IJMRSET

e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 5, Issue 6, June 2022

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.54

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506021 |

Securing IOT Devices against DOS Attacks

B. Pavithra[1], BH. Jyothi Sai[2], G. Reshma[3], Ch. Keerthi [4]

Dept. of Electronics and Communications Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

ABSTRACT: With the high popularity of IoT devices, industrial IoT platforms, such as smart factories and oilfield industrial control systems, have become a new trend in the development of smart city. Although various manufacturers pay wide attention to the different functional requirements of IoT platforms, they seldom consider security issues, especially in terms of data security, which has led to a large number of cases of privacy leakage. Some works have been made to provide secure and reliable communication solutions for industrial IoT platforms, unfortunately, as different communication protocols and interaction models are adopted in different scenarios, these solutions are mainly isolated and fragmented. Therefore, it is an urgent challenge to construct a universal cross-platform secure communication scheme for industrial IoT platforms. In this article, we analyze the logic and requirements of different industrial IoT scenarios to abstracts them into a universal model. We summarize the possible attacks on different industrial IoT platforms and design a security scheme to capture these attacks based on the conditional proxy re-encryption primitive. The proposed scheme ensures that data cannot be accessed by an unauthorized user. We also evaluate the security and performance of our scheme, and the experimental results show that our scheme can achieve the functionality and security requirements with low overhead.

I. INTRODUCTION

Cloud Computing refers to each the applications delivered as services over the web and also the hardware and computer program within the datacenters that give those services. The services themselves have long been named as computer code as a Service (SaaS). The datacenter hardware and computer code is named as a cloud once a Cloud is formed obtainable during a pay-as-you-go manner to the general public, it's referred to as a Public Cloud. The service being sold is Utility Computing. Current samples of utility Computing embrace Amazon net Services, Google App Engine, and Microsoft Azure. The term non-public Cloud id accustomed visit internal datacenters of a business or alternative organization that aren't created obtainable to the general public. Thus, Cloud Computing is that the total of SaaS and Utility Computing, however doesn't usually embrace non-public Clouds. Cloud Computing term is employed during a general manner, exchange it with one amongst the opposite terms only if clarity demands it.

As far as we know, few works can solve the commondata security problems of industrial IoT platforms on a largescale, which means that customized security requirementsgreatly increase the deployment cost and difficulty of different platforms. Therefore, we hope to propose a solution that canbroadly address data security risks faced by different industrial IoT platforms.

II. RELATEDWORK

In the era of smart city, the attack and security of IoT control system has become a hot issue. Due to its wide coverage and low security, industrial IoT control systems often cause huge losses after being attacked. Pollet et al. conducted more than 100 security assessments on SCADA, EMS, DCS, AMI and smart grid systems, and the main cause of SCADA incidents was enterprise IT network traffic and third-party network interconnection. Security in industrial IoT systems was not an issue when industrial IoT protocols were first introduced. As a result, common protocols such as MODBUS, Ethernet/IP, DNP 317, and iso-tsap do not provide confidentiality, authentication, or data integrity at runtime, making them vulnerable to various attacks.In order to solve the security problems in industrial IoT control systems, many solutions have been proposed. Sun et al. Developed a network physical monitoring system (CPMS) to detect intelligent meter intrusion and bad data injection attacks. Celik et al. Introduced SAINT, a static pollution analysis tool for Internet of things applications, to assess the security and privacy risks of IoT devices, but it does not guarantee data security over links. Mahmood et al. Proposed a hybrid lightweight authentication scheme based on diffie-hellman and ensured message integrity, however, he did not consider the security of intermediate nodes. Lin et al. Proposed a blockchain-based security mutual authentication system BSeIn to implement fine-grained access control strategy, but the overhead of BSeIn can not be ignored in most industrial IoT control systems. Esfahani et al.proposed a lightweight authentication mechanism based on hash and XOR operations for M2M communication in industrial IoT environments, but this scheme cannot even guarantee secure key negotiation. Saxena et al. proposed an authentication and authorization scheme for smart grid, which can effectively prevent various internal and external attacks on different devices. However, due to weak password attacks and other problems, this scheme cannot effectively identify the attacked malicious devices.

