Cloud Assisted IoT Application's Security Attacks and their Countermeasures

[1.] Devidas Kalaskar
Assistant Professor,
Department of Computer Science,
Govt. Women's First Grade College, Kalaburgi
Akkamahdevi Women's University, Vijayapura

[2.] Manjunath V
Assistant Professor,
Department of Computer Science,
Govt. First Grade College, Gurumatkal, Yadgir
Gulbarga University, Kalburagi

Abstract— **Internet of things is an developing technology having the quality to improve the different aspects of human life. Furthermore, integration of IoT with cloud computing has allowed the wide range of applications in different areas such as commercial, manufacturing, engineering, supply chains, etc. Currently security threat obstacles the adoption of IoT technology in many areas. This paper presents the architecture of cloud assisted IoT applications for smart cities, telemedicine and intelligent transportation system. We investigate the security threats and attacks due to unauthorized access and misuse of information collected by IoT nodes and device. Further, we describe the possible countermeasure to these security attacks.**

Keywords- IoT; Cloud Computing; Smart cities; intelligent transport system; Telemedicine;

1. INTRODUCTION

The Internet of things (IoT) consists of combined different sensors and objects that can collaborate with each other with no human interference necessary. The "things" in the IoT comprises objects, such as cars, microwaves, refrigerators, toaster, air conditions etc, which collect useful data from its surroundings with the help of sensors and transmit this to the other connected devices that take actions/decisions based on it. In other words, it can be said that IoT is an architecture that encompasses smart embedded devices that are connected to Internet so they can be controlled and triggered by internet.

It is estimated that by the end of 2020, around 30 billion objects will become the integral part of global IoT network, which will pose new challenges in securing IoT systems. It will become easy target for hackers as these systems are often deployed in uncontrolled and hostile environment. The main security challenges in IoT environment are authorization, privacy, authentication, admission control, system conformation, storage, and administration. There are security solutions available already for Internet, which should be equally applicable to IoT networks as well. However, constrained resources, different operational environment, and complex interconnectivity among huge number of devices in IoT make those security solutions insufficient.

The IoT systems are prone to various different types of security attacks: Denial of Service (DoS), Jamming attacks, Sybil attacks, blackhole attacks, wormhole attacks, and malware attacks etc. Even after implementing proper security solutions in IoT devices, there are still possibilities of different kind of attacks on the network. Therefore, proper security can be ensured by providing patches as soon as any vulnerability has been identified in the system. The devices must have updated regularly with those patches in order to avoid unfavorable circumstance caused by exploitation of identified vulnerabilities. IoT systems have direct effect on everyday life of its users so there is need to provide well-defined security mechanisms and procedure in those systems in order to protect from possible security attacks and threats. This paper aims to review the current security issues and vulnerabilities of the IoT applications in area of smart city, telemedicine and intelligent transportation system. We discuss possible counter measure for various security attacks in order to minimize risk and improve IoT security.

The rest of paper is organized as follows. Section 2 describes the integration of cloud computing with IoT. Section 3 describes the different cloud assisted IoT applications. Section 4 discusses the security attacks and possible countermeasures. Section 5 presents the security architecture of IoT integration with cloud computing and lastly Section 5 concludes the article.

2. CLOUD COMPUTING AND IOT

Presently, cloud computing provides a new generation of computational systems, cloud represents a software and hardware resources which provide a high availability of their services through web and accessible through a broad types of devices. However, the cloud could create its own services through IaaS (Infrastructure as a Service) [22]. The flexibility and availability of services provided by cloud allow users to tune their requirement according their preferences such as time, cost, priority etc.

On the other hand, the developments in Internet of Things (IoT); is the networking of physical smart devices, constructions, and other items which enable these senores to give-and-take data [23] [24] [25]. Cloud computing is web based computing system provides a computation services for wide range of devices each with its own specific requirement. The cloud model allowing ubiquitous, on-demand access to set computing assets (e.g., servers, software, hardware storages,).

In the IoT, cloud computing technology could be utilized to process the huge data produced by sensors smoother and provides the IoT devices with storage and processing resources on-demand [26]. It also provides high processing capabilities, inexpensive services, flexibility, and high availability services [27].

By combining cloud into IoT the sensors data could be stored and processed in real-time which provide a scalable and more reliable solution. The issue need to be considered is power limitation and access control and variable connectivity [28].

However, cloud users confronted by many security challenges such as, access management, Denial of service (DoS), data access controls, and hardware security [26].

