control Layer

It's the job of Data Link Layer to ensure that the initial connections have been set up and then further helps in dividing the output data into data frames. It also provides with the acknowledgements that the data has been received successfully from the recipient. It also analyses the bit patterns at discrete places in the data frames [10].

In Power generation sector the whole power is generated using huge Power Stations which further include several Power Plants. A power station is a built-up source which is intended for manufacture of electric energy or power. Common design of an energy station comprises of one or a number of generators, a rotating machine so as to converse motorized energy into electric energy thus the electric flow formed, is by the absolute movement among repellent area and conductors. The power resources used for rotating generators differ widely, but mainly power stations raze fuels from remnants such as coal, oils or the natural gas which gives out electric energy.

Furthermore all the operations of the power stations are managed with help of energy Controlling System centered on data obtained from system which is situated distantly and is both computerized and manual. So the energy station

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

controlling system deals with a number of types of systems with associating instrumentation employed in a power station for production Purposes. A energy station controlling systems include various sub systems; that are programmable logic controllers (PLC), Distributed Controlling Systems (DCS), Distributed Digital Controlling Monitors and Information System (DDCMIS), the Supervisory Control and Data Acquisition System (SCADA).

II. MOTIVATION AND OBJECTIVES

Associating IoT with power plant operations is a big thing in itself but at the same time the security needs to be taken care of with equal zeal. Therefore while using the automated power plant stations based on IoT security should be an elevated concern because any small loop hole can bring a whole power system down with devastating results. Some objectives are stated below in support of IoT security in Power plants:

1. Using IoT security all the generating processes can be made flexible and thus operations will be more efficient and resourceful and finally result in more amount of power accordingly.
2. When the analytics are accurate the power emission will accordingly be higher.
3. With the onset of IoT security trusting mechanisms during the transmission of data are achieved.
4. IoT security even plays a vital role in maximizing the security aspects of different operations to be performed.
5. IoT security can provide us with enhancement of vital information regarding operations on different devices.

III. NECESSITY OF PROPOSED METHOD

1. The sensors or controls or any software's that currently run equipments and facilities in power plant stations have become complex to operate and challenging to include any new features or make improvements, whereas by the introduction of IoT security different sensors, operating technologies or communicating modules work together in a mesh and make the operations easy to operate.
2. Sometimes a data silos gets created because of limitations between different interior and exterior systems while technologies working in a mesh created by IoT technologies result in the formation of commendable and intelligent results too.
3. It has been seen many time the operating systems that are aging or technologies that are vulnerable can add to risks and therefore the IoT security plays a vital role against such risks.
4. Currently the intelligence controls and embedded computing are very much bounded at power plant stations but by sourcing the power plants based on IoT security these controls become trustworthy and even durable to any sort of compromises.
5. The different edge devises that produce enormous amounts of real time data like different reading in temperature, pressure, oil conditions or levels, accelerometers etc are very critical for the smooth functioning of power plants and hence need to be protected against any third part attacks or intrusions. Therefore by the use of different cryptographic practices while the transmission of this data will be helpful accordingly.
6. Likewise the IoT hub that forms the entering location of data and as well as the exit location for various commands too needs to be kept secure as well.
7. Similarly different data analytics are to be performed on the data and then fetched back or fro so that the decisions and predictions are further made accordingly. So this data too needs to be kept safe and secure so we end up with exact predictions and right decisions.

IV. OUR PROPOSITION

Based on the requirements, control rooms within power plant are installed with various control systems. The system controls are positioned within or near a power plant. Control Rooms acts as access point for controlling and monitoring the power plant as these control rooms at field level indicate the data or information that pass to diverse I/Os module of control systems where data is processed at different control stations. Lone power plants consist of required system controls for proper operations plus groups along required information and skill for accurate working of power plants.

