International Journal of Civil Engineering and Technology (IJCIET)
Volume 8, Issue 8, August 2017, pp. 920–925, Article ID: IJCIET_08_08_097
Available online at http://http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=8&IType=8
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

FRAMEWORK OF CYBER PHYSICAL SECURE SYSTEMS USING INTERNET OF THINGS (IOT) DEVICES

E. Ravi Kumar, K. Kotaiah Swamy
Department of Information Technology
Vardhaman College of Engineering, Hyderabad, India

B. Dhanalaxmi, A.Praveen
Department of Information Technology
Institute of Aeronautical Engineering, Hyderabad, India

ABSTRACT

A cyber physical secure systems using Internet of Things (IoT) is proposed. The proposed framework includes deciphering of enciphered record points from an IoT device, massive quantity of aggregated record points form a massive quantity of record sets, retrieve a massive quantity of primary record point corresponding to the record sets, primary record points form a primary core record set; retrieve a massive quantity of secondary record points corresponding to the primary core record set and a secondary core record set, secondary core record set corresponds to other IoT devices; determining whether the IoT device is in an inconsistent state based on the secondary record points; and isolating the IoT device to a specific virtual network when the IoT device is in the inconsistent state.

Key words: Cyber Physical Systems, Secure Systems, Internet of Things Devices, Record Points

Cite this Article: E. Ravi Kumar, K. Kotaiah Swamy, B. Dhanalaxmi and A.Praveen, Framework of Cyber Physical Secure Systems Using Internet of Things (IOT) Devices, International Journal of Civil Engineering and Technology, 8(8), 2017, pp. 920–925.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=8&IType=8

1. INTRODUCTION

The Internet of Things, an under developing global Internet-based technical architecture ensuring the exchange of technology and services in global supply chain networks has an impact on the security and privacy of stakeholders [1].

The term cyber -physical systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities [2]. The ability to interact with, and expand the capabilities of, the physical

world through computation, communication, and control is a key enabler for future technology developments [2].

Issues with the security of the cyber-physical systems include the malicious attempts by an adversary to intercept, disrupt, defect or fail cyber-physical systems that may affect a large group of population, an important government agency or an influential business entity by denying availability of services, stealing sensitive data, or causing various types of damages, as well as the security breaches in small scale cyber-physical systems that may affect few individuals or relatively smaller entities[4].

2. RELATED WORK

Anees Ara [2015] proposes a Secure Service provisioning architecture for Cyber Physical Cloud Computing Systems (CPCCS), which includes the combination of technologies such as CPS, Cloud Computing and Wireless Sensor Networks. We also highlight various threats/attacks; security requirements and mechanisms that are applicable to CPCCS at different layers and propose two security models that can be adapted in a layered architectural format.

Somayya Madakam [2016] proposes integration of the physical world into the fabric of Web imposes advanced security requirements that need to be satisfied in order to ensure a stringent control over IoT service interaction. Security and privacy trials of the Internet of Things (IoT) that appear are due to the connection of diverse technologies.

Rajeev Alur [2015] interprets success in developing value-added capabilities around IoT requires a broad approach that includes expertise in sensing and hardware, machine learning, networked systems, human-computer interaction, security, and privacy. Strategies for making IoT practical and spurring its ultimate adoption also require a multifaceted approach that often transcends technology, such as with concerns over data security, privacy, public policy, and regulatory issues.

Robert S. Metzger [2016] proposed an adversary may exploit cyber-active devices or the means by which these are connected to or managed by infrastructure to deny, disrupt or impair functionality of defense systems. Measures taken by DoD focus on contractor protection against counterfeit electronic parts (physical) and protection of information and information systems (cyber) but not on cyber/physical threats.

John Pescatore [2014] proposes that Internet enables any-to-any connectivity. Smart buildings, HVAC and even physical security technologies are now connected, as are handheld smart devices and more. The latest wave of 'things' connecting to users, businesses and other 'things' using mixtures of wired and wireless connectivity, includes but is not limited to automobiles, airplanes, medical machinery and personal (implanted) medical devices, and SCADA systems.

Brian Russell [2015] will allow unseen linkages to be made which may cause concern for the privacy of individuals or groups of people. Individuals may not even be aware that they are being tracked or recorded given the ability for next generation microchips to be embedded in virtually any platform. Assuring the security of each component within an IoT system is important to keep mischievous actors from taking advantage of the power of the IoT in an unauthorized manner.

