DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4841

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURITY AND PRIVACY OF CYBER PHYSICAL SYSTEMS IN IOT USING CLOUD INFRASTRUCTURE

Jayashree Agarkhed
Professor, Department of Computer Science & Engineering,
P.D.A College of Engineering, Kalaburagi, India.

Abstract: The idea of cyber-physical systems (CPS) is the incorporation of computation processes and physical processes which can help towards the recognition of real smart cities capable to ensure sustainability and efficiency. IoT refers to the junction of Internet technology using RFID, sensors and smart objects. Sensor based hardware, data collection, management of data, mining of data and WWW (World Wide Web) are the latest trend technologies used in IoT. The major security challenges are considered as the key issues for the consideration. They include data confidentiality, privacy and trust issues. This paper identifies some of the key issues, applications and challenges of IoT facing in the real world today. CPS along with their cyber-physical object (CPO) is the key elements in the context of a smart city nature.

Keywords: Cloud computing, Security, IoT, Cyber Physical System

1. INTRODUCTION

Cloud computing is adopting significance in the current technology. Due to the advent in the communication technology, any objects can get connected with any other objects. This is the era of where the things speak instead of livings humans. This technology has been termed as Internet of Things (IoT). For IoT to speak, there is a need of powerful essentialnetwork infrastructure that is Internet. This is in turn prone to physical threats in the cloud network. IoT is an integrated part of future Internet and can be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [1].

The continuous growth of the urban population has generated a tremendous expansion of our cities.Nowadays, indeed, more than 50 % of the world's population is living urban, and they estimate that it will reach 70% by the year 2050. Therefore, cities need to be ready to accommodate this huge amount of citizens and to face new challenges like traffic congestion, air pollution, waste management and so on. Majority of the IoT companies included are Amazon, CISCO, MS Azure, Salesforce, Oracle and much more. IoT is the integration of multiple heterogeneous networks. It is difficult to establish the junction of relationship as the relationship of trust between nodes that are constantly changing. Security has become a serious aspect of IoT because of the inclusion of the latest technologies and various applications to enormous users.

IoT is basically a cloud of interconnected devices. In simple terms devices like microcontrollers and microprocessors when connected to internet in such a way that each of these device can communicate with every other device forms IoT infrastructure. IoT has many security issues like privacy issues, authentication and access control network configuration issues, infor mation storage and management and so on. IoT refers to the incorporation of multiple heterogeneous networks. It is difficult to establish the junction of relationship as the relationship of trust between nodes that are constantly changing. The key issues can be deciphered by key management and routing protocols. A mashup is a Web 2.0 concept where an application uses data and functionality from a variety of web resources. Some researchers proposing WOT model suggest building on the mashup paradigm, except this time applying it to physical devices instead of applications [1].

The structure of the paper is as follows. Section II gives the related work. Section III presents the challenges in CPS. The section IV gives the security in IoT. Section V gives the conclusion.

2. RELATED WORK

Extensive literature survey has been prepared for securing the CPS in cloud infrastructure. A map reduce framework has been introduced which includes cloud infrastructure and end-user devices. The cyber security system uses cloud based system which can be used for large computer network [2]. With the invention of Information Communication Technology (ICT), the good will is to enable ubiquitous as well as pervasive computing to control the physical processes and physical objects. This concept invented the version of CPS. ICT provides pervasive computing concept. The networking abstractions of cyber physical internet include various protocol layers like physical, transport, network and medium access application layer. The real time challenges in CPS have operating systems, network protocols, timing guarantees, data aggregation, and performance compositionality [3].