The proposal aims at remotely inspecting and supervising of a power plant. It includes a shift of power plants to field of IOT (Internet of Things) in which there is a direct M2M communications without requiring any physicals presence of people for the proper functioning of the plant that includes various controlling and monitoring tasks. As the system is remotely accessed and there occurs machine to machine communication there is a need of Internet (Ethernet) and as the Internet is a public network and is inherently insecure and give rise to the issues regarding data privacy, authenticity, integrity and confidentiality. Therefore our proposition is aimed at encryption of data that is being received from field controls and then the encrypted data will be passed from field controls to local servers which in turns make this encrypted data accessible to distant servers through Internet.

Next recipient decrypts received encoded info. and sends back response the remote station again in encrypted form. The data in response in encoded mode is decoded. Next it is passed to control module plus filed controls where the required actions are performed. The area tools example actuators and sensors are connected to control systems through I/O controlling module. The area tools transmit factors example temperatures, pressure flows, and different operational conditions to controllers. This document puts forward RSA AES and DES for encryption. The simulation is performed using MATLAB. The data is provided by NTPC, India.

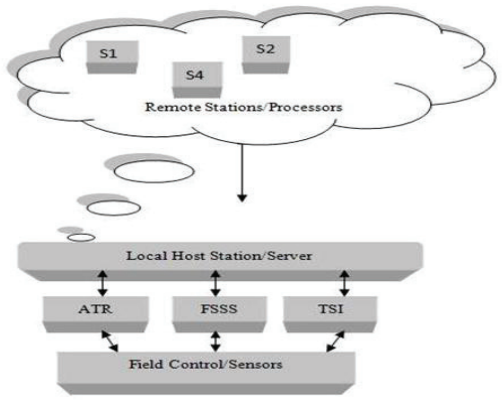

Fig. 1. Generalized proposed architecture

V. IMPLEMENTATION

The accomplishment of the projected design is done at the branch of NTPC Dadri, India. This research paper was initiated with the unit start-ups/shutdowns schemes of a SGS Gas turbine of NTPC Power station. The system (S1) was later on allied to the Tx/Rx (Transmitter/Receiver) of the turbine's control station. As on the other hand a server was connected to the same system using Ethernet router.

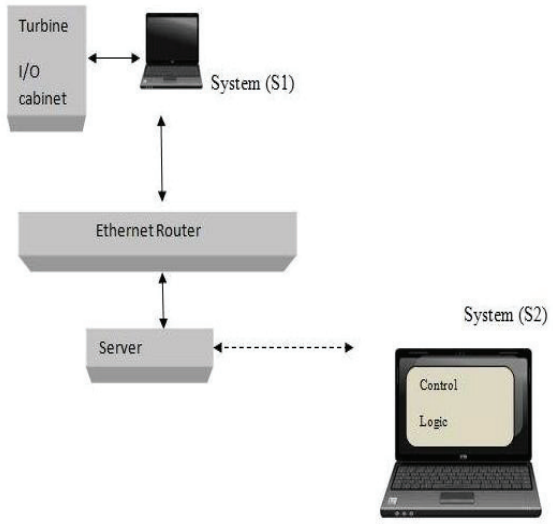

Fig. 2. Implementation Architecture

VI. COMPARISON ANALYSIS

TABLE I. ENCRYPTION TIME COMPARISONS

Text size	RSA	DES	AES
100 bytes	45	56	63
1 kb	62	60	64
2kb	78	66	65

TABLE II. DECRYPTION TIME COMPARISONS

Text size	RSA	DES	AES
100	141	6	2
1kb	156	3	2
2kb	169	2	3

VII. TERMINATION AND SCOPE

Execution segment of the method proposed was approved by the C&I sector of NTPC, Dadri India and information safety issues were handled using RSA, DES and AES encoding techniques at layer 2 of the communication set of rules. The proposed method is approved by the C&I sector although the encoding decoding time used by all algos is more than predicted, thus creating a time delays in entire procedure.

Upcoming usage of the paper will push to improvise the encoding techniques used to beat the time wait issues and maintain the safety also.

ACKNOWLEDGEMENT

Writers of this research are thankful to the Founder President of Amity University, Dr. Ashok K. Chauhan, who has overpoweringly shown his eager attention in development study in Amity University and is an inspiration for accomplishing advanced triumph.