Measurement and Management tools 2nd Release [2011] prepared a patch that will eliminate such vulnerability, allowing its customers to remediate the threat once the vulnerability is made public by the researchers.

The Internet of Things (IoT) drastically changes how individuals interact with objects, wherever those may be located [9]. It creates significant opportunities for more efficiency, convenience and comfort and can improve performance and reduce inefficiencies in numerous

sectors. promising gains and applications include traffic efficiency thanks to connectivity between vehicles and with infrastructure (towards autonomous vehicles), the provision of personal health care (mHealth or eHealth1) through implantable or wearable connected medical devices including apps (Software as a Medical Device), smart homes and buildings, smart factories and supply chains, smart cities, and smart grids. IoT technologies include specific infrastructure with sensors and processors for wired and wireless applications, and a range of connectivity and security solutions.

3. PROPOSED SYSTEM

A proposed framework of cyber physical secure systems using Internet of Things (IoT) is capable of providing cyber physical security function to an Internet of Things device, preventing the Internet of Things device from a mischievous cyber attack or stolen data.

The proposed framework provides deciphering a of enciphered record points from an IoT device, the massive quantity of aggregated record points form a massive quantity of record sets, retrieve a massive quantity of primary record point corresponding to the record sets, the primary record points form a primary core record set; retrieve a massive quantity of secondary record points corresponding to the primary core record set and a secondary core record set, the secondary core record set corresponds to other IoT devices; determining whether the IoT device is in an inconsistent state based on the secondary record points; and isolating the IoT device to a specific virtual network when the IoT device is in the inconsistent state.

The framework includes enciphering a data and transmitting the enciphered data to the IoT device when a data is to be transmitted to the IoT device.

The framework comprises when the enciphered record points belong to a compressed packet to be transmitted by the IoT device to a target IoT device, converting the compressed packet into a network packet having an Internet format, the compressed packet corresponds to a genuine packet in the Internet of Things device; routing the network packet; and compressing the network packet and transmitting the compressed network packet to the target Internet of Things device.

The step of aggregating the record points into aggregated record points includes, characterizing a massive quantity of successive record points as one of the aggregated record points.

The step of determining whether the Internet of Things device is in an inconsistent state based on the secondary record points includes: executing a data stream cluster algorithm on the secondary record points to determine whether a massive quantity of anomalous record points appeared in the secondary record points; if yes, determining the Internet of Things device is in the inconsistent state.