3. APPLICATIONS

There are plenty of applications utilizing cloud assisted IoT technologies. This section discusses the three main applications in this area:

A. Smart Environments and Smart City

Smart city concept is defined as the combination of conventional infrastructure and modern information and communication technologies to boost operational productivity, efficient resources utilization and assets management, and enhance the quality of government services and citizens welfare. Smart city infrastructure is implemented by collaboration between government, and public and private organizations.

Although, smart cities concept is attaining publicity nowadays, there is no single existing city that accomplish all requirements for a smart city. Rather, we could refer to it as smart technologies that can provide solutions for cities by helping them to manage resources efficiently, cost-cutting, reduce carbon dioxide emissions and traffic management, improved circulation, safe and easy information access to connect people-to-people and people to services as a community. Some of the smart technologies relevant for smart cities include energy, buildings, mobility, authority and education, and healthcare. Smart city applications implementation use notions from the area of artificial intelligence, embedded computing, machine learning, cloud computing, heterogeneous networks, and biometrics. In addition, it makes use of different components including sensors, RFIDs, computing and networking objects to maximize the usage of resources in different applications.

Managing various services in smart city requires a complex network infrastructure. Each connection is at risk and susceptible to a security threat; the amount of access points is folded in smart cities. It is possible to attack and halt the entire system or network by only compromising a single point.

Smart city applications are monitoring and recording the citizen's private information therefore, it is critical to properly secure this data. Possible threats to smart cities infrastructure are eavesdropping, theft, denial of service, failure of hardware or software, manufacturing bugs, insufficient testing and natural disasters. Security risks are mitigated by utilizing solutions such as: intelligent threat detection and advanced proactive antivirus protection.

B. Telemedicine or E-health

Thee Health concept is used to describe the new "model centered on consumer" of health systems, that combine the health science and technologies with information and communication technologies that can be used as a key solution to provide significant health benefits at individual level as well as at society level [3]. IoT has a high potential to improve the human health and safety.

In health sciences, technologies have been developed in recent years based on their capabilities to monitor various health parameters [4], that can be now transmitted by health devices via a gateway onto secure cloud base platforms where they are stored and analyzed [5]. Data gathered from these devices can be stored and analyzed by the medical specialists helping them in diagnosis and enabling the possibility to monitor the patient from any location and responding timely manner, based on the alert received[6].

Tele medicine or E-health systems are used to collect and process confidential and private data of patients so it requires an infrastructure that should provide high level of security and privacy [14]. E-health system provider would have to bear severe consequences and legal penalties in case of disclosure of health data intentionally or accidently for infringing privacy laws.

In this context, health data is secured by providing confidentiality, integrity, authenticity, and availability services. Privacy of health data is assured by acquiescence with personal data protection laws and regulations. This will promote the acceptance of e-health system by users with high confidence that their personal confidential health data is protected and secure.

C. Intelligent Transportation System

Intelligent transportation system (ITS) is application which utilizing several technologies aiming to improve safety, mobility and proficiency in public transportation.

Some of the technologies relevant for intelligent transport include:

a. **Traffic control**: Smart traffic lights control technology aims to minimize the amount of time that cars spend idling and ensure smooth flow of traffic.

b. **Public transport surveillance**: As the public transit population grows, it becomes increasingly important to utilize surveillance system on the public transport to ensure the safety and security of public transportation. The public transport can remotely be monitored and take action against any accidents/incidents.

c. **Parking** A smart parking controls parking sensors to provide efficient usage of the parking spaces and utilizing time and energy.

Principally, the security requirements of ITS traffic and mobility data comprise confidentiality, integrity, availability, authentication and non-repudiation. Vehicular adhoc networks (VANET) are important part of ITC and have particular characteristics including absence of central control, intermittent connectivity of vehicles, high mobility, dynamic network topology and hard delay constraints, which make it more challenging to provide these basic security requirements. Along with security, the other most important requirement is to provide privacy to ITS users. It is hard to deliver security and user privacy simultaneously. The users are likely not to share their identities and location history with ITS central authorities while requiring security at the same time making it contradictory to achieve. One of the possible solutions is to provide user security along with anonymity to protect its private information.

Possible ITS attackers are nation states, criminal gangs, hack typists, cyber terrorists, insiders, unscrupulous operators, and natural disasters. ITS attacker motives are ransom, data theft, information warfare, system gaming, theft, revenge, and terrorism.

Possible attacks on ITS can be categorized into three different categories i.e physical attacks, networks attacks, and wireless attacks. These three different types of attacks are overlapping with each other in the sense that one attack leads to another or make it possible to instigate another.

