www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

Secure and Efficient Communication System Using Cyber Physical Systems in IOT by Wireless

M. Manjurekha, T. Jayabharathi, N. Shanthi & M. Hemasri

Department of Information Technology

Er. Perumal Manimekalai College of Engineering, Hosur

ABSTRACT:

Wireless sensors and actuators connected by the Internet-of-Things (IOT) are central to the design of advanced cyber physical systems (CPSs). In such complex, heterogeneous systems, communication links must meet stringent requirements on throughput, latency, and range, while adhering to tight energy budget and providing high levels of security. In this paper, we first summarize wireless communication principles from the perspective of the connectivity needs of IOT and CPS. Based on these principles, we then review the most relevant wireless communication standards before focusing on the key security issues and features of such systems. In particular, the gap between the security features in the communication standards used in CPSs and IOT and their actual vulnerabilities are pointed out with practical examples and recent attacks. We emphasize the need for a more in-depth study of the security issues across all the protocol layers, including both logical layer security and physical layer security.

Keywords: *Cyber Physical System (CPS); Internet-Of-Things (IoT), Machine - Type Communication (MTC); Security.*

1. INTRODUCTION

1.1 GENERAL

Cyber-physical systems (CPSs) are complex, heterogeneous distributed systems typically consisting of a large number of sensors and actuators, which are connected to a pool of computing nodes. With the fusion of sensors, computing nodes, and actuators, which are connected through various means of communications, CPSs aim to perceive and understand changes in the physical environment, analyze the impacts of such changes to their operation, and make intelligent decisions to respond to the changes by issuing commands to control physical objects in the system, thereby influencing the physical environment in an

autonomous way [1]. The connection between actuation and sensing through the physical environment, and between sensors and actuators through one or multiple (distributed) computing or intelligent control node(s) forms a feedback loop which aims at achieving a desired objective or steady state.

As such, a CPS either acts with full autonomy or at least provides support for a human-in-the-loop mechanism as part of semi-autonomous control functions. This distributed closed-loop process allows a CPS to remotely influence, manage, automate, and control many man-made (but also natural) small-, medium-, and large-scale systems. Due to the operational nature of CPSs in most industrial control processes, CPSs are also known as operational technology systems (OT systems) which will be discussed in further detail. The massive adoption of internet protocol (IP)-enabled devices (i.e., IP sensors and actuators) in CPSs and the increasing wireless connectivity has thereby blurred the boundary between CPSs and the Internet-of-Things (IoT).

The concept of IOT stems from connected smart devices [2], which may or may not be interacting with a physical object. Hence, there are application scenarios even in the classical IOT domain that can already be conveniently classified under either the IOT or the CPS domain, e.g., distributed set of sensor nodes to monitor and control the energy usage of a manufacturing plant. Famous examples for CPSs and IOT systems and corresponding applications [3], include but are not limited to, large-scale environmental systems (e.g., natural resource management), power and energy generation and distribution, transportation infrastructure, home automation, autonomous driving, personal healthcare, logistics, or industrial manufacturing. Due to the diverse variety of applications, CPSs are expected to have a tremendous economic impact [4] through their critical role in OT as well as intelligent control systems. In the following, while discussing these applications, we use the collective term as CPSs to stress the rich interaction with the physical world and the consequent security issues that originate from this interaction.

