Shodhasamhita : Journal of Fundamental & Comparative Research
Vol. VIII, No. 1(X) : 2021
ISSN: 2277-7067

DATA SECURITY PROTECTION AND OVERALL PERFORMANCE USING A SECURED AND FINE GRAINED SYSTEMS IN INDUSTRIAL IOT PLATFORM

[1]P Kalyani, [2]G. Sudarsanam, [3]V. Mahesh Kumar, [4]K.Sumathi
[1,2,3]Dept of Computer Science and Engineering, Sree Venkateswara College of Engineering, Nellore (Dt), Andhra Pradesh, India.
[4]Dept of Electronics and Communication Engineering, Sree Venkateswara College of Engineering, Nellore (Dt), Andhra Pradesh, India.

ABSTRACT
Due to the enormous success of IoT devices, industrial IoT platforms, such as smart factories and oilfield industrial control systems, have emerged as a new trend in the creation of smart cities. Despite the fact that many manufacturers pay close attention to the unique functional needs of IoT platforms, they seldom look into security issues, particularly those related to data protection, which has led to a sizable number of instances of privacy leakage. Several initiatives have been undertaken to offer safe and dependable communication options for industrial IoT systems; nevertheless, these solutions are mostly dispersed and fragmented since different communication protocols and interaction styles are employed in diverse scenarios. As a result, creating a sizable, tightly integrated cross-platform system is a crucial challenge for industrial IoT systems. In this essay, we examine the wisdom and requirements of unique industrial IoT scenarios in order to abstract them into a general model. We list the potential attacks on specific industrial IoT structures and design a defence strategy to counter them that is entirely based on the conditional proxy re-encryption primitive. The suggested system makes sure that unauthorized users can't access information. The trial results show that our plan can meet the performance and safety requirements while incurring minimal overhead when it comes to security and overall performance.
Key words : Protocols, Control systems, Cloud computing, Data security

1. INTRODUCTION

Undoubtedly, the growth of the IoT has accelerated the adoption of smart city technology. Consumers are increasingly focusing on industrial control systems rather than just smart home software. With remarkable advantages for remote monitoring, data gathering, and labour cost reduction, industrial IoT management has become a popular issue [1]. This has led to its widespread use in a variety of IoT manipulation scenarios, such as smart grid [2], digital oilfield [3], smart manufacturing facility [3], smart chemical company, and others. The centralised monitoring and administration of infrastructure is made possible by industrial IoT management software, which provides two-way communication between distant equipment and the manipulate end. Each industrial IoT structure has a different set of duties and tasks.

For instance, the smart grid and digital oilfield have both made substantial use of the Supervisory Control and Data Acquisition (SCADA) technology [4]. Sensors, Programmable Logic Controllers (PLC), and Remote Terminal Units (RTU) are also equipped to gather data and control facilities in the domain of infrastructure setup. Data are relayed verbally inside the community to a neighbouring community for processing. However, in scenarios like clever factory, the enormous amount of statistics and complex management logic force the records to typically be preliminary processed and analysed via a third-party cloud, and then provided to the relevant businesses or consumers [5].

The risk of information leakage in IoT systems is significantly increased by decentralised architecture and diverse utility requirements. Industrial businesses and the creators of industrial data exchange protocols, however, have not given the potential security issues enough attention [6]. Traditional high-risk industries include the oil and power grids; nevertheless, many data management and message transmission modules are suffering from serious attacks from both insiders and outsiders [7].

Common industrial IoT protocols, such Modbus, BACnet, and MQTT, are no longer built for data security [8], and they frequently have issues with identity verification, data confidentiality, and data integrity testing. This puts information from business conversations vulnerable to eavesdropping, identity theft, and other assaults. In particular, Zolanvari et al. [9] examined the vulnerability of the widely used protocols in the context of the industrial IoT, including backdoor, buffer overflow, and other vulnerabilities that may potentially give attackers the opportunity to launch attacks.

2. REVIEW OF LITERATURE

Off-site data storage is a cloud service that frees users from having to concentrate on their records storage systems. It is described in DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party by authors M. Ali, S. Malik, and S. Khan. However, there are significant safety risks when outsourcing records to a third-party administrative system. Additionally, data leaking may occur as a result of attacks by other cloud users and computers. A problem that arises in the cloud context is the wholesale distribution of statistics by cloud carrier issuers.

We (a) implement a working DaSCE prototype and evaluate its performance entirely based on the time consumed during multiple operations, (b) formally model and analyse DaSCE's operation using High Level Petri nets (HLPN), and (c) confirm DaSCE's operation using the Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The findings demonstrate that DaSCE may be successfully utilised for outsourced data security through key management, access control, and file specific destruction.

