Cloud based Cyber Physical Systems Security Issues: A Survey

Yogita Borse
Assistant Professor,
Department of Information Technology
K J Somaiya College of Engineering
Mumbai, India

Mohammed Saleh Shaikh
PG Student,
Department of Information Technology
K J Somaiya College of Engineering
Mumbai, India

ABSTRACT
Data processing and physical interaction are combined by cyber physical systems (CPSs). CPSs have limited computation and storage capabilities due to their small size and resource constraints. With the emergence of cloud computing there are several new opportunities for these CPSs to extend their capabilities by taking advantage of the cloud resources in different ways. Cloud based cyber physical system (CCPS) is the integration of cloud computing technology with CPSs where complex computations can be transferred to the cloud platform. This paper presents a survey of research done on cloud based cyber physical systems security issues.

General Terms
Cloud computing, Cyber physical system.

Keywords
Cloud cyber physical system, Cloud security, Cyber physical system security.

1. INTRODUCTION
Cloud computing is the on-demand delivery of various computer system resources such as compute power, data storage, software and other IT resources as services over the internet [8]. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are three standard cloud computing models [7]. Cyber physical systems supports both IaaS and PaaS architectures.

IaaS is a cloud computing offering which provide system infrastructure such as server hardware, networking services and storage space as a service through the internet. Service provider's infrastructure is used by organizations to deploy their own platforms and applications. Amazon Web Services (AWS) EC2 is the most popular Infrastructure-as-a-Service (IaaS) provider. EC2 helps developers to expand computing capabilities of their application by creating required instance type using API calls. As stated in Amazon's FAQ, "It typically takes less than 10 minutes from the issue of the RunInstances call to the point where all requested instances begin their boot sequences" [3].

PaaS is another cloud computing offering that provides a platform for developers to develop, run, and manage their applications without the complexity of constructing and maintaining the required infrastructure and services. PaaS has a constrained environment as compared to IaaS. Google App Engine (GAE) is an example of Platform as a Service (PaaS) in which an instance is an application like Java Virtual Machine (JVM) operating on a server. Multiple instances can be hosted by physical machines and this is the main advantage of GAE's instance startup time of few seconds. As machines have been booted up in advance before its activation is required, an application can be started easily by executing its code into the target machine.

Recently there has been a significant rise seen in the development of CPSs technology such as Smart Medical System, Industry 4.0, Intelligent Transportation Systems and Smart Cities. However, it is difficult to process the fast growing volume of data generated by large scale CPSs. The present CPSs does not support high-speed processing, and thus it is unable to provide reliable and real-time services required by mission critical systems. Fortunately, cloud computing services can deliver fast, scalable and on-demand processing power and large-capacity cloud storage for data streams. CPS can thus utilize the technology of cloud computing, along with the scalability and flexibility of resources. CPS have two key components as shown in Fig 1: the physical component, which is composed of sensors and actuators that are used for interacting with the physical environment and the cyber component, which is the software part used to manage and enhance the hardware capabilities of the CPS as well as to interact with the cyber world. Cloud technology prevalence and its advantages allow us to expand the cyber component of CPSs to the cloud. Thus, cloud computing technology can effectively and efficiently support the large scale CPSs, this is referred to as cloud cyber physical systems (CCPS).

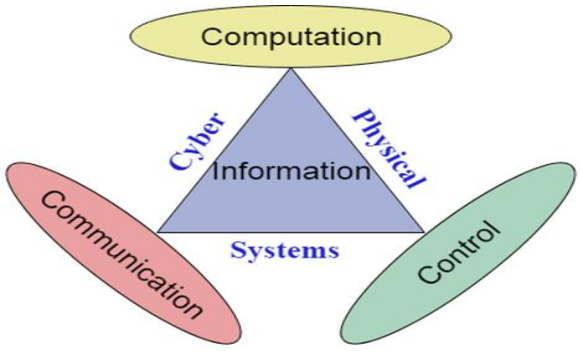

Fig 1: Three main functional components of CPS [14]

Although the combination of cloud and cyber physical systems is advantageous, it is subjected to new types of threats which are different from threats encountered in traditional computing systems. CPSs frequently gather sensitive and confidential information regarding physical environment. Thus, a loss of security for CPS can have serious adverse effects including privacy loss, potential physical damage and costs associated with operational disruption. While numerous security measures in the cyber domain have been adopted to solve the given issue, their applicability to the CCPSs domain remains doubtful because

they are usually difficult to implement and ineffective due to the heterogeneous distributed nature of the CCPS.