III.OVERVIEW OF INDUSTRIAL IOT CONTROL SYSTEMS

A large number of industrial IoT systems use proprietary communication protocols based on functional requirements and scenarios. There are dozens of common industrial IoT protocols, which are applied in different industrial IoT control scenarios. Common industrial IoT control systems can be roughly divided into two categories: one is SCADA system represented by smart grid and digital oilfield; the other is industrial IoT control system based on cloud platform represented by intelligent factory.

A.SCADA system

In general, there are two main roles in the SCADA system, center and periphery. Peripheries are the data holders, usually the infrastructure. In the case of digital oilfields, peripheries are oil wells. In order to ensure the normal operation of the well, a large number of sensors are distributed in the well for sensing field data. In addition, each infrastructure in theacquisition site is also equipped with PLC and RTU for converting electrical signals into digital signals, processing data and controlling equipment. The center is the data requester or command initiator. The data interaction between the controller and the monitoring center is generally transmitted by wireless network. Under normal circumstances, unified monitoring and control is managed by the monitoring center, and the authority is distributed to different operators to supervise the infrastructure in different areas.Fig.1 shows the architecture of the SCADA system.

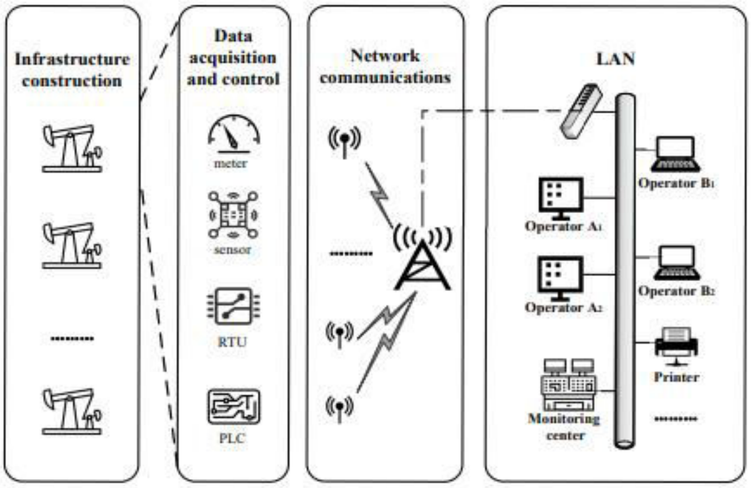


Figure1. Architecture

B. Cloud-based industrial IoT control system

The operation of intelligent factory and smart home equipment is a typical cloud-based industrial IoT control system. Intelligent factory uses the technology of Internet of things and equipment monitoring technology to strengthen information management and service, and realizes the unmanned management of workshop. As shown in Fig. 2, each assembly line in different workshops is equipped with a workshop controller, which is responsible for issuing workshop production conditions and receiving instructions. Because there are many companies involved in industrial production, centralized management cannot be realized. Therefore, the workshop controller is connected to the cloud, and the cloud connects to corporate networks. The cloud performs preliminary processing and analysis of the data, and delivers the data to the corresponding company and workshop for further processing. The underlying equipment in SCADA system is often weak and needs to be equipped with data acquisition and control devices in the field. However, the cloud-based industrial IoT control system adds the cloud, which transfers some computing tasks to the cloud to reduce the burden on the monitoring center.

IV. ATTACKS

A. Unsafe industrial IoT protocols

Most industrial IoT protocols are designed only to consider different application scenarios, functional requirements, and operational efficiency, without considering security issues. As an industry standard protocol, Modbus also has the following problems.

Lack of identification. This means that an attacker only needs to find a valid address to set up a Modbus session.

Lack of authorization. This means that there is no classification among users and no division of users' rights, whichgreatly increases the possibility of internal attacks.

Lack of data encryption mechanism. Data is transmitted in plaintext form, so it is easy for an attacker to intercept and parse the data. Since there are so many industrial IoT protocols, we cannot even fix these security problems by uniform protocol modification.