Using fully anonymous attribute-based encryption, you may manage the access privileges and anonymity for cloud data. Wan, Z., Li, X. Y., Jung, T., and Wan, M. Cloud computing is a cutting-edge paradigm for computing that enables flexible, on-demand, and cost-effective utilisation of computer resources. However, because the data is outsourced to certain cloud servers, many privacy concerns result. To completely secure cloud storage, a number of Attribute-Based Encryption-based techniques have been put forth.

However, the majority of effort focuses on data content privacy and access control, with far less attention dedicated to privilege control and identity privacy. In this research, we provide a semi-anonymous privilege control technique called Anony Control to address both the information privacy and the customer identifying privacy in current access control schemes. Achieving semi-anonymity, AnonyControl decentralises the central authority to limit identity leaks.

Two-Factor Access Control with Fine Grained Control for Web-Based Cloud Computing Services, Huang X, Lu, R., Li, J., Liu, J. K., Au, M. H., and Lu We present a novel fine-grained two-factor authentication (2FA) access control mechanism for web-based cloud computing services in this study. In particular, our suggested 2FA access control system applies an attribute-based access control method with the need for both a personal secret key and a lightweight security device.

The approach can improve system security, especially in circumstances where multiple users use the same computer for web-based cloud services because a user cannot access the device if they don't maintain both. Additionally, attribute-based control of the device enables the cloud server to prevent access to users who have the same set of attributes while maintaining user privacy. In other words, the cloud server only knows that the user satisfies the necessary criteria and is unaware of their precise identity. Finally, in order to demonstrate the viability of our suggested 2FA system, we also carry out a simulation.

3. PROPOSED SYSTEM

Today, 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 the air conditioning, and if no humans are detected, then the IOT sensor turns off the air conditioning. In a similar manner, sensors will open doors when known people arrive at the gate. Such homes are known as smart homes that form smart cities.

Due to the success of IOT in smart cities, the industrial sector has begun using IOT sensors to control their machinery. SCADA is a technology used in the industrial sector to monitor oil well conditions without the need for human assistance. This technology uses plain text and communication protocols to send sense data

to a centralised server. Often, IOT will use cloud servers to process data. These servers send this data to the cloud in plain text format, which can be misused by cloud internal employees and occasionally some hacking.

In order to secure this IOT data, this study employs FINEGRAINED Identity Based Encryption, which only allows authenticated users to access IOT data and encrypts data using keys created by IBE algorithm. All current solutions were focused on efficient communications but did not give security to IOT data.The following layers make up this proposed technique: Device Layer: This layer is made up of IOT devices that include PLC and RTU units and are in charge of handling user requests. This layer accepts user requests and sends created or sense data to the users who made the request. Data will be encrypted by this layer using IBE keys obtained from trusted authorities.

A data user or data processor who has the appropriate identification and authentication keys can decrypt data.

Data Processing Layer

Only authorized users with valid keys can send requests for IOT data, and then those users can decrypt the data with those keys when it has been sensed or created by IOT.

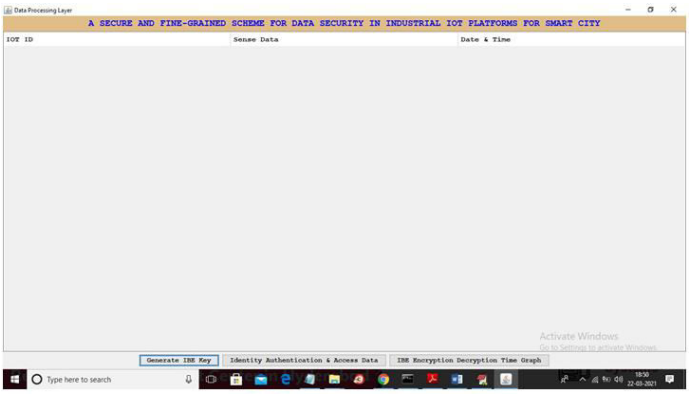
Data Forwarding Layer: To connect to the internet, SCADA System IOT devices will use network communications like WIFY. Using this connection, they will send sense data to a cloud server in encrypted format. The cloud will then apply some logic to remove any redundant and garbage values before sending the data to workshops and businesses for additional processing or to monitor the condition of their machines.

We can see that the IBE encryption algorithm is used to secure the data in the top three layers. Only authorised users are permitted access to data, and only internal employees are permitted to view or otherwise abuse data. Since encrypted data is sent to cloud servers via IOT, the cloud itself cannot be stolen or understood from encrypted data.In order to protect IOT data from all three types of attackers, we proposed work.