REFERENCES

[1] Anderson, C. R. 2014. The internet of Things: The possibilities are endless, but how will we get there? IDC APeJ Internet of Things Web Conference on 19 June 2014.

[2] Q. Guo, T. Johansson, and P. Stankovski, "A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors," Advances in Cryptology (ASIACRYPT 16), LNCS 10031, Springer, 2016, pp. 789–815.

[3] R. Benabdessalem, M. Hamdi, Tai-Hoon Kim, A Survey on Security Models, Techniques, and Tools for the Internet of Things 7th International Conference on Advanced Software Engineering & Its Applications, 978-1-4799-7761-1/14 2014 IEEE

[4] T. Alghamdi, A. Lasebae, M. Aiash, Security Analysis of the Constrained Application Protocol in the Internet of Things, 978-1-4799-2975-7/13/ 2013 IEEE

[5] Ojha, Deo Brat, et al. "An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel." International Journal of Advanced Networking and Applications 2.5 (2011): 841-845.

[6] Pandey, N., 2013. Secure Communication Scheme with Magic Square. Journal of Global Research in Computer Science, 3(12), pp.12-14.

[7] Hussain, Iqra, and Nitin Pandey. "Carrier data security using public key steganography in ZigBee." In Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on, pp. 213-216. IEEE, 2016.

[8] G. Gan, L. Zeyong, J. Jun, "Internet of things security analysis", Proc. IEEE Conf. iTAP, pp. 1-4, 2011.

[9] Bijoy Babu, Thafasal Ijyas, Muneer P., Justin Varghese, Anti-Cyber Crimes (ICACC), 2017 2nd International Conference, Abha, Saudi Arabia, "Security issues in SCADA based industrial control systems"

[10] Vivek Umasuthan, Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES "Protecting the Communications Network at Layer 2"

[11] Hyun-Jin Kim; Hyun-Soo Chang; Jeong-Jun Suh; Tae-shik Shon, 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA), "A Study on Device Security in IoT Convergence"

[12] Ajay Vikram Singh, Moushumi Chattopadhyaya, "Mitigation of DoS Attacks by Using Multiple Encryptions in MANET", 2015 4th IEEE International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 at AUUP, NOIDA, India, September 02-04, 2015 DOI: 10.1109/ICRITO.2015.7359300

[13] Minela Grabovica; Srđan Popić; Dražen Pezer; Vladimir Knežević2016 Zooming Innovation in Consumer Electronics International Conference (ZINC), "Provided security measures of enabling technologies in Internet of Things (IoT): A survey"Arunan Sivanathan; Daniel Sherratt; Hassan Habibi Gharakheili; Vijay Sivaraman; Arun Vishwanath, 2016

IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)

[14] S. Ghosh, A. Rana, V. Kansal, "A Hybrid Nonlinear Manifold Detection Approach for Software Defect Prediction" in 7th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2018, pp 453-459 (2018).

[15] H. Walia, A. Rana, V. Kansal, "Word Sense Disambiguation: Supervised Program Interpretation Methodology for Punjabi Language", in 2018 7th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2018, pp 762-767 (2018).

[16] B. Dayal Chauhan B, A. Rana, N. K. Sharma, "Impact of development methodology on cost & risk for development projects", in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, pp 267-272 (2018).

[17] S. Chawla, G. Dubey, A. Rana, "Product opinion mining using sentiment analysis on smartphone reviews", in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, pp 377-383 (2018).

[18] H. Walia, A. Rana, V. Kansal, "A Naïve Bayes Approach for working on Gurmukhi Word Sense Disambiguation", in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, pp 432-435 (2018).

[19] D. Gupta, A. Rana, S. Tyagi, "A novel representative dataset generation approach for big data using hybrid Cuckoo search", in International Journal of Advances in Soft Computing and its Applications, Vol. 10, Issue 1, pp 55-70 (2018).

[20] S. Ghosh, A. Rana, V. Kansal, "A Nonlinear Manifold Detection based Model for Software Defect Prediction", in Procedia Computer Science, Vol. 132, pp 581-594 (2018).