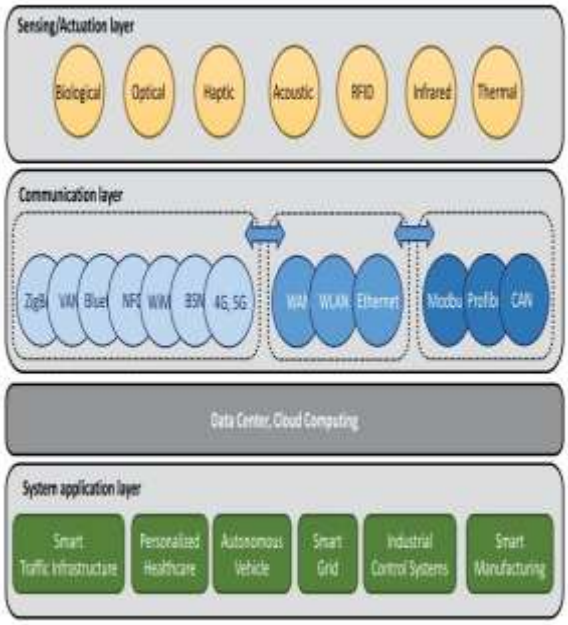

Fig No. 1.1 Cyber Physical Systems

Interestingly, this trend toward physically fully detached nodes is experienced not only in an increasing number of cases where wires are unacceptable, but also for cases where power supply from the mains and wired network connections would in principle be feasible or even available. Reasons for preferring wireless connectivity are often simply the reduced installation cost or the desire to ease the installation. The increasing availability of a wide range of wireless technologies, optimized for different communication scenarios and requirements (also those specifically relevant to CPSs) has therefore been an important driver for the success and rapid adoption of CPSs in our society and will remain of critical importance for its future evolution. An abstract view of the CPS/IOT layers is depicted in Fig. 1.1. The sensing/actuation layer that is enabled by IOT sensors and actuators is supported by a transport/communication layer by interconnecting the nodes to the system application layer with a pool of computation nodes for data analytics and decision making to support a wide varieties of OT applications. The different components in these layers can be connected through different wireless and wired communication protocols, including also the frequently cited “IP-based IOT infrastructure.” When such systems also act on the physical

world through the integration of connected actuators, they form a CPS. Hence, the IOT forms the basis for many modern complex CPSs. In essence, CPSs carry their name due to their interaction with the physical environment through sensing and actuation devices.

However, while some CPSs may also be known as IOT systems from the protocol perspective, if the sensing and actuation devices are IP-capable, we note that many other local CPSs exist today that are still fully detached from the global IP network (a situation that will change over time). Yet, a CPS may be viewed from the functional perspective and be known as an OT system if it is used for supporting the operation of industrial control processes. Unfortunately, albeit the obvious advantages of wireless connectivity, eliminating the wires also comes with a number of difficulties and challenges regarding communication performance (e.g., latency, range, and throughput), power consumption of the node, and security. Together with the requirements of a CPS, these concerns dictate the choice of the right wireless communication standard and set the stage for research on the next-generation secure wireless connectivity of CPSs through all layers of the network stack.

In this paper, we draw attention to the myriad of wireless communication systems and standards utilized in CPSs and in IOT. We discuss their technologies and properties from a communications perspective, and also the security practices for CPSs which interface with wireless communication security standards/protocols. The security of CPSs and IOT systems, for which we point inquisitive readers also to [5] to [7]. The study of physical side channel attacks, which pertains to the implementation security of CPS or IOT devices are left outside the scope of this paper and can be referred to in [8] and [9]. The rest of this paper is organized as follows. We summarize the wireless communication and security properties and requirements of CPSs and IOT systems, the communication aspect and we discuss some fundamental technologies of the different communication layers as a basis for understanding the properties of different standards. The most important communication standards for CPSs and IOT based on the previously discussed fundamentals and together with their most important properties as a basis for selecting the right standard for a particular system with respect to the initially described requirements. Section V then proceeds to the security issues and measures of CPSs and IOT in general, it specifically concerned with the security issues of wireless CPSs and IOT Systems.

1.2 OBJECTIVE

To allow smart devices to share data equally between other networks and have fast data access and higher bandwidth.

- To reduce the time delay of data sharing that protects our data from hackers.
- To analyze the performance is more efficient and can be used in IOT applications.

2. LITURATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration taken into account for developing the proposed system.