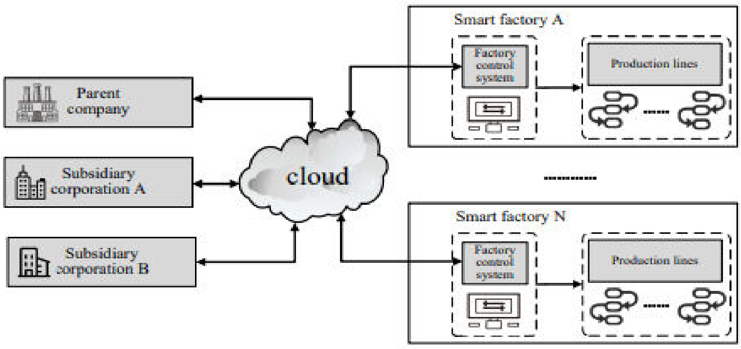


Figure 2: The architecture of cloud-based industrial IoT control system.

B. Weak password security configuration

This problem is more serious in the industrial IoT control system, which has a lot of infrastructure, industrial control router, PLC, RTU, HMI application software and so on. Because these devices are scattered and cannot be protected at the physical level, this means that the weak password problem is undoubtedly a vulnerability in industrial IoT control systems . We actually surveyed 11 companies, but only received samples of 23 devices from 6 companies. we consider an empty password, a default password, and a pure numeric password of less than 8 bits as weak passwords. 18 of them adopt weak passwords.Pure numeric passwords of less than 8 bits may be a high threshold, but of the 18 weak passwords we collected, nine used pure numeric passwords of less than eight bits, and four of them had very simple logic. In other words, at least 13 of 23 devices adopt weak passwords, which is still a large number.

C. The possibility of internal attacks

After data flows through the wireless network and reaches the company's LAN, it is piled up in the temporary storage area of data, waiting for the corresponding monitor to extract and process. However, as shown in Fig. 3, existing industrial IoT protocols do not set the division of user rights, and few corporate networks partition data in advance, which means that all users in the LAN can access any piece of infrastructure information. In fact, different groups of operators handle messages from equipments of different areas.They should not access other equipment information without authorization. In addition, since there are low-security devices in the internal network, such as printers and routers, attackers can also read the data of the internal network byattacking low-security devices.

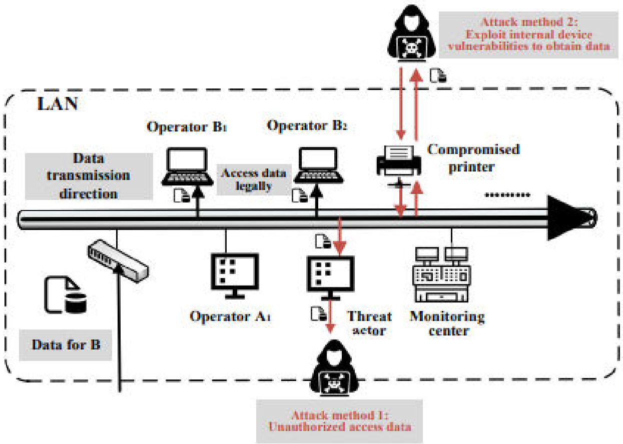


Figure. 3: Internal attack mode

D. Unreliability of cloud platform

Many industrial IoT control systems make use of cloud to carry out preliminary data analysis and transfer to corresponding equipment and users in order to achieve efficient data management. However, data in industrial IoT control systems is not encrypted, which means that the data stored and processed in the cloud is plaintext. Therefore, as a thirdparty platform, the cloud can obtain all the private data flowing through it. The number of cases of enterprise losses caused by data leakage from the cloud increases year by year, and has gradually become one of the key security issues concerned by the network community.

