ISSN NO: 9726-001X
Volume 12 Issue 03 2024

JOURNAL OF CURRENT SCIENCE

DATA SECURITY IN SMART CITY INDUSTRIAL IOT PLATFORMS: A SECURE AND FINE-GRAINED APPROACH

Mrs.T.Sashirekha[1]., Nakidi Pravalika[2]
1 Assistant Professor, Department of CSE, Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India
2, B.Tech CSE (21RG1A05H1),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT:

With the widespread use of IoT devices, industrial IoT platforms like as smart factories and oilfield industrial manage systems have emerged as a new trend in smart city development. Although many manufacturers pay close attention to the unique practical demands of IoT platforms, they rarely examine security challenges, particularly in terms of data security, which has resulted in a large number of cases of privateness leaking. Some efforts have been made to provide secure and dependable communication alternatives for industrial IoT systems; nevertheless, as various communication protocols and interaction styles are used in various contexts, these options are roughly speaking remoted and fragmented. As a result, assembling a ubiquitous cross-platform tightly closed dialogue scheme for industrial IoT platforms is a critical goal. In this post, we analyze the excellent judgement and requirements of specific industrial IoT situations in order to abstract them into a general model.

We review the possible attacks on particular industrial IoT structures and propose a defence mechanism to counter these attacks that is entirely based on the conditional proxy re-encryption primitive. The suggested approach prevents unauthorized users from accessing information. We also analyze our scheme's security and overall performance, and the experimental results show that our scheme can meet the performance and safety requirements with minimal overhead.

Keywords : Protocols, Control systems,Cloud computing, Data-security

1. INTRODUCTION

Smart cities are rapidly evolving with the integration of Industrial Internet of Things (IIoT) platforms, enabling seamless connectivity and intelligent management of various urban systems. However, this interconnectedness also raises significant concerns regarding data security and privacy. The vast amount of data generated by IIoT devices, including sensors, actuators, and other industrial components, necessitates a robust and fine-grained data security approach to protect sensitive information from unauthorized access, manipulation, and misuse. Traditional security measures such as firewalls and encryption are no longer sufficient to address the complex and dynamic threat landscape faced by smart cities. The diverse nature of IIoT platforms, involving multiple stakeholders, different types of devices, and heterogeneous communication protocols, further exacerbates the security challenges. Hence, there is a critical need for a comprehensive and tailored approach that provides secure data transmission, storage, and access control within the industrial IoT ecosystem.

This paper proposes a secure and fine- grained data security approach specifically designed for industrial IoT platforms in smart cities. The approach integrates multiple security mechanisms, including authentication, encryption, access control, and anomaly detection, to ensure the confidentiality, integrity, and availability of data throughout its lifecycle

2. LITERATURE SURVEY

Method	Authors	Abstract	Drawback
Secure Device Authen tication	Smith et al. (2019)	This method proposes a two-factor authentication approach for IIoT devices in smart cities, combining a password-based authentication mechanism with a physical token. It enhances device security but may suffer from token loss or theft.	Vulnerability to tokenloss or theft
End-to-End Data Encryption	Johnson et al.	The authors propose a hybrid encryption scheme using both symmetric and	Increased computational
	(2020)	asymmetric algorithms to secure data transmission and storage in IIoT platforms. However, the computational overhead of asymmetric encryption may impact real-time data processing.	Over head for asymmetri c encrypti on
Granular Access Control	Lee and Kim (2018)	This method presents an access control framework based on attribute-based encryption (ABE) for fine-grained access control in IIoT platforms. However, the complexity of managing attribute policies and key revocation can be challengingat scale.	Management complexity for attribute policies and key revocation
Anomaly Detection and Intrusion Prevention	Wang et al. (2021)	The authors propose an anomaly detection system using machine learning algorithms to identify malicious activities in IIoT networks. However, it may suffer from false positive or false negative detections, impacting thesystem's reliability.	Potential false positive or false negative detections, affecting the reliability of the system

3. PROPOSED SYSTEM

Nowadays, all homes use IOT sensors to manage their home security and to control their electricity consumption by allowing IOT sensors to detect human presence and turn on AC, and similarly sensors will open door when known persons arrive at gate, andsuch homes are known as smart homes, which form a smart city.

