Multi Dimensional Framework For Securing Industrial Internet of Things

Mrs.A. Hemalatha, M.E.,[1], T.Bhuvaneshwari[2]
[1]Assistant Professor, Dept of CSE
[2]Dept of CSE
[1, 2] SembodaiRukmaniVaratharajanEngg College, Sembodai, Nagapattinam-614-809

Abstract- *Many of the industries such as manufacturing, F&B, transportation have recently shown a growing interest in Industry Internet of things (IIoT) to gain competitive advantage. The IIoT is technology stack of combining internet of things, machines, computers and people enabling intelligent business transformational through advanced big data analytics. With the growing complexity of IIoT in a large-scale interconnectivity deployment, access control and authorization of IIoT objects such as smart devices, human or computers becomes the pressing requirements. It supports multi-dimension and large data processing with flexible and efficient authorization model to meet new security the authorization model works efficiently in a large-scale deployment to meet new IIoT security requirements needs of IIoT. In order to demonstrate the validity of the proposed framework, a prototype is implemented with test results.*

Keywords- Industry Internet of Things (IIoT), Multidimension, Authorization

I. INTRODUCTION

Many enterprises have recently shown a growing interest in IIoT which refers to all activities performed by businesses to model, monitor and optimize their business operations through insights collected from thousands of connected internet of things, machines, computers and people to assist them in gaining competitive advantage. An Industry Internet of Things as its name implies, is a concept that proactively manages how smart devices, computers, applications and people, behave in holistic end-to-end industry processes across one or more systems using advanced big data analytics.

With the growing complexity of IIoT, it is facing withtremendous uncertainty due to its internal complexity and large scale interconnectivity. There is an urgent need to ensure its compliance, reliability and security during IIoT design and runtime.

- Only the owner has full rights to control the process.
- Each of them in the process has to do any work and no one can be idle.
- Authorization framework can answer all the security queries in the IIoT context.
- Each and every data in the database can be fully monitored.

Enterprises has large metadata that is to be stored in the database and every data should ensure security.

Smart devices also connected and share information between them with the permission of the authorized person and unknown person cannot access the database.

II. OVERVIEW OF APPROACH

2.1 Password-Based Authentication

Password-based authentication is the most widely used proof of identity for people to interact with a device or a system. It belongs to the bucket as shown in the above diagram, and allows managing multiple levels of account privileges. In addition to the client-server applications, passwords are also used as secrets for securing access to operating system resources.

Password-based authentication was never designed for the M2M world and, as such, this method presents multiple challenges for IIoT deployments.

Some of the concerns are as follows:

- Scalability
- Managing passwords
- Secured storage
- Defaulter syndrome

2.2 Biometrics

The use of biometrics as an authentication factor is becoming more and more common. Biometrics not only

provides the convenience of password-less authentication, but can also be used as a second factor in multi-factor authentication schemes. Fingerprints, facial geometry, voiceprints, etc. are various unique attributes used in biometrics-based authentication.

Biometric security companies such as Hyper (www.hypr.com) are promoting the concept of decentralized biometric tokenization.

Biometrics-based security, also known as Bio-T, is finding faster adoption in the consumer IoT use case,

2.3Multi-Factor Authentication

Multi-factor authentication is widely used in client-server sessions, and is also recommended for edge to cloud communications. IoT cloud providers such as AWS and Microsoft Azure use multi-factor authentication (primarily in human-to-machine use cases).

2.4 Key-Based Authentication

Key-based authentication is a fully automated authentication technique wherein encryption keys are used as secrets.

This method heavily relies on cryptographic algorithms.

Cryptography utilizes encryption algorithms to perform two basic operations:

1. Encryption: Converts information from its plaintext form into an encrypted version, known as cipher text, using encryption keys.
2. Decryption: Performs the reverse transformation, to transform the encrypted cipher text back into the plaintext format

2.5 Symmetric Keys

In symmetric key cryptography, the sender and receiver share a common secret to encrypt and decrypt messages. Unlike a password, in symmetric key-based authentication, keys are not required to be sent between the parties at the time of the authentication event. The keys are usually established before a session is initiated using a public key algorithm.

2.6Asymmetric Keys

Asymmetric cryptography, also known as public key cryptography, solves the scalability problem of symmetric cryptography by issuing a pair of keys one private and one public to each participant. The robustness of the public key-based approach depends on the degree of computational difficulty in deriving the private key using the public key.
Asymmetric cryptography is based upon the difficulty of solving complex mathematical problems.

2.7Zero-Knowledge Keys

The concept of proving the knowledge of an assertion without revealing any information about the assertion itself offers benefits over existing options such as shared key and public key cryptography.

In zero-knowledge cryptography, the prover is able to prove its knowledge of the secret to the authenticator without having to reveal the secret itself at any time during the operations. The authenticator can ask questions to confirm the prover indeed knows the secret, but it is impossible for the authenticator or any third party to discover information about the secret.

While using zero-knowledge key-based authentication, it is recommended to evaluate the complexity of the infrastructure matrix providing the service, resource requirements, ease of maintenance, and cost-effectiveness.

2.8 Certificate-Based Authentication

Certificate-based authentication goes a step further. It uses the public key cryptography framework, where the public key is signed by a trusted Certificate Authority (CA). The CA uses its private key to sign the requester's public key. This assures the remote endpoint that the originating endpoint has the private key and also serves as the proof of identity.

III. ANALYSIS

System analysis is the overall analysis of the system before implementation and for arriving at a precise solution.
Careful analysis of a system before implementation prevents post implementation problems that might arise due to bad analysis of the problem statement.

3.1Existing System

The existing techniques utilize the high memory for storage and take the more time for processing or just focus the particular constrained network or ignore the fine-grained

access control enforcement on the devices and local conditions.