E. Insecure remote support

Infrastructure is often distributed in a wide range of areas, and the configuration, update, debugging, maintenance and other work of on-site equipment is often handed over to thirdparty technicians and partners. In this case, the interface of the device to the external network cannot be avoided, and the virus can invade the system through these interfaces, resulting in data leakage. In addition, industrial IoT protocols often do not have default authentication and data encryption mechanisms. This directly causes an attacker to use network sniffing tools to find vulnerable external interfaces based on these unencryptedRemote Procedure Call instructions to carry out attacks such as injecting malicious information worms.We want to defend against the four possible attacks we define in the previous section without affecting the system’s function and performance. Since industrial IoT control systems are often based on different protocols, our scheme cannot be based on a particular communication protocol.In order to design a universal scheme for various industrial IoT control systems, we abstract these application scenarios into a unified model, which is divided into three layers: equipment layer, data forwarding layer and data processing layer

V. IMPLEMENTATION

The highest-privileged user H first distributes the keys to the operators and infrastructures as the trusted user. Specifically, H first runs Setup function to generate a system public key PK and a master secret key MK. Based on the ID of each infrastructure and user, he uses KeyGen to generate private key SK for them, and informs each infrastructure and user of SK and PK. At this point, each user and infrastructure has its own public-private key pair. Since the infrastructure of different regions is managed by different operation groups, H needs to configure access control permissions for the infrastructure of different regions in the initialization phase. Specifically, taking group A as an example, H first defines the condition set CA={t, IDA} for group A to limit the time how long members of group A can access XA. The conditional set is signed and encrypted to IDXA [σH(CA), PK] and sent to the infrastructure XA. Infrastructure XA uses the private key to decrypt and verify signatures to obtain the conditional set CA, which is set to encrypt the default condition set. At the same time, H performs IBE.ReKeyGen1 and IBE.ReKeyGen2 by using the identity information of all users in group A and group A, and generates the re-encryption key RK for each member of group A and group A, which is then encrypted and sent to the data forwarding layer. The data forwarding layer decrypts and records RK. H completes initialization after similar treatment for all infrastructures.

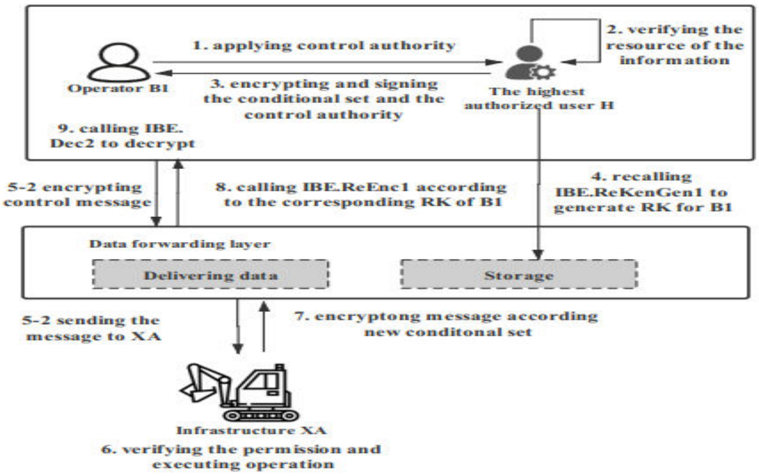
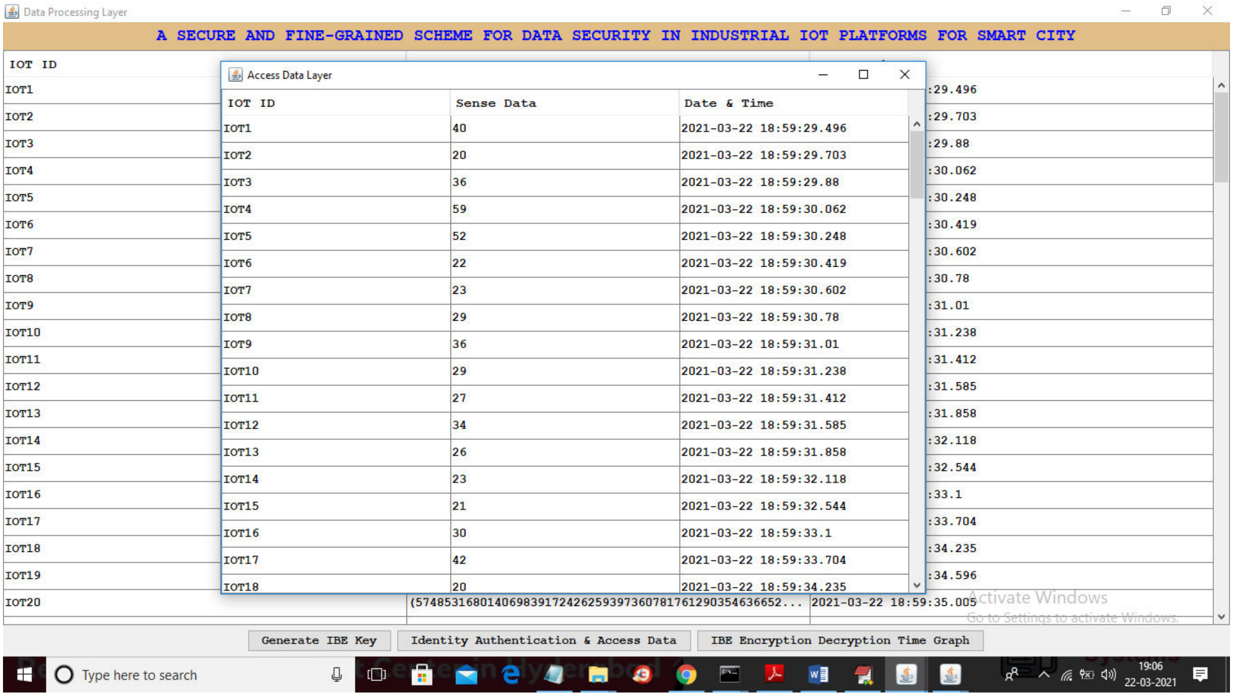