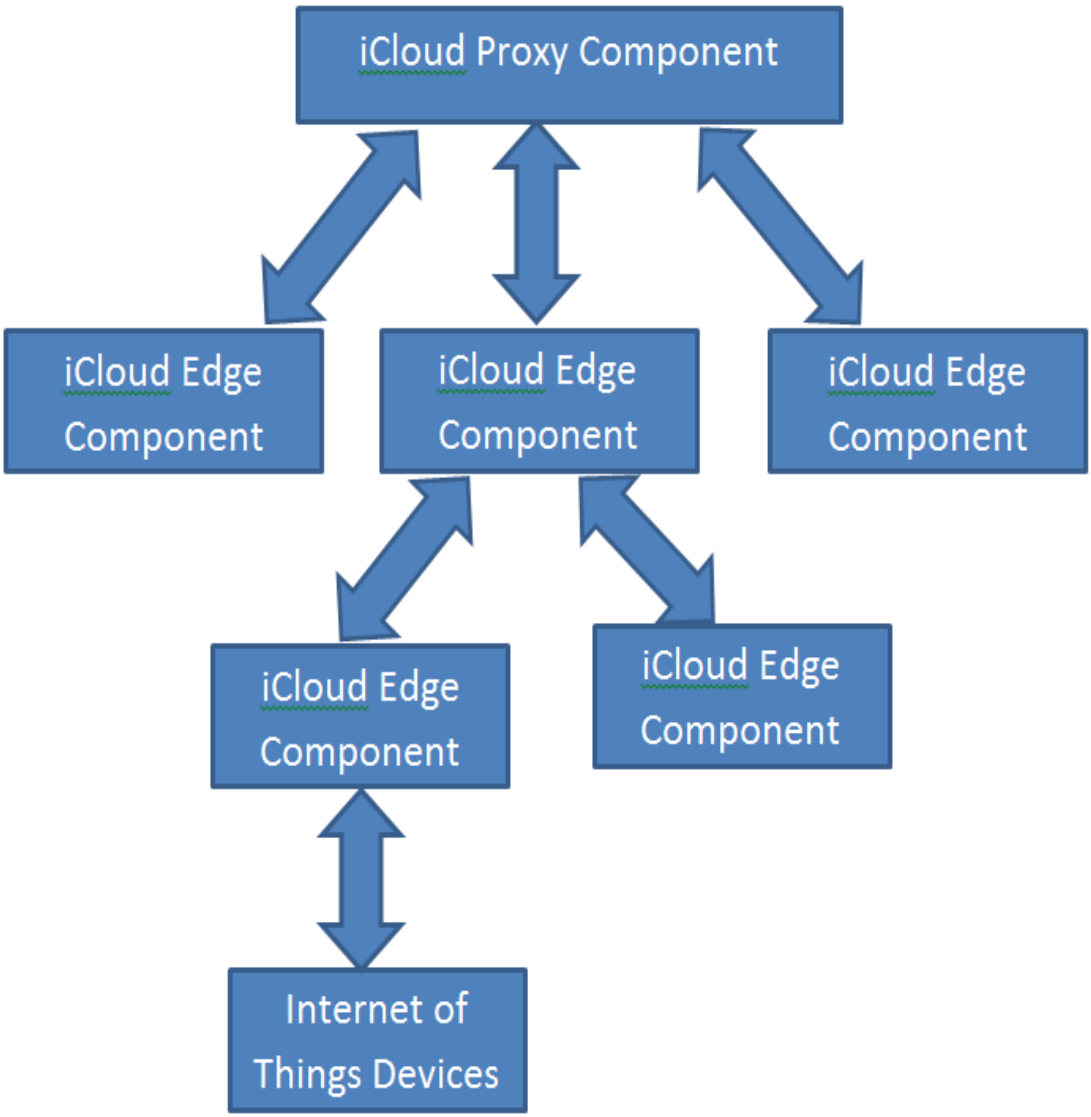

Figure 1 Framework of cyber physical systems for secure components

The above framework provides a cyber physical secure systems including an iCloud edge component, a iCloud hub component, and a iCloud proxy component. The iCloud edge component is configured to decrypt a massive quantity of encrypted record points from an IoT device; aggregate the record points into a massive quantity of aggregated record points, the aggregated record points form a massive quantity of record sets; retrieve a massive quantity of primary record points corresponding to the record sets, the primary record points form a massive quantity of primary core record sets. The iCloud hub component is configured to retrieve a massive quantity of secondary record points corresponding to the primary core record sets and a secondary core record set, the secondary core record set corresponds to other IoT devices; determining whether the IoT device is in an inconsistent state based on the secondary record points. When the IoT device is in the inconsistent state, the iCloud proxy component isolates the IoT device to a specific virtual network.

When a data is transmitted to the IoT device, the iCloud edge component encrypts the data and transmits the encrypted data to the IoT device.

The system includes another iCloud edge component. When the encrypted record points belong to a compressed packet to be transmitted by the IoT device to a target IoT device controlled by the other iCloud edge component, the iCloud edge component converts the compressed packet into a network packet having an Internet format, the compressed packet corresponds to a genuine packet in the IoT device. The iCloud edge component, the iCloud hub component, and the iCloud proxy component are configured to route the network packet to the other iCloud edge component. The other iCloud edge component compresses the network packet and transmits the compressed network packet to the target IoT device.

The iCloud edge component characterizes a massive quantity of successive record points as one of the aggregated record points.

The iCloud hub component is configured to execute a data stream cluster algorithm on the secondary record points to determine whether a massive quantity of anomalous record points appeared in the secondary record points. If yes, the iCloud hub component determines the IoT device is in the inconsistent state.

Based on the above, under the premise that the IoT device itself has weaker computing capability, the cyber physical secure systems framework and the cyber physical secure systems provided in the embodiments of the invention can provide cyber physical secure systems function to the IoT device via greater computing capability.

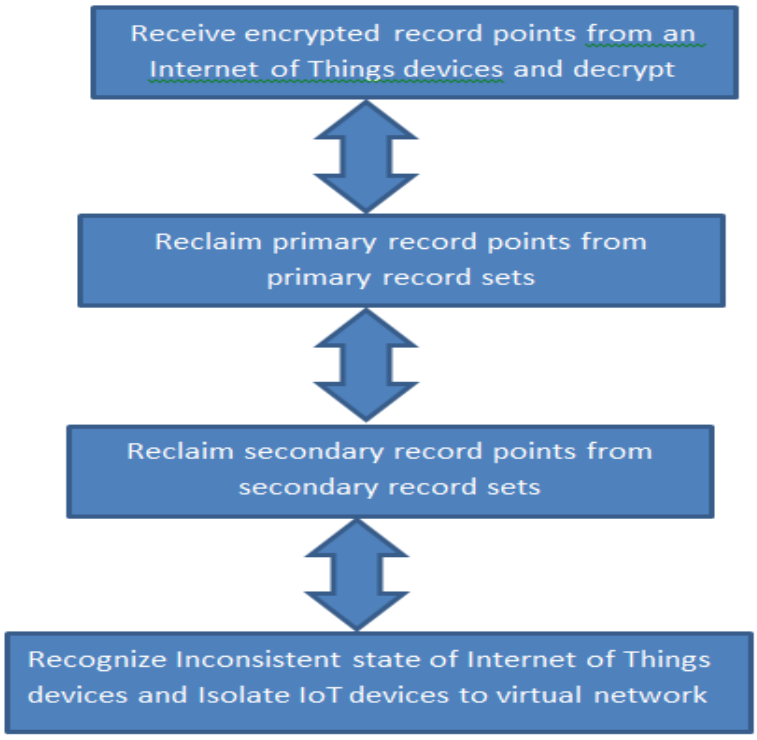

Figure-2: Flowchart of cyber physical secure systems approach

The figure 2 provides receiving encrypted record points from Internet of Things devices and decrypt, reclaim primary record points from primary records sets, reclaim secondary record points from secondary record sets and recognize inconsistent state of Internet of Things devices and isolate IoT devices to virtual network. The whole process of securing IoT devices is achieved.

4. CONCLUSION

The framework provides deciphering of enciphered record points from an IoT device, involving iCloud hub component, iCloud edge component and iCloud proxy component by considering massive quantity of primary record points and massive quantity of secondary record points from IoT devices. By deciding whether the IoT device is in an inconsistent state and isolating the IoT device to a specific virtual network when the IoT device is in the inconsistent state.

REFERENCES

[1] Weber, Rolf. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review. 26. 23-30. 10.1016/j.clsr.2009.11.008.

[2] Baheti, Radhakisan, and Helen Gill. Cyber-physical systems. *The impact of control technology* 12 (2011): 161-166.

[3] Yang, Gang, and Xingshe Zhou. Cyber-physical systems. (2013).

[4] Md E. Karim, Vir V. Phoha. Cyber-physical Systems Security, Applied Cyber-Physical Systems pp 75-83, August 2013

[5] N. Adam, Cyber-physical systems security, Presented at the Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee, 2009.

[6] E. K. Wang, et al., Security Issues and Challenges for Cyber-Physical System, presented at the Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications \& Int'l Conference on Cyber, Physical and Social Computing, 2010.

[7] M. Yilin, et al., Cyber-Physical Security of a Smart Grid Infrastructure, *Proceedings of the IEEE,* Volume 100, pp. 195–209, 2012

[8] J. Mirkovic, et al., Internet denial of service: attack and defense mechanisms: Prentice Hall, 2005.

[9] P. Dayaker, Y. Madan Reddy and M Bhargav Kumar, A Survey on Applications and Security Issues of Internet of Things (IoT), International Journal of Mechanical Engineering and Technology, 8(6), 2017, pp. 641–648.

[10] Dr. Kavitha, C. Ramesh Gorrepotu and Narendra Swaroop, Advanced Domestic Alarms with IOT, International Journal of Electronics and Communication Engineering and Technology, 7(5), 2016, pp. 77–85.

[11] B. Durga Sri, K. Nirosha, P. Priyanka and B. Dhanalaxmi, GSM Based Fish Monitoring System Using IOT, International Journal of Mechanical Engineering and Technology 8(7), 2017, pp. 1094–1101.

[12] International risk governance center, Governing Cyber Security Risks and Benefits of the Internet of Things: Application to Connected Vehicles and Medical Devices.