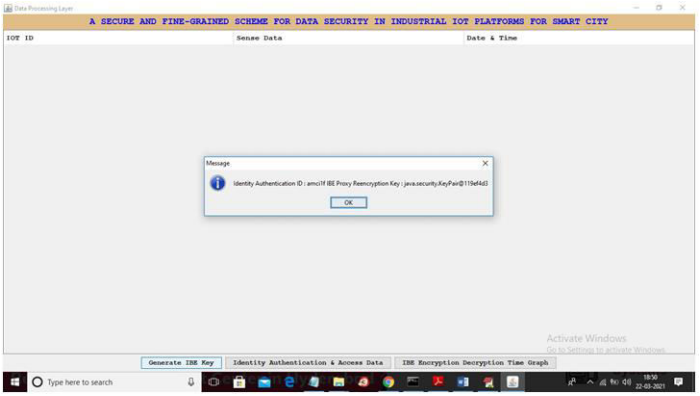
To generate IBE keys application perform below steps

- Generate random value or authorized user id
- Generate master key
- Generate secret key by combining master key and user id
- Extract public key and private from secret key
- IOT will encrypt data by using public key
- Authorized user can decrypt data by using private key
- Above steps will repeat for proxy re-encryption

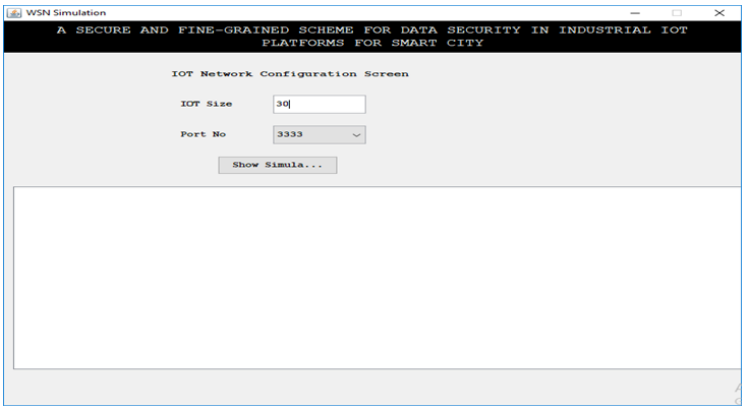
4. RESULTS AND DISCUSSION



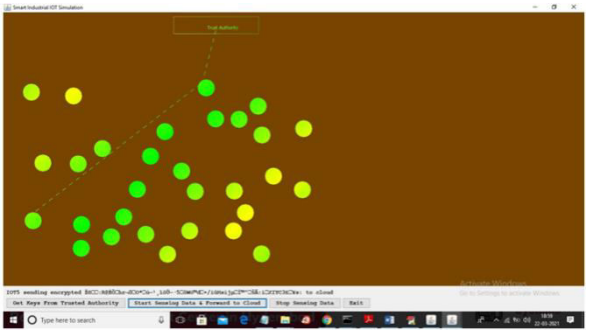
In above screen data processing layer started and now click on „Generate IBE Key‟ but onto generate keys and to get below screen



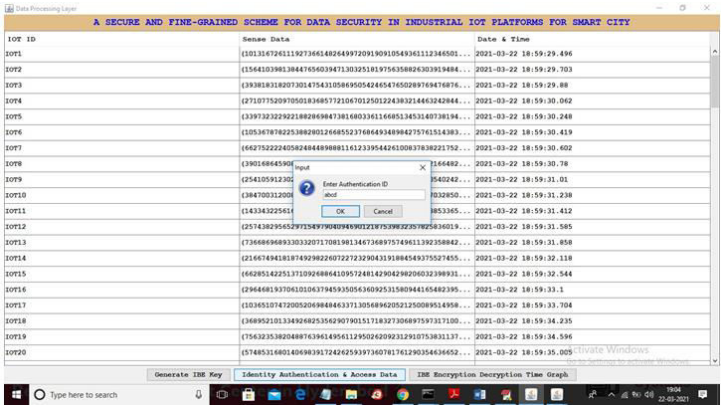
In above screen in dialog box we can see authentication id and java key pair security to encrypt and decrypt data and from above dialog just copy or remember authentication id so while access data you can give this key to decrypt data other wise it will not decrypt and in above dialog the authentication 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