1. applying control authority
2. verifying the resource of the information
Operator B1
3. encrypting and signing the conditional set and the control authority
The highest authorized user H
9. calling IBE. Dec2 to decrypt
5-2 encrypting control message
8. calling IBE.ReEnc1 according to the corresponding RK of B1
4. recalling IBE.ReKenGen1 to generate RK for B1
Data forwarding layer
Delivering data
Storage
5-2 sending the message to XA
7. encryptong message according new conditonal set
Infrastructure XA
6. verifying the permission and executing operation

Figure 5: Temporarily authorized user control infrastructures.

VI. RESULTS AND DISCUSSION

Here we can see the result of our scheme i.e., the decrypted data from the encrypted data which is converted to provide security from Attacks:


Data Processing Layer
A SECURE AND FINE-GRAINED SCHEME FOR DATA SECURITY IN INDUSTRIAL IOT PLATFORMS FOR SMART CITY
Access Data Layer
Generate IBE Key
Identity Authentication & Access Data
IBE Encryption Decryption Time Graph
Type here to search
19:06
22-03-2021
Activate Windows
Go to Settings to activate Windows.

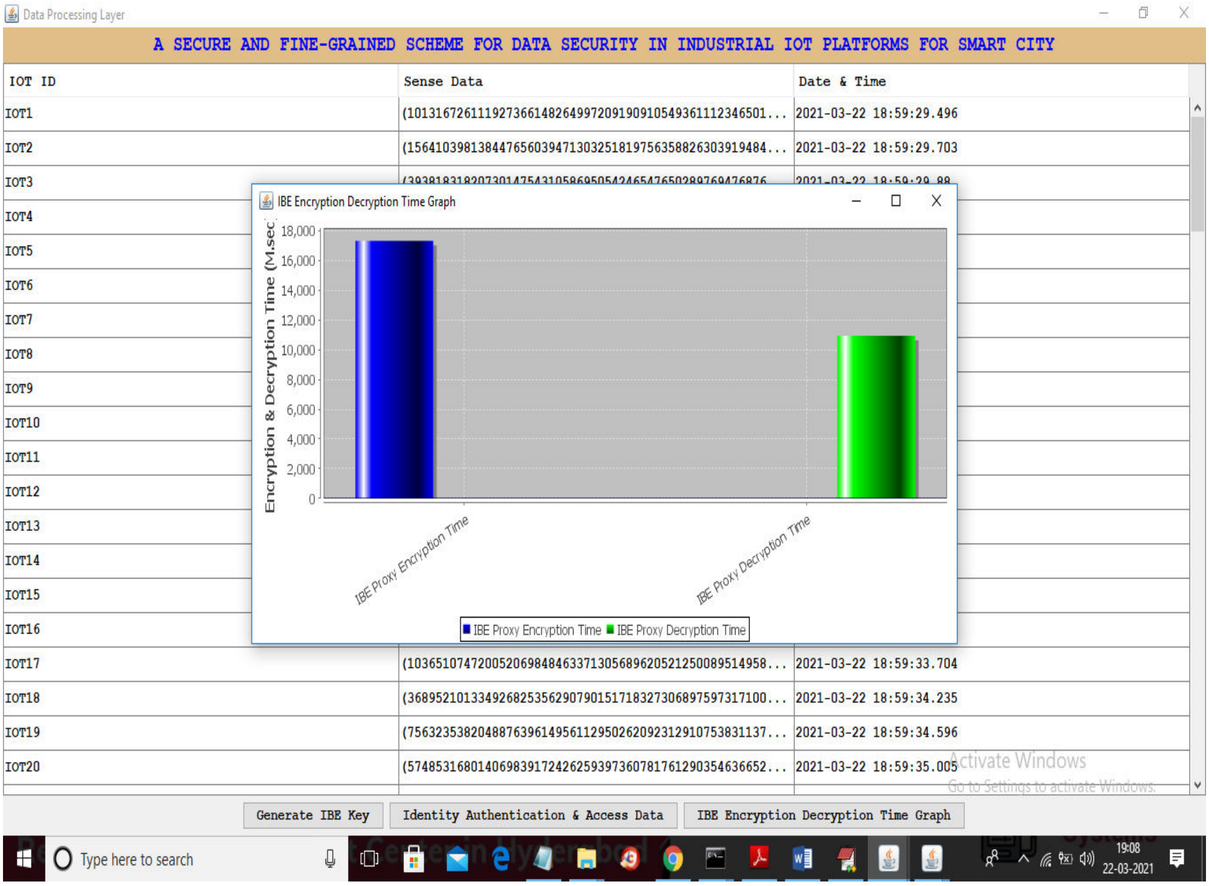
IOT ID	Sense Data	Date & Time
IOT1	40	2021-03-22 18:59:29.496
IOT2	20	2021-03-22 18:59:29.703
IOT3	36	2021-03-22 18:59:29.88
IOT4	59	2021-03-22 18:59:30.062
IOT5	52	2021-03-22 18:59:30.248
IOT6	22	2021-03-22 18:59:30.419
IOT7	23	2021-03-22 18:59:30.602
IOT8	29	2021-03-22 18:59:30.78
IOT9	36	2021-03-22 18:59:31.01
IOT10	29	2021-03-22 18:59:31.238
IOT11	27	2021-03-22 18:59:31.412
IOT12	34	2021-03-22 18:59:31.585
IOT13	26	2021-03-22 18:59:31.858
IOT14	23	2021-03-22 18:59:32.118
IOT15	21	2021-03-22 18:59:32.544
IOT16	30	2021-03-22 18:59:33.1
IOT17	42	2021-03-22 18:59:33.704
IOT18	20	2021-03-22 18:59:34.235

IOT ID		
IOT1		:29.496
IOT2		:29.703
IOT3		:29.88
IOT4		:30.062
IOT5		:30.248
IOT6		:30.419
IOT7		:30.602
IOT8		:30.78
IOT9		:31.01
IOT10		:31.238
IOT11		:31.412
IOT12		:31.585
IOT13		:31.858
IOT14		:32.118
IOT15		:32.544
IOT16		:33.1
IOT17		:33.704
IOT18		:34.235
IOT19		:34.596
IOT20	(5748531680140698391724262593973607817612903546366 52...	2021-03-22 18:59:35.005