The network infrastructure in smart city concept is highly interconnected, energy-efficient, cost-efficient and reliable in nature. CPS includes number of physical processes in medical devices, assisted living, traffic control and so on [4]. The IoT is a striking technology which has distinctive IoT characteristics that Unit IoT and Ubiquitous IoT or simply U2IoT model has been presented for the future IoT. The information security model is established to describe the mapping relations among U2IoT, security layer, and security requirement, in which social layer and additional intelligence and compatibility properties are infused into Internet and physical management (IPM). The physical security referring to the external context and inherent infrastructure are inspired by artificial immune algorithms. The security strategies are suggested for social management control. The proposed IPM combining the cyber world, physical world and human social provides constructive proposal towards the future IoT security and privacy protection. The cyber physical social based security architecture includes physical and management security features. IoT has been related to both cyber world with digital as well as physical entities. The information security architecture includes social factor for security layer in sensor, network and application layer [5].

A dynamic component model for CPS includes different levels like parametric adaptation, architectural adaptation, dynamic provisioning and adaptation for remote management [6]. CPS has the capability to check, share and also provide the information in the world. Security and privacy preserving in CPS are the important issues to be considered in today's real world. CPS includes integration, computation, communication and control into the physical systems. Major applications include transportation, energy and industrial automation, healthcare, bio-medical and critical infrastructure. A CPS is globally connected to the web of things and focus on physical processes in a closed looping system [7].

The core technology behind CPS and IoT is the Internet which works as large scale network. Scientific workflows require huge amount of data as well as computing jobs over the cloud network. The cloud computing environment provides enormous opportunities in order to solve various scientific problems in multi cloud setup. CPS can be characterized as a thematic subject as opposed to a disciplinary topic.Multidisciplinary areas such as mechatronics, robotics and CPS typically start as themes, and may then eventually evolve into disciplinary areas. IoT can be seen as a bottom-up vision, an enabling technology, which can be used to create a special class of CPS means systems including the Internet. A CPS does not necessarily include the Internet options. Some visions of the IoT go beyond basic communication, and consider the ability to link "cloud" representations of the real things with additional information such as location, status, and business related data [8]. The integrated version of IOT and cloud computing paradigms can be created with smart environments. This is used with multiple stake holders for various services. Multiple users are supported for high reliability and decentralization. The cloud computing applications are used for creating applications using particular programming tool and environment. The various types of resources and application execution are used for better QoS requirements [9].

3. CHALLENGES IN CPS

CPS is the main source of smart grid technology which helps to monitor, transfer and manage information and actions in the real world. The smart city concept has features like user-centric, ubiquitous, and highly integrated on multiple users. The Cloud IoT means the interconnection of uniquely identifiable embedded computing devices within the Internet infrastructure.

I) The need for smart city can be classified into two different ways.

a) Service or application oriented type for view of users
b) Operational type used for city authorities and network administrators

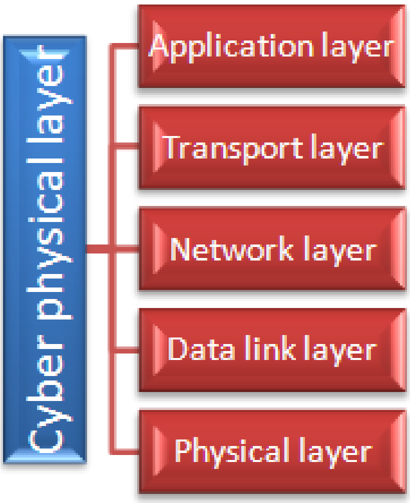

Fig 1. Network protocol stack architecture

The figure 1 shows the cross layer network management for cyber physical layers. Different layers of protocol stack include application, transport, network, data link and physical layer in the network. The CPS includes physical process and includes various computations.

i) Some of the design challenges in CPS are given as follows.
   a) Cross domain with cross-network
   b) Embedded and mobile sensing
   c) Elastic load
   d) Accumulated intelligence
   e) Interactions among many objects

ii) The challenges in IoT are given as follows.
   a. Security structure
   b. Key management
   c. Security law and regulations
   d. Requirements for burgeoning applications

4. SECURITY IN IOT

Security and privacy are the great concerns for IoT applications, and still face some enormous challenges. By deeply analyzing the security architecture and features, the security requirements are given. On the basis of these, we discuss the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and briefly outline the challenges. The security requirements are based on security features and its network architecture. IoT needs highest security and privacy for the progress in this fastest world. IoT has four levels which includes perceptual, network, support and application layer for supporting security features in network.