3.2Proposed System

- An indexing framework for securing IIoT object with annotated metadata is presented. It allows the IIoT objects owners to define constraints such as time-constrained and location-constrained on the IIoT services in a fine-grained and flexible manner.
- The authorization model works efficiently and flexibly in a large-scale deployment to meet newly increasing IIoT security demands.
- The SecIIoT is an authorization framework that can answer security queries efficiently based on the requesters' roles in an Industrial Internet of Things context.

4. DESIGN AND IMPLEMETATION

System design concentrates on moving from problem domain to solution domain. This important phase is composed of several steps. It provides the understanding and procedural details necessary for implementing the system recommended in the feasibility study. Emphasis is on translating the performance requirements into design specification.

4.1Input Design

System design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development.

Input Design is the process of converting a user oriented description of the inputs to a computer-based business system into a programmer-oriented specification.

4.2Output Design

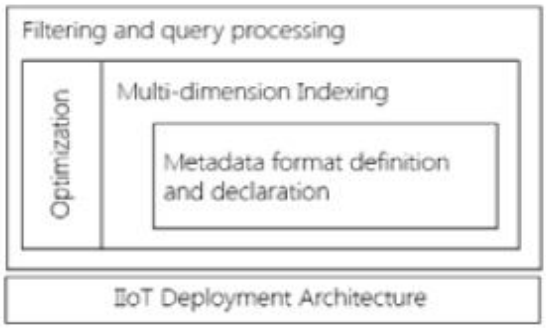
A quality output is one, which meets the requirements of the end user and presents the information clearly.

In any system results of processing are communicated to the users and to other system through outputs.

In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively.

4.3System Architecture



The SecIIoT is an authorization framework that can answer security queries efficiently based on the requesters' roles in an Industrial Internet of Things context. It consists of 1) metadata definition and declaration module 2) multi-dimension indexing 3) filtering and query processing 4) optimization and 5) interface.

4.4 The Metadata – Definition and Declaration

Data can be classified into IIoT Service metadata and IIoT Access metadata. Both of the metadata have the same number of attributes that can be defined by an owner. For example, IIoT Service metadata can be read from a table of a relational database or a flat file.

4.5 Multi-dimension Indexing

Multidimensional Indexing means naming data in the database with multiple names in multiple direction of views. Naming is done only with authorized person and unauthorized persons cannot access the database.

4.6 Filtering and Query Processing

Based on the input User ID, his profiles are fetched from the Profile DB, which is an object for storing all the users' profiles information. It follows a hash table structure and maps User ID with the user's profile (RAPs).

Storage has the hash set structure and it perform query with a constant time regardless of the size of the bucket.

4.7 Optimization

Optimization is broadly classified as profile and memory optimization. Profile attributes means reducing number of attributes in the database. Memory optimization means reducing the area of occupying.

Optimization improves the processing speed and produce output in required period of time.

4.8 Interface

Interface means connecting two different things using an intermediate medium in order to send and receive information or data between them.

Using this interface flow of data between these two medium becomes easy and reliable.

V. CONCLUSION

The Industrial Internet of Things is a promising technology that will transform companies through integrating of Internet of Things, people, data, and computers with intelligent data analytics. It will led to operational and productivity effectiveness of industries. However, with the growing complexity of IIoT, the access control and authorization of IIoT objects are indeed become the major challenges in the success of IIoT.

VI. FUTURE ENHANCEMENT

Industrial Internet of Things are much more efficient for multi-dimension and large data processing with flexible and efficient authorization. The future enhancement is to develop query processing and stored in RDBMS. Filtering process also done in the future. Time and location constrains are also strengthen for the future. An indexing framework for securing IIoT are also increased in the future.

REFERENCES

[1] K. Shvachko, H. Kuang, S. Radia, and R. Chansler, “The Hadoop Distributed File System,” Mass Storage Systems and Technologies (MSST), 2010.
[2] “Industrial Internet Reference Architecture,” Industrial Internet Consortium, 2015.
[3] P. Lade, R. Ghosh, and S. Srinivasan, “Manufacturing Analytics and Industrial Internet of Things”, IEEE Intelligent Systems, 2017, Volume: 32, Issue: 3.
[4] J. Mass, C. Chang, and S. N. Srirama, “WiseWare: A Device-to-Device-Based Business Process Management System for Industrial Internet of Things”, IEEE International Conference on Internet of Things (iThings),2016.
[5] Z. Ding, X. Gao, L. Guo, and Q. Yang. "A hybrid search engine framework for the internet of things based on spatial-temporal, value based, and keyword-based conditions." In Green Computing and Communications (GreenCom), 2012 IEEE International Conference on, pp. 17-25. IEEE, 2012.
[6] F. Chen, P. Deng, J. Wan, D. Zhang, A.V. Vasilakos, and X. Rong."Data mining for the internet of things: literature review and challenges." International Journal of Distributed Sensor Networks (2015).
[7] E. Borgia. "The Internet of Things vision: Key features, applications and open issues." Computer Communications, 54, pp. 1-31, 2014.
[8] R. Zhang, Y. Zhang, and K. Ren, “Distributed Privacy-Preserving Access Control in Sensor Networks,” IEEE Transactionson Parallel and Distributed Systems, vol. 23, no. 8, pp. 1427–1438, 2012.
[9] S. Ludwig, G. Selander, and C. Gehrmann. "Authorization framework for the internet-of-things." In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a, pp. 1-6. IEEE, 2013.
[10] P.P. Pereira, J. Eliasson, and J. Delsing. "An authentication and accesscontrol framework for CoAP-based Internet of Things." In Industrial Electronics Society, IECON 2014-40th Annual Conference of the IEEE, pp. 5293-5299. IEEE, 2014.