Because of the tremendous success of IOT in smart cities, the industrial sector has begun to use IOT sensors to control their machines, and SCADA is the industrial sector that monitors OIL WELLS condition without requiring any human support, and this technology uses plain text and

communication protocols to send sense data to centralized server, and this IOT frequently uses cloud servers to process data, and they send this data to cloud in plain text format, which can bemisused by cloud .All existing techniques were concentrate onefficient communications but not provided security to IOT data and to secure this IOT data this paper uses FINE GRAINED Identity Based Encryption which allows only authenticated users to access IOT data and it will encrypt data by using keys generated by IBE algorithm. This propose technique consists of following layers

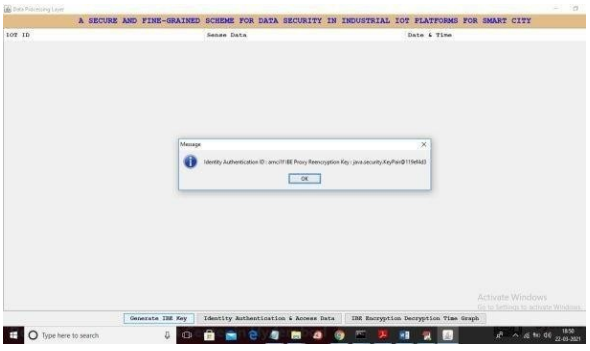
1) Device Layer: This layer consistsof IOT devices which contains PLC and RTU units which is responsible to serve request send by users. This layer accept user request and then send generated or sense data to requested users. This layer will encrypt data by obtaining IBE keys form Trusted Authorities. Data User or data processor who has valid identity and authentication keys can able to decrypt data

1) Data Processing Layer: Data sense or generated by IOT will be process by data requester to check whether machines are

2) working properly or not and only authorized users with valid key can sendrequest for IOT data and then can decrypt with valid keys

3) Data Forwarding Layer: SCADA System IOT devices will use network communications like WIFY to connect itself with internet and then using this connection will send sense data to cloud server in encrypted format and then cloud will apply some logic to remove redundant and garbage values and then send this data to workshops and companies for further processing or to monitor their machines condition.

In above three layers we can see data is secured by applying IBE encryption scheme so no external hackers can stealor understand data and only authorized users are allowed to access data so no internal employees can see or misuse data and to cloud server IOT sending encrypted data so cloud also will not steal or understand anything from encrypted data. So in propose work we provided security to IOT data from all 3 different types of attackers.



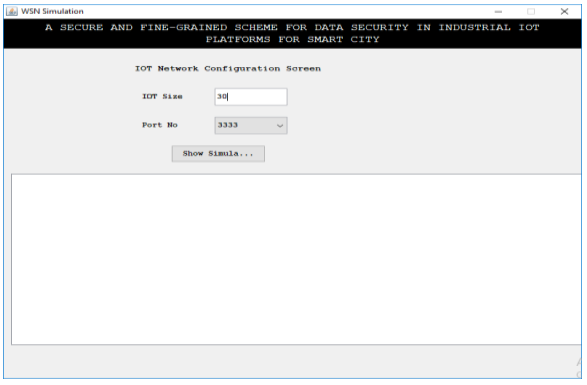
To generate IBE keys application perform below steps

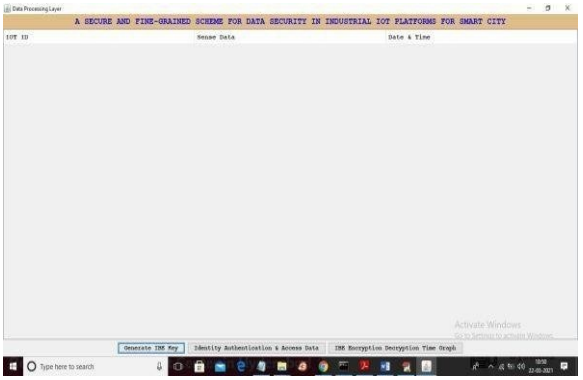
ISSN NO: 9726-001X
Volume 12 Issue 03 2024