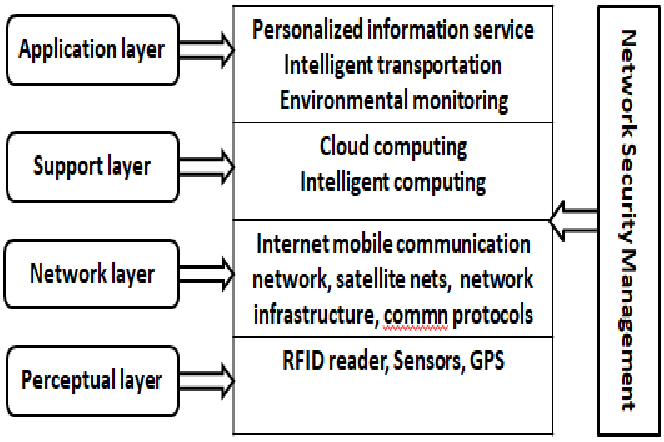
Application layer
Personalized information service
Intelligent transportation
Environmental monitoring
Support layer
Cloud computing
Intelligent computing
Network layer
Internet mobile communication
network, satellite nets, network
infrastructure, commn protocols
Perceptual layer
RFID reader, Sensors, GPS
Network Security Management

Figure 2. Network security architecture

Figure 2 depicts the security architecture in network security management. The security requirements are considered at each level of IoT. The first level includes perceptual layer which is also called as recognition layer. Next level is network layer which includes reliable transmission of information. Third level is the support layer for supporting reliable platform. Last level includes application layer for users to make use of IoT through television and computer, laptops or mobile phones.

5. CONCLUSION

CPS includes cyber physical objects for real time smart cities concept using latest technologies in IoT. IoT has become a focus of great research today. It refers to the newest technology in the field of information technology which has billions of smart objects having interconnection with all the resources associated with it. The security and privacy protection of cyber physical systems are considered using cloud computing area.

REFERENCES

[1] Petrolo, Riccardo, Valeria Loscri, and Nathalie Mitton. "Cyber-Physical Objects as key elements for a Smart Cyber-City." Management of Cyber Physical Objects in the Future Internet of Things. Springer International Publishing, 2016. 31-49.

[2] Xu, Guobin, et al. "A cloud computing based system for cyber security management." International Journal of Parallel, Emergent and Distributed Systems 30.1 (2015): 29-45.

[3] Koubâa, Anis, and BjörnAndersson. "A vision of cyber-physical internet." 8th International Workshop on Real-Time Networks (RTN'09). InstitutoPolitécnicodo Porto. Instituto Superior de Engenharia do Porto., 2009.

[4] Karnouskos, Stamatis. "Cyber-physical systems in the smartgrid." Industrial Informatics (INDIN), 2011 9th IEEE International Conference on. IEEE, 2011.

[5] Ning, Huansheng, and Hong Liu. "Cyber-physical-social based security architecture for future internet of things." Advances in Internet of Things 2.01 (2012): 1.

[6] Fouquet, Francois, et al. "A dynamic component model for cyber physical systems." Proceedings of the 15th ACM SIGSOFT symposium on Component Based Software Engineering. ACM, 2012.

[7] Wang, Lihui, Martin Törngren, and Mauro Onori. "Current status and advancement of cyber-physical systems in manufacturing." Journal of Manufacturing Systems 37.Part 2 (2015): 517-527.

[8] Petrolo, Riccardo, Valeria Loscri, and Nathalie Mitton. "Cyber-Physical Objects as key elements for a Smart Cyber-City." Management of Cyber Physical Objects in the Future Internet of Things. Springer International Publishing, 2016. 31-49.

[9] Xu, Guobin, et al. "A cloud computing based system for cyber security management." International Journal of Parallel, Emergent and Distributed Systems 30.1 (2015): 29-45.

[10] Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.