ITS infrastructure smart devices such as cameras, digital signboards are under the physical access of anyone on roadways and roadsides. The attacker can gain access to these devices by physically connecting through different exposedportsi.e.USB,PS2, serial, etc. After gaining access to device, the attacker can get login credentials by brute force or guessing attack. Once attacker has successfully login to the physically accessible device then he can use this device as an entry point in to the network perform different network attacks on ITS infrastructure.

4. ATTACK AND COUNTER MEASURES

This section describes the security attack and possible counter measures for different cloud assisted IoT applications discussed in previous section.

A. Denial of service(DoS)Attacks

The safety of the drivers and vehicles is ensured by the availability of ITS systems. Looking into this context, denial of service (DoS) attacks are presently identified as the most serious threat to the availability of ITS systems, because of their significant influence at the network assets. Definitely, the principle goal of these attacks is to restrain legitimate users from the usage of the network resources and services [8]. Furthermore, distributed denial of service (DDos) is a type of DoS attack, where several infected systems, are used to launch a Dos attack against a single victim and making it more difficult to identify the real attacker [10].

B. Jamming Attack

This attack mainly targets the wireless networks and carried out by hindering the communication channels by transmitting the unwanted messages or high frequency noisy signals in order to corrupt the contents of original message or block it to reach the destination. The jammer can be insiders and part of the network or outside. These attacks are detected or prevented by different mechanisms, which employ the cryptography and steganography algorithms. Some of the counter measures include the developing reputation systems, credit-based systems, and communication-intensive acknowledgment schemes [11].

C. Sybil Attack

In Sybil attack the malicious node present itself in the network with multiple identities. Legitimate nodes in the network are unable to find out that the received messages are originating from a single node or multiple other nodes. The objective of the attacker is to have an effect on the network based on his aspiration. This attack is prevented by employing the identity based validation of nodes in the network by central authority which guarantee a one-to-one mapping of an identity and a node. Moreover, other countermeasures to Sybil attacks are trusted certification, resource testing, privilege attenuation, location verification, and message authentication and passing [12, 13, 14].

D. Blackhole Attack

Like Sybil attack, black hole attack also shapes the networks as per attacker's desire. All types of adhoc networks including ITS, smart cities and e- health are susceptible to this attack. In this attack the malicious node shows its active participation in the network routing communication in such a way that most of traffic goes through it. It received all the communication messages from different nodes in the network but do not forward any of it to its correct destination and simply discard them which results in heavy packet loss in the network. These attacks are very harmful for latency-sensitive applications such as road safety, emergency patient treatment, and disaster recovery applications. Secure proactive and reactive routing protocols are proposed in literature to detect and prevent this attack by finding the correct routing path and discarding them malicious routing messages from the attacker nodes [15].

E. Worm hole Attack

A wormhole attack require the participation of at least two attacker nodes namely “A” and “B” which are geographically located distant apart from each other. During this attack, the attacker node “A” sends encapsulated a routing message to attacker node “B” which broadcast this routing message to its neighborhood. As packet is encapsulated so hop count will not be decremented by intermediate nodes between “A” and “B” and when it is received by neighborhood of B, they would believe node “A”as their neighbor. The purpose of this attack is to create unreal routes in the network in order to gather or alter large quantity of network traffic, routing disruption, traffic analysis, or selective drop of date packet. This attack can be launched without compromising any legitimate node in the network or without the knowledge of any cryptographic mechanism. Worm hole formation can be prevented by using specialized hardware which provides information of time of flight, geographical position or signal direction information. Wormhole attacks can be detected by different mechanisms such as location free network planarization techniques [16] timing analysis [17], wireless election algorithm coordinator [18, 19].

F. *Malware Attacks*

Malware is a short form of malicious software, these are the intrusive programs comprising computer virus, worms, ransom ware, and trojan horse, which are designed to execute on infected system without the user consent and harm the infected system. Leading malware threats on IoT enable smart cities infrastructure can not only influence the city and its administration, but also the residents and businesses which inhabit there[20]. These attacks usually exploit those vulnerabilities in the systems, which are not updated timely or not configured properly while installing the devices. Popular countermeasures of such attacks are the use of anti-malware, anti-virus software, and timely software update with cryptographic signing verification [21].

CONCLUSION

Utilizing cloud computing in the IoT environment facilitate storing and processing of large amount of data in a real-time applications. However, the common IoT security architecture and standard of IoT is not enough for highly dynamic and heterogeneous networks. On the other hand, IoT faces a main challenge, which is the lack of a common security standardization frame. There is a need to adopt a dynamic defense based mechanism. This paper discusses the main security attack and possible countermeasure on well know real-life IoT applications.