Secure Communication in Cyber-Physical Systems and Internet-Of-Things Systems.[1] These billions of smart devices connected to the internet are sensitive to a wider range of attacks and design flaws.[2] CPSs and IOT systems can be also exploited to launch DOS attacks against other targets.[3]

EXISTING SYSTEM

- By connecting these billions of smart devices to the Internet, the IOT will provide developed smart and autonomous cyber-physical environments in the area of smart grids, smart cities, smart homes, and smart medical and healthcare systems.
- A huge amount of data are generated that requires high computational capabilities for storage, processing, and analyzing purposes in a secure and efficient manner.
- Generally, the smart devices have limited resources.
- On the other hand, cloud resources have virtually unlimited storage and processing capabilities with scalability and on-demand accessibility anywhere.

- Thus with the help of the cloud, the IOT smart devices can relieve the burden of limited resources.

PROPOSED SYSTEM

- To propose a cyber-physical systems with lightweight cryptographic scheme so that IOT smart devices can share data with all security-oriented operations are offloaded to nearby edge servers.
- Finally, security and performance analysis shows that our proposed scheme is efficient and reduces the computation and communication overhead of all entities that are used in our scheme.
- To propose a secure data-sharing scheme at the edge of network connected IoT smart devices that utilizes both secret key encryption and public key encryption.
- In this scheme, all security operations are offloaded to nearby edge servers, thereby, greatly reducing the processing burden of smart devices.
- Hence, proposed scheme attains the integrity of shared data and searching resultant data. Finally, we analyze the performance of our proposed scheme and prove that our scheme is efficient and can be used in IoT applications.

3. SYSTEM ARCHITECTURE

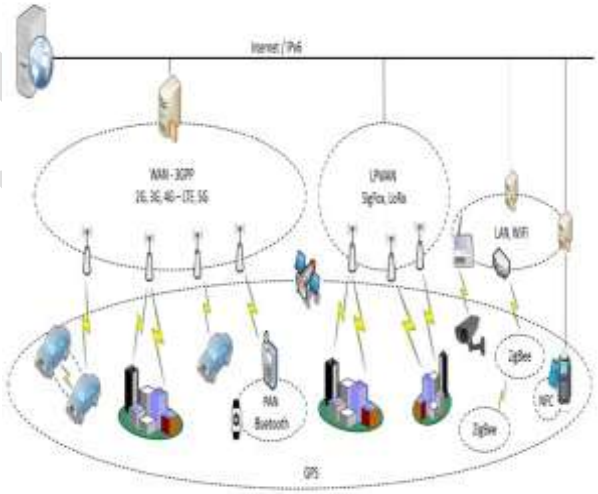

Figure 3.1: System Architecture

The architectural design of a system emphasizes the design of the system architecture that describes the structure, behavior and more views of that system and analysis. This diagram shows the various kinds of networks like WiFi, 2G, 3G, 4G, LAN, Bluetooth that are connected to the internet. By implementing the cluster, every network will be able to receive the equal bandwidth and time delay. With this method, the communication system is said to be secure and more efficient than any form of communications.

4. Algorithms & Techniques Used

- Secure Data Sharing
- Edge Server
- High Bandwidth
- Novel Algorithm (Generating Cluster)
- DES Algorithm(Data Encryption Decryption Process
- RLE Algorithm(File Compress)
- LEARN Algorithm (High Speed Data Transfer)

4.1 TECHNIQUES USED:

Secure Data Sharing

We propose a secure data-sharing scheme at the edge of cloud connected IoT smart devices that utilize both secret key encryption and public key encryption. In this scheme, all security operations are off loaded to nearby edge servers, thereby, greatly reducing the processing burden of smart devices. We provide a background overview followed by a brief description of our proposed scheme. We then analyze the performance and compare it to related works. Finally, we conclude our paper by stating future works.

Edge Server

The edge servers are semi trusted and secure entities located at the proximity of smart devices that are capable of sharing data with a number of smart devices. It is responsible for security-oriented operations such as secret key generation and management, encryption, and

decryption. The edge servers are maintained by clouds. Moreover, the edge servers provide data storage and processing of the smart devices.