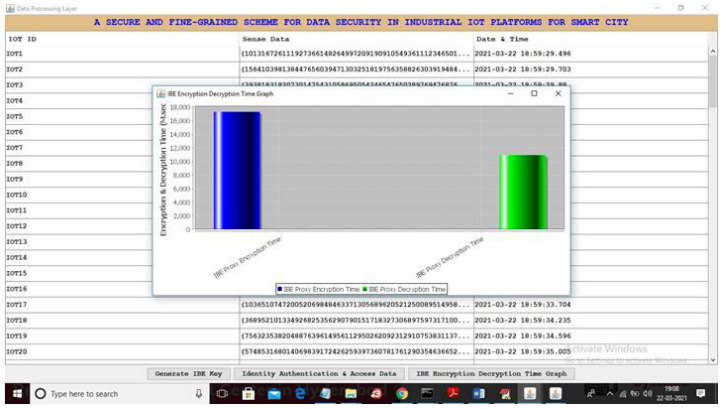
In above screen enter number of IOT devices which I enter as 30 and then click on „Show Simulation "button to get below screen



In above screen each IOT will sense data and then send to cloud and it will send data inencryptedformatandinabovescreeninbeforebuttonsyoucanreadIOTsending encrypted data to cloud and this data will be received 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 for authentication id and I gave wrong id as „abcd" and now click OK button to get below response



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

CONCLUSION

In this essay, we discuss several industrial IoT manipulation structure types, discuss their difficulties, and conduct a thorough analysis of their security risks. Current research cannot offer a universal protective strategy for industrial IoT manage structures because to the variety of manage structures and the complexity of the protocols employed. Determining the safety requirements that industrial IoT manage structures must fulfil, we summarise various industrial IoT manage structures into an everyday model in this study. We provide a secure and efficient method to protect data in industrial IoT control systems based on this proven model and identity-based groupable conditional proxy re-encryption. We theoretically demonstrate that our plan can successfully thwart the four assault types we identify. Our method only adds a little amount of overhead when analysing performance. We present a summary of user experience and scheme graph concepts, which offer guidance for the investigation of impermeable and eco-friendly industrial IoT manipulation device scheme in the future.

REFERENCES

1. Y. Liao, E. D. F. R. Loures, and F.Deschamps, "Industrial internet of things:Asystematicliteraturereviewandinsights,"IEEEInternetofThingsJournal,vol.5,no.6,pp.4515–4525,2018.
2. K.K.Zame,C.A.Brehm,A.T.Nitica,C.L.Richard,andG.D.SchweitzerIII,"Smartgridandenergystorage:Policyrecommendations,"RenewableandSustainableEnergyReviews,vol. 82, pp. 1646– 1654, 2018.
3. G. Cheng, L. Liu, X. Qiang, and Y.Liu,"Industry4.0developmentandapplication of intelligent manufacturing,"in2016internationalconferenceoninformationsystemandartificialintelligence (ISAI), pp. 407–410, IEEE,2016.
4. Z.H.SunandX.Tian,"Scadainoilfields," Measurement and Control, vol.43, no. 6, pp. 176–178, 2010.

5. M. A. Pisching, F. Junqueira, D. J.Santos Filho, and P. E. Miyagi, "Servicecompositionintheclou-basedmanufacturingfocusedontheindustry4.0,"inDoctoralConferenceonComputing,ElectricalandIndustrialSystems,pp. 65–72,Springer, 2015.
6. D.Dzung,M.Naedele,T.P.VonHoff,andM.Crevatin,"Securityforindustrialcommunicationsystems,"Proceedings of the IEEE, vol. 93, no. 6,pp.1152–1177, 2005.
7. H.Ren,H.Li,Y.Dai,K.Yang,and
8. X. Lin, "Querying in internet of thingswithprivacypreserving:Challenges,solutionsandopportunities,"IEEENetwork,vol.32,no.6,pp.144–151,2018.
9. T.Morris,R.Vaughn,andY.Dandass,"Aretrofitnetworkintrusiondetection system for modbus rtu and asciiindustrial control systems," in 2012 45thHawaiiInternationalConferenceon System Sciences, pp. 2338–2345, IEEE,2012.
10. M.Zolanvari,M.A.Teixeira,L.Gupta,K.M.Khan,andR.Jain,"Machinelearning-basednetworkvulnerabilityanalysisofindustrialinternetofthings,"IEEEInternetofThings Journal, vol. 6, no. 4, pp. 6822–6834, 2019.
11. H.Li,Y.Yang,Y.Dai,J.Bai,and Y.Xiang,"Achievingsecureandefficientdynamicsearchablesymmetricencryptionovermedicalclouddata,"IEEE Transactions on Cloud Computing,vol. PP, no. 99, pp. 1–1,2017.