Figure 6: Decrypted Sense Data

Now in Figure 6, we can see that all encrypted values in second column are decrypted into original text file and showing valid temperature values. Here we can see the original text data or sense data. Here we can also observe the data and time of the sensed data. Now close the above screen and click on 'IBE Encryption Decryption Time Graph' button to get below graph. This graph shows the time taken for the encryption and decryption process. From this below graph we can observe how efficiently this scheme is securing IoT devices from attacks.

In Figure 7, x-axis represents encryption decryption names and y-axis represents total time taken to encrypt and decrypt data.We also evaluate the security and performance of our scheme, and the experimental results show that our scheme can achieve the functionality and security requirements with low overhead.Finally, we construct a universal security scheme by using the identity-based groupable conditional proxy re-encryption primitive. The results show that this scheme can realize the data security of smart control with low overhead.We analyze the logic and requirements of different industrial IoT scenarios to abstracts them into a universal model. We summarize the possible attacks on different industrial IoT platforms and design a security scheme to capture these attacks based on the conditional proxy re-encryption primitive. The proposed scheme ensures that data cannot be accessed by an unauthorized user.


Data Processing Layer
IBE Encryption Decryption Time Graph
Encryption & Decryption Time (M.sec
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
IBE Proxy Encryption Time
IBE Proxy Decryption Time
■ IBE Proxy Encryption Time ■ IBE Proxy Decryption Time
Generate IBE Key
Identity Authentication & Access Data
IBE Encryption Decryption Time Graph
Type here to search
19:08
22-03-2021
Activate Windows
Go to Settings to activate Windows.

A SECURE AND FINE-GRAINED SCHEME FOR DATA SECURITY IN INDUSTRIAL IOT PLATFORMS FOR SMART CITY

IOT ID	Sense Data	Date & Time
IOT1	(101316726111927366148264997209190910549361112346501...	2021-03-22 18:59:29.496
IOT2	(156410398138447656039471303251819756358826303919484...	2021-03-22 18:59:29.703
IOT3	(393818318207301475431058695054246547650289769476876	2021-03-22 18:59:29.88
IOT4		
IOT5		
IOT6		
IOT7		
IOT8		
IOT9		
IOT10		
IOT11		
IOT12		
IOT13		
IOT14		
IOT15		
IOT16		
IOT17	(103651074720052069848463371305689620521250089514958...	2021-03-22 18:59:33.704
IOT18	(368952101334926825356290790151718327306897597317100...	2021-03-22 18:59:34.235
IOT19	(756323538204887639614956112950262092312910753831137...	2021-03-22 18:59:34.596
IOT20	(574853168014069839172426259397360781761290354636652...	2021-03-22 18:59:35.005

Figure 7: IBE encryption decryption time graph

VII.CONCLUSION

In this paper,The proposed algorithm uses different types of industrial IoT control systems and their challenges, and analyze the security threats of industrial IoT control systems in detail. Due to the variety of industrial IoT control systems and the complexity of the protocols used, existing works cannot provide a common security mechanism for them. Therefore, in this paper, we abstract different industrial IoT control systems into a universal model, and define the security requirements that industrial IoT control systems should meet. Based on this universal model and identity-based groupable conditional proxy re-encryption, we design a secure and efficient scheme to secure data in industrial

IoT control systems. We prove theoretically that our scheme can effectively prevent the four kinds of attacks we define. In evaluating performance, our scheme introduces only minimal overhead. We summarize users' experience and scheme design ideas, which provide inspiration for the future exploration of secure and efficient industrial IoT control system scheme

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] Z. H. Sun and X. Tian, “Scada in oilfields,” 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, “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.
[6] 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.
[7] 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. 6, pp. 144–151, 2018.
[8] 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.
[9] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, “Machine learning-based network vulnerability analysis of industrial internet of things,” IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822–6834, 2019.
[10] 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.