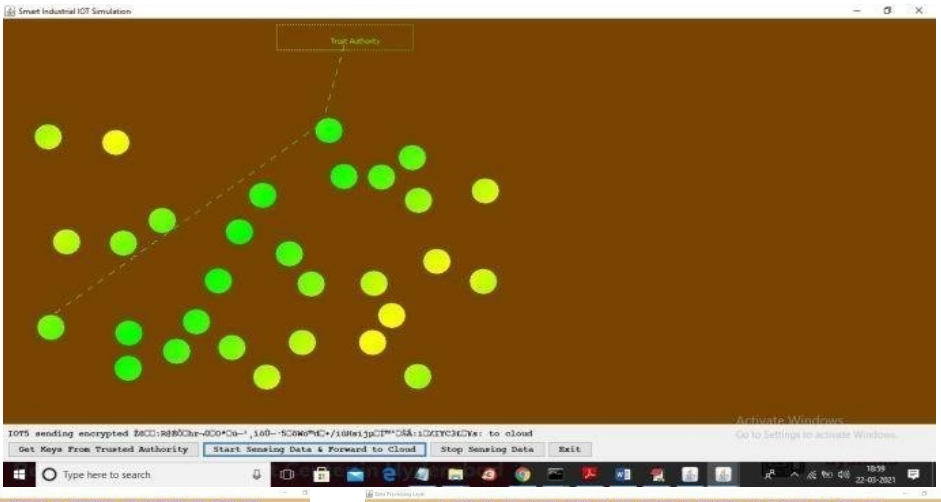
1) Generate random value or authorized user id
2) Generate master key
3) Generate secret key by combining masterkey and user id
4) Extract public key and private fromsecret key
5) IOT will encrypt data by using publickey
6) Authorized user can decrypt data by using private key
7) Above steps will repeat for proxyre-encryption

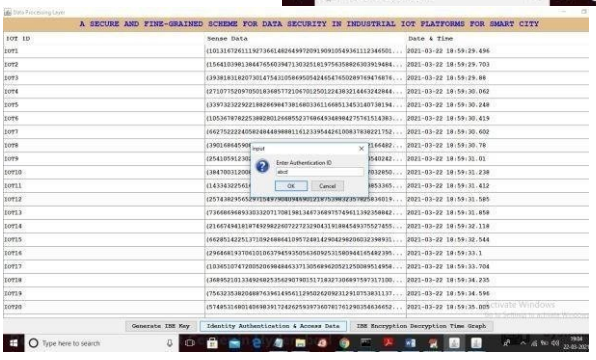
4. RESULTS AND DISCUSSION

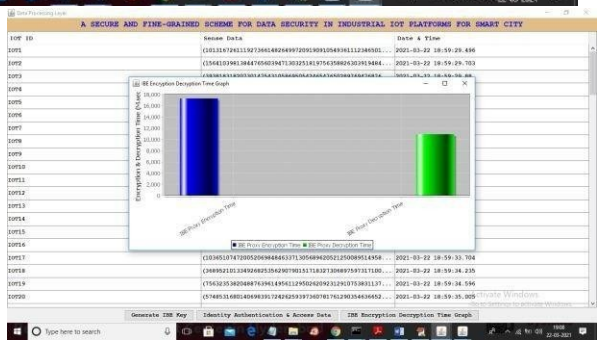
In above screen data processing layer startedand now click on 'Generate IBE Key' buttonto generate keys and to get below screen











In above screen in dialog box we can see authentication id and java key pair security to encrypt and

decrypt data and from above dialog just copy or remember authentication id so while access data youcan give this key to decrypt data otherwise it will not decrypt and in above dialog the authentication id is 'amci1f' and after saving authentication id you can click on 'OK' button and now double click on 'run.bat' file from 'Device Layer' folder to get below screen In above screen enter number of IOT devices which I enter as 30 and then click on 'Show Simulation' button to get below screen

In above screen each IOT will sense data and then send to cloud and it will send data in encrypted format and in above screen in before buttons you can read IOT sending encrypted data to cloud and this data will bereceived by first data processor screen. See below screen and in any time in above screen you can click on 'Stop Sensing Data'to stop sending data to cloud. Now see below screen

In above screen application asking forauthentication id and I gave wrong id as'abcd' and now click OK button to get below response

In above graph x-axis represents encryptiondecryption names and y-axis represents total time taken to encrypt and decrypt data.