REFERENCES

[1] Z. Yan, P. Zhang, A.V. VasilakosA survey on trust management for InternetofThingsJ.Netw.Comput.Appl.,42(2014),pp.120-134

[2] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D.QiuSecurity of the Internet of Things: perspectives and challenges Wirel. Netw., 20 (8) (2014), pp.2481-2501.

[3] S.E. Colesca, L. Dobrica, “The e-Health concept”,Economia, Management, vol.12, no.1, 2009.

[4] Konrad Lorincz, David J. Malan, Thaddeus R.F. Fulford-jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoffrey Mainkand,Matt Welsh, Steve Moulton, “Sensor networks for emergency response: challenges and opportunities“, IEEE Pervasive computing, vol. 3, no. 4,2004.

[5] Chiuchisan I., Costin H.N., Geman O., Adopting the Internet of Things Technologies in Health Care Systems, Proceedings of The 2014 International Conference and Exposition on Electrical and Power Engineering (EPE2014), Workshop on Electromagnetic Compatibility and Engineering in Medicine and Biology, Iasi, Romania, 2014, 532-535,2014.

[6] Chiuchisan, I. Chiuchisan and M. Dimian, "Internet of Things for e- Health: An approach to medical applications", 2015 International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM), 2015.

[7] Daniel Minoli ,Kazem Sohraby , Benedict Occhiogrosso, “IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications” IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE),2017.

[8] Hamida, Elyes ben, Wassim Znaidi and Felipe Jimenez. “Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures.”(2015).

[9] Gartner, Inc. It can be accessed at https://www.gartner.com/newsroom/id/2905717

[10] Pelechrinis, K., Iliofotou, M. and Krishnamurthy, S.V., “Denial of service attacks in wireless networks: The case of jammers”, IEEE Communications Surveys & Tutorials, 13(2), 245–257, (2011).

[11] L. Lazos, M. Krunz Selective jamming/dropping insider attacks in wireless mesh networks IEEE Network, Volume 25, Issue 1, pp. 30- 34,2011.

[12] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, “Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method,” The Scientific World Journal, vol. 2015, Article ID 841267, 7 pages, 2015.doi:10.1155/2015/841267

[13] Xiao, B.; Yu, B.; Gao, C. Detection and localization of sybil nodes in VANETs. In Proceedings of the 2006 Workshop on Dependability Issues in Wireless ad Hoc Networks and Sensor Networks, Los Angeles, CA, USA, 29 September 2006; ACM: New York, NY, USA, 2006; pp.1–8.

[14] John, RincyMedayil et al. “A survey of techniques to prevent sybil attacks.” 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (2015):1-6.

[15] Tseng, FH., Chou, LD. & Chao, HC. "A survey of black hole attacks in wireless mobile ad hoc networks" Human-centric Computing and Information Sciences, Vol 1, Number 1, November2011.

[16] Xiaopei Lu, Dezun Dong, Xiangke Liao. “WormPlanar: Topological Planarization Based Wormhole Detection in Wireless Networks”. ICPP 2013: 498-503

[17] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, “Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks”, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 2, FEBRUARY 2009.

[18] R. Arun Prakash, W. R. Salem Jeyaseelan and T. Jayasankar. “Detection, Prevention and Mitigation of Wormhole Attack in Wireless Adhoc Network by Coordinator” Appl. Math. Inf. Sci.12, No. 1, 233-237(2018).

[19] R. Maheshwari, J. Gao, and S. R. Das, “Detecting wormhole attacks in wireless networks using connectivity information,” in Proc. INFOCOM2007.

[20] Byungho Min , Vijay Varadharajan, “Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT)”,EngineeringofComplexComputerSystems(ICECCS),2015.

[21] https://www.csoonline.com/article/3148157/security/top-malware-threats-for-smart-cities.htmlaccessed on 16th Feb2018.

[22] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. 2009. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility". Future Gener.Comput. Syst. 25, 6, pp.599-616, Jun2009.

[23] CIGREF, " Cloud Computing basics - Large companies' perspective", March2013.

[24] Brown, Eric (13 September 2016)."Who Needs the Internet of Things?". Linux.com. Retrieved 23 October2016.

[25] Brown,, Eric (20 September 2016)."21 Open Source Projects for IoT".Linux.com.

[26] Brown,, Eric Retrieved 23 October 2016."Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.

[27] Horrow, S., Anjali, S., 2012. Identity management framework for cloud based Internet of Things. In: Proceedings of the First International Conference on Security of Internet of Things, SecurIT ’12 ,200–203.

[28] Botta, A., De Donato, W., Persico, V., Pescapé, A., 2016. Integration of cloud computing and internet of things: a survey. Future Gener. Comput. Syst. 56,684–700.