Edge Servers Work

- Data Encryption Decryption
- Data Management.
- Generating Cluster Network
- File Compress
- Providing High Bandwidth Speed For All Users

High Bandwidth

The data are of little use if the smart devices do not share data with other devices. Data sharing at the edge allows smart devices to share data with lower latency and have fast data access and higher bandwidth. The next generation wireless communications technology (5G) will greatly depend on such solutions where massive IoT smart devices are interconnected with high data rates at ultralow latency. Evaluate a performance comparison of the cloud and edge/fog server in terms of latency and bandwidth.

4.2 ALGORITHM

1. Novel Algorithm (Generating Cluster)

An efficient clustering algorithm is proposed in an unsupervised manner to cluster the given data set. This method is based on regulating a similarity measure and replacing movable vectors so that the appropriate clusters are determined by a performance for the classification validity. The proposed clustering algorithm needs not to predetermine the number of clusters, to choose the appropriate cluster centres in the initial step, and to choose a suitable similarity measure according to the shapes of the data. The location of the cluster centres can be efficiently determined and the data can be correctly classified by the proposed method. Several examples are considered to illustrate the effectiveness of the proposed method.

2. DES Algorithm (Data Encryption Decryption Process)

Data Encryption Standard (DES) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to cipher text using keys of 48 bits. It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

3. RLE Algorithm (File Compress)

Run-length encoding (RLE) is a form of lossless data compression in which runs of data (sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run.

4. LEARN Algorithm (High Speed Data Transfer)

LATENCY AWARE REPLICA PLACEMENT (LEARN) ALGORITHM

Replication technology has been widely used to improve the performance of network-based applications. By serving clients with nearby replicas, it can significantly reduce the overall network latency. Additionally, the replication would also benefit service reliability. In practice, all of the computing resources such as processors, storage, and networks, are not failure free, and a failure is usually fatal to an existing running system. As a result, replica sites have to be selected to serve all clients of the failed nodes so that the service could be continuous.

5. CONCLUSION & FUTURE ENHANCEMENT

The diversity and the heterogeneous nature of CPSs and the IOT possess a number of requirements on the communication systems (wired and wireless) that connect their components. In particular in a CPS, this connectivity and its requirements may even be different for various parts of the system. No single standard can meet all of the requirements. However, a plethora of different standards exist that cover a large part of the design space. Nevertheless, there is still a need for innovation in the development of future wireless systems

REFERENCES:

[1] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in Proc. Int. Conf. Wireless Commun. Signal Process. Nov. 2011, pp. 1-6, doi: 10.1109/WCSP.2011.6096958.

[2] M. Weiser, "The computer for the 21st century," SIGMOBILE Mob.Comput.Commun. Rev., vol. 3, pp. 3-11, Jul. 1999.

[3] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyber physical systems: A survey," IEEE Syst. J., vol. 9, no. 2, pp. 350-365, Jun. 2015, doi: 10.1109/ JSYST.2014.2322503.

[4] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput., Jun. 2008, pp. 1-9, doi: 10.1109/SUTC.2008.85.

[5] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," IEEE Commun. Surv.Tuts., vol. 17, no. 3, pp. 1294-1312, 3rd Quart., 2015, doi: 10.1109/COMST.2015.2388550.

[6] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyberphysical systems security—A survey," CoRR, 2017.

[7] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure cyber-physical systems: Current trends, tools and open research problems," in Proc. DATE, 2017, pp. 1104-1109.

[8] F.-X. Standaert, Introduction to Side-Channel Attacks. Boston, MA, USA: Springer-Verlag, 2010, pp. 27-42.

[9] V. Pudi, A. Chattopadhyay, and K.-Y. Lam, "Secure and lightweight compressive sensing using stream cipher," IEEE Trans. Circuits Syst. II, Exp. Briefs, 2017, doi: 10.1109/ TCSII.2017.2715659.

[10] Y. Liu and G. Zhou, "Key technologies and applications of Internet of Things," in Proc. 5th Int. Conf. Intell.Comput. Technol. Autom., Jan. 2012, pp. 197-200, doi: 10.1109/ ICICTA.2012.56.