The advancement in technology have enormous advantages with the integration of cloud and physical system functionalities. Microsoft, Honeywell and Schneider Electric are some of the tech companies that are investigating the CCPSs because of its resource flexibility and scalability benefits. Some of the application of CCPS functionalities are in traffic control, location detection of vehicles, robotic surgery, and healthcare. CCPS enables detection of enemy in the war field and also modernize the defense technologies.

This paper discusses various security issues such as Cyber attacks, Real time Monitoring, Access control, Rootkits, Data storage and Data management problem.

2. LITERATURE SURVEY

Cloud and physical systems integration had opened the door to the attacker for initiating various types of cyber attacks. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, phishing and Man in the Middle attacks are some of the possible cyber attacks.

Different types of possible threats and attacks at different layers of CCPS as discussed by Anees et al. [16] are as follows:

1. **Application layer -** Cross site scripting (XSS), DoS, DDoS, security misconfiguration, SQL injection, Session hijacking, buffer overflow and failure to restrict URL access.
2. **Support layer -** Denial of Service (DoS), Data Breaches, Data Loss, Account Hijacking, Abuse of Cloud Services, Insecure APIs, Malicious Insiders, Insufficient Due Diligence and Shared Technology Issues.
3. **Network Layer -** Denial of Service Attack, Man in the Middle Attack, Eavesdropping, Data Modification, Identity Spoofing (IP Address Spoofing), Sniffer Attack, Password Based Attacks and Compromised Key Attack.
4. **Perceptual Layer -** DDoS as a result of jamming, Obstruction, destruction, malfunction or manipulation of physical devices.

Cloud technology provides real-time and reliable monitoring of both virtual and physical resources which helps in supporting application Quality of service (QoS) properties in the cloud as well as determining various possible security threats. Cloud resource surveillance methods are based on web interfaces such as RESTful APIs and SOAP, which cannot efficiently provide real-time information due to a lack of assistance for fine-grained surveillance capacities. Moreover, their implementation overhead leads to performance loss, creates latency jitter, and causes delay in reliable delivery of time sensitive data [18]. In order to monitor the cloud's virtual resource efficiently, [1] presents a monitoring model based on periodically and event-driven push (PEP) mechanism. This model can provide relatively appropriate data on the use of virtual resources and their status. It can also facilitate the communication between Master and Work Nodes without losing the track of major problems that occurred during the interval of push.

There has been an increase in DDoS attacks on cloud computing systems. This is one of the security threats to the availability. These attacks decreases the availability of the service by increasing resource utilization and cause costly business disruptions. It can reduce the cloud performance thus affecting mission critical Cyber physical systems (CPSs). Chonka et al. developed a defence system called Pre-Decision, Advance Decision, Learning System (ENDER) to detect and mitigate HX (HTTP and XML) DoS attacks on web services in Cloud based cyber physical systems. ENDER was successful at detecting and mitigate 99% with 1% false positive of HX-DoS attack traffic [6]. A cloud application which is intrusion tolerant can handle DoS attacks by denying access to possible malicious requests. For instance, Ficco and Ra [5] proposed a framework that blocks requests from reaching the cloud application that contain an excessive number of nested XML elements.

