CLOUD SECURITY: ONGOING CHALLENGES IN IoT

Alka Verma[1], J. C. Patni[2], Amit Agarwal[3]
[1]Research Scholar, [2,3]UPES, Dehradun

ABSTRACT

The ongoing challenges in "Internet of Things" (IoT) are explicitly allied to the wide-scale applications of its system. IoT brings out opportunities for wearable devices, healthcare systems, home appliances, and various small devices communicating over internet. Ubiquitous or pervasive nature of small devices challenges the security and privacy of the data. Moreover the storage and flow of information via cloud is always subjected to many challenges like integrity, transparency, and identity from the perspective of wide-scale applications. In this paper we discuss and analyse various ongoing challenges involved with IoT in a cloud deployed environment. We primarily focus on security and privacy concerns from the perspective of service providers and users in the cloud.

Keywords: Internet of things, pervasive computing, ubiquitous computing, Cloud deployment environment.

I. Introduction

Kevin Ashton was the one who introduced the term "The Internet of Things" (IoT) for the first time almost a decade ago [1]. IoT is expeditiously gaining pervasiveness, not only in commercial and industrial environment, but also in our day to day life through small smart devices and systems at our home. In IoT every entity whether it's virtual or substantial is accessible, communicable and addressable via cloud services. IoT significantly consists of various wide scale applications. Small smart system like noise and home monitoring system, congestion detection, real-time vehicle networks, and smart framework are few applications of IoT [2]. Many personal health and life care systems inherits the health care services [3]. Diverse wide scale applications of IoT are commonly interconnected via cloud deployed environment that provides easy and global access. Due to the miniaturization of the devices there is increase in computational power and deduction in the consumption of energy, IoT will remain the centre of attraction [4]. Ubiquitous or pervasive nature of the small objects increases the need of the security and privacy while transmitting the data for public or private use. With various heterogeneous devices connected and communicating with each other via cloud services, IoT brings forward the concern of security and privacy like confidentiality, authenticity, integrity of the data, as huge data is associated with them. Many of these devices store basic security system, which is unable to handle the confidentiality and integrity of the data, thus these small devices are much vulnerable for intrusion and can be attacked easily by an attacker, also these devices rely on very few outside resources and are often left unattended. Security and privacy remains the key challenges in the IoT. This paper briefly discusses the ongoing challenges in IoT from the perspective of security and privacy in a cloud deployed environment.

The cloud acts as a base technology for open data sharing; the data is transmitted and shared between various heterogeneous devices and applications. Section –II gives an overview of challenges in IoT, while communication and global access via cloud. The IoT architecture inherits the cloud as a basic component [5]. Cloud is scalable and can serve several of systems, services, and devices. Security challenges in IoT-cloud are discussed in section – III. Identifying billion of devices and authentication of all those devices in IoT is a tedious task to perform. Identification mechanism being one of the important challenges is described in section - IV. Different devices connected and communicating with each

other and applications in IoT raise the concern of trust, transparency and certification. Section – V referred to all such challenges. Section – VI concludes the important considerations in Internet of Things (IoT) with references at the end.

Cloud provides an infrastructure which is scalable and can do variety of services for you. Cloud being the basic component of an IoT architecture [5], we consider an IoT architecture which inherits the cloud infrastructure and unifies cloud services. The IoT architecture scales to various applications which can be built on the same devices. Various heterogeneous devices behind firewall or low-level sensor network have gateway and through cloud services access open or wide scale application and communicates, and shares data.

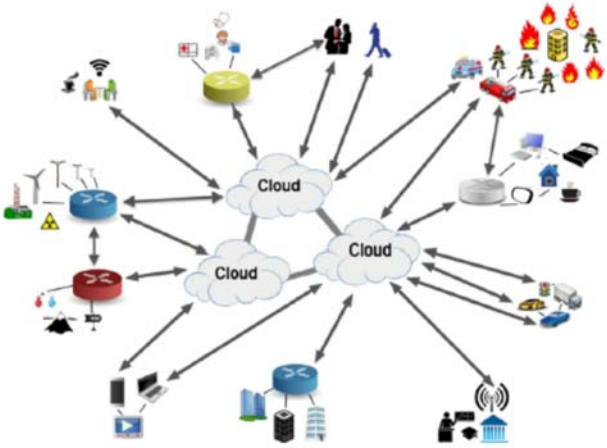

Fig. 2 Connectivity in IoT in cloud deployed enviornmet

The above figure shows connectivity in IoT "things" unifying cloud services. Cloud computing [6] – [8] is an important paradigm in which cloud service provider provide services to their customer (tenants) to host their application or use the computational resources. The tenant can in turn provide services to the end-users of a system. The consumer (end-users) of the system can communicate with cloud provider of their own or could with the help of services provided by the tenant. Clouds consist of three important components: **first**; The three types of models based on the type of services provided.1) software as a service (saas), where any software is provided as a service and everything else is managed and controlled by the service provider.2) platform as a service (paas),where the user is allowed to develop or host and mange his own application, thus platform is provided as a service.3) infrastructure as a services (iaas),where user can process, store or use any other computing resources, the underlying infrastructure is provided as a service to the user. **Second**; Three types of cloud models on the basis of their deployment.

1) Public, where anyone can access the public cloud and can store data, process and, use the services provided.

2) Private where a single organization owns and manages the services provided by the service provider, and its resource access is limited to its users only.

3) Hybrid consists of both public and private, the use of the public and private cloud depends upon the sensitivity of the data and **third**; Important features like Broad Network Access, providing elasticity, Measured and On-demand services. All this three parameters defines an architecture cloud. Virtualization [9] is an important aspect in Infrastructure as a service. In paas or iaas, various "things" could interact with the applications which could be in turn tenant itself. The service provider manages and controls the underline cloud infrastructure, such as Amazon [7] and Microsoft [8]. Any small sub system or device is considered as a thing. These sub system generally have a gateway component, and via cloud services connects and share data across the wide-scale applications.

II. Challenges in IoT while communication and global access via cloud

Communication between things and cloud demands secrecy and integrity. The data could be store up in the cloud and the cloud could be the channel via which the data is sent to the sub systems or small devices. With various heterogeneous devices connected to the internet security and privacy always remains the challenge as huge volume of data is associated with it [10]. The devices which do not have any malware protection are easily subjected as "bolts" to carry forward malicious code to infect other devices [10]. Moreover, by compromising the network layer it becomes very easy to access the devices maliciously and to attack the nearby other devices with