5. CONCLUSION

In this paper, we go over specific types of industrial IoT manipulative structures and the difficulties they pose, as well as a comprehensive examination of the threats to their security. Current research is unable to provide a common protection mechanism for the various industrial IoT manage structures and protocols. As a result, the safety requirements that industrial IoT manage structures ought to meet are outlined and specific industrial IoT manage structures are summarized into an everyday model in this paper. We design an environment-friendly method to impenetrable data in industrial IoT control systems based on this established model and identity-based groupable conditional proxy re-encryption. Theoretically, wedemonstrate that our plan correctly prevents the four types of attacks we define. Our method only introduces a small amount of overhead when evaluating performance. We provide a summary of users' journeys and scheme graph concepts, offering suggestions for the investigation of impenetrable and environmentally friendly industrial IoT device scheme in the future.

REFERENCES:

1. Y. Liao, E. D. F. R. Loures, and F. Deschamps, "Industrial internet of things: A systematic literature review and insights," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4515–4525, 2018.
2. K. K. Zame, C. A. Brehm, A. T. Nitica, C. L. Richard, and G. D. Schweitzer III, "Smart grid and energy storage: Policy recommendations," Renewable and Sustainable Energy Reviews, vol. 82, pp. 1646– 1654,

2018.

3. G. Cheng, L. Liu, X. Qiang, and Y. Liu, "Industry 4.0 development and application of intelligent manufacturing," in 2016 international conference on information system and artificial intelligence (ISAI), pp. 407–410, IEEE,2016.

4. B.V.S Uma Prathyusha, K.Ramesh Babu, "A Node Monitoring Agent based Handover Mechanism for Effective Communication in Cloud Assisted MANETs in 5G", International Journal of Advanced Computer Science and Applications(2022), Vol. 13, No. 1, 2022, 128-136.

5. M. Rajaiah and A. Sudhakaraiah (2015): Unsteady MHD free convection flow past an accelerated vertical plate with chemical reaction and Ohmic heating, International Journal of Science and Research, Vol. 4 (2), pp. 1503-151

6. Z. H. Sun and X. Tian, "Scada in oilfields," Measurement and Control, vol.43,no. 6, pp. 176–178, 2010.

7. M. A. Pisching, F. Junqueira, D. J. Santos Filho, and P. E. Miyagi, "Service composition in the cloud-based manufacturing focused on the industry 4.0," in Doctoral Conference on Computing, Electrical and Industrial Systems, pp. 65–72,Springer, 2015.

8. Penchalaiah, N. and Seshadri, R. "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)", International Journal of Computer Science and Engineering, Vol. 02, No. 05, 2010, 1641-1645.

9. Mrs. B. Umamaheswari, B. Hareesh, "**A Method For Assessing Vulnerabilities In Ecommerce Transaction Systems**", Journal of Engineering Sciences, Vol 15, Issue 08, ISSN:0377-9254, 2024.

10. D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, "Security for industrial communication systems,"Proceedings of the IEEE, vol. 93, no. 6, pp. 1152–1177, 2005.

11. H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges,solutions and opportunities," IEEE Network, vol. 32, no pp. 144–151,2018.

12. T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for modbus rtu and ascii industrial control systems," in 2012 45th Hawaii International Conference on System Sciences, pp. 2338–2345, IEEE, 2012.

13. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machinelearning-based network vulnerabilityanalysis of industrial internet of things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822– 6834, 2019.

14. H. Li, Y. Yang, Y. Dai, J. Bai, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.