Yenumula et al. [12] discusses about rootkit as a threat to cloud based cyber physical system. Rootkit is a major security threat in operating systems based on Linux. Attackers can gain entry to target computer via backdoor entry created by rootkit without the notice of the owner. Rootkits malware are very hard to detect and eliminate as they often disguise themselves. They are currently used to conceal malware payloads more efficiently. When applied to the cloud environment, existing antiviruses have limitations. Lingchen et al. [13] propose RootkitDet, an end-to-end defense system that can detect and diagnose rootkits in guest operating systems with the aim of recovering system changes caused by rootkits in cloud environments. RootkitDet is able to detect rootkits by analyzing suspicious code in the kernel space of guest operating systems through the underlying hypervisor. It then diagnoses the detected rootkit code in order to categorize it and recognize changes, and if possible reverses the changes caused to the system by the rootkits.

As far as access control is concerned, exhaustive data control and permissions management should be implemented among all the entities that collaborate along the production life cycle, due to multiplicity of attack points and technological heterogeneity. Javier et al. [17] identified the requirements for flexible access control mechanisms to prevent unauthorized users from gaining access to heterogeneous systems and proposed a unique industrial architecture where various models of access control are evaluated during integration of cloud technologies.

A large-scale cyber physical system can utilize cloud services to meet its enormous computing requirements. However, the use of untrusted cloud for computation can give rise to data privacy issues in CPS. Zhiheng et al. [11] described a safe and practical mechanism for secure outsourcing of a large-scale CPS output feedback control issue. The strategy used combines a standard homomorphic encryption (SHE) and a customized homomorphic encryption (CHE), enabling the cloud to perform operations on the ciphertexts and return the expected outcome.

Cyber physical systems (CPSs) generates large amounts of data which are stored in the cloud. In the absence of any special protection, the data can get in the hands of the malicious user or third party for unauthorized use. To address cloud computing data storage and data sharing issues Shuaishuai et al. [10] described a new tree-based dataset management model. Data encryption, data proof and data boundary maintenance are few operation techniques which are extracted from different entities view in the cloud. The view management on the tree controls behaviors of different users. To ensure the privacy of entities, availability of data and secure transmission of data a flexible data management mechanism is described in this model.

Nurul et al. [9] discuss the challenges associated with a cloud based cyber physical system attacks and emphasizes the need for forensic-by-design and also proposed conceptual cyber

physical cloud system (CPCS) forensic-by-design model. The framework described by Nurul et al. consists of six elements which are as follows: principles and practices of risk management, principles and practices of forensic readiness, principles and practices of incident handling, laws and regulations, requirements for CPCS hardware and software and requirements specific to the industry. When forensics tools are combined with cyber physical cloud system in forensic-by-design framework, it enables organizations to quickly recover from cyber physical attacks.

Vehicular cyber physical systems with context-aware cloud based services is proposed by Wan et al. [4]. Context-aware vehicular clouds consists of three types of architecture. Vehicles use cloud based services through roadside infrastructure in the first type. A group of vehicles enables external customers to use their computing systems in the second type. The first two are combined in the third type. Context aware vehicular security mechanisms is also proposed by Wan et al. whose implementation requires a framework which includes collection of data, detecting malicious activity, management of trust and policy.

Demand response (DR) systems is an example of cyber physical system which include a cyber communication element and physical control element. Since DR systems often handle random occurrences, they intrinsically require considerable variation in the number of resources needed for computing. Although cloud technology adapts to such changes by default, it creates severe security risks in DR systems. Mission critical applications often contains cyber physical systems to operate physical processes. Thus, attacks on CPS can cause major harm to DR systems [2].

Cloud based industrial CPS is presented by Colombo and Karnouskos [15]. New security threats are created by cloud computing and its connectivity. Major factors of threat on-device or in-cloud includes the type of functionality, degree of reliance on external resources, computing capacity, operations, and connectivity of networks. The cyber part should be separated from cloud and physical devices with suitable interaction in cloud based design, development, and operation.

3. CONCLUSION

This paper presents a literature survey on cloud cyber physical systems (CCPS) and security issues related to it. CCPS provides effective solutions to the issues in today's world. Cyber Physical Systems have changed the way how humans interact with the physical world. Integrating the cloud and cyber physical systems have improved the computational power and storage need of large amount of data. But CCPS poses high security risks due to its complex behavior and highly distributed nature. CCPS have an additional attack vector as cloud which poses new security challenges in addition to security issues of traditional cyber physical systems. CCPS security issues such as Cyber-attacks, Real time Monitoring, Access control, Rootkits, Data storage and Data management problem have been discussed in this paper.

4. ACKNOWLEDGMENTS

Research reported in this publication was supported by K J Somaiya College of Engineering, Vidyavihar Mumbai, University of Mumbai.

5. REFERENCES

[1] F. F. Han et al., "Virtual resource monitoring in cloud computing," J. Shanghai Univ., vol. 15, no. 5, pp. 381–385, 2011.

[2] A. Mohan and D. Mashima, "Towards secure demand-response systems on the cloud," 2014 IEEE Int. Conf. Distrib. Comput. Sens. Syst., pp. 361–366, 2014.

[3] Amazon. (2019, 2) Amazon ec2 faqs. [Online]. Available:http://aws.amazon.com/ec2/faqs/

[4] J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions," IEEE Commun. Mag., vol. 52, no. 8, pp. 106–113, 2014.

[5] M. Ficco and M. Rak, "Intrusion tolerance in cloud applications: The mOSAIC approach," 2012 6th Int. Conf. Complex, Intelligent, Softw. Intensive Syst., pp. 170–176, 2012.

[6] A. Chonka and J. Abawajy, "Detecting and mitigating HX-DoS attacks against cloud web services," 2012 15th Int. Conf. Network-Based Inf. Syst., pp. 429–434, 2012.

[7] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," 2009 Fifth Int. Jt. Conf. INC, IMS IDC, pp. 44–51, 2009.

[8] M. Armbrust *et al.*, "A view of Cloud Computing," *Commun. ACM 53*, vol. 4, 2010.

[9] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K. K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," IEEE Cloud Comput., vol. 3, no. 1, pp. 50–59, 2016.

[10] S. Zhu, Y. Han, and Y. Wei, "Controlling Outsourcing Data in Cloud Computing with Attribute-Based Encryption," in 2015 International Conference on Intelligent Networking and Collaborative Systems, 2015, pp. 257–261.

[11] Z. Xu and Q. Zhu, "Secure and practical output feedback control for cloud-enabled cyber-physical systems," in 2017 IEEE Conference on Communications and Network Security (CNS), 2017, pp. 416–420.

[12] Y. B. Reddy, "Cloud-based cyber physical systems: Design challenges and security needs," 2014 10th Int. Conf. Mob. Ad-Hoc Sens. Networks, pp. 315–322, 2014.

[13] L. Zhang, S. Shetty, P. Liu, and J. Jing, "RootkitDet: Practical End-to-End Defense against Kernel Rootkits in a Cloud Environment," in Computer Security - ESORICS 2014, 2014, pp. 475–493.

[14] N. Wu and X. Li, "RFID Applications in Cyber-Physical System," Deploying RFID - Challenges, Solut. Open Issues, pp. 291–302, 2011.

[15] Colombo et al., "Industrial cloud-based cyber-physical systems," The IMC-AESOP Approach, 2014.

[16] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A Secure Service Provisioning Framework for Cyber Physical Cloud Computing Systems," Int. J. Distrib. Parallel Syst., vol. 6, no. 1, pp. 1–11, 2015.

[17] J. Lopez and J. E. Rubio, "Access control for cyber-physical systems interconnected to the cloud," Comput. Networks, vol. 134, pp. 46–54, 2018.

[18] K. An, S. Pradhan, F. Caglar, P. Patil, S. Shekhar, and A. Gokhale, "Cloud Computing for Cyber Physical Systems: Reliability and Security Challenges and Solutions," Dre.Vanderbilt.Edu, no. 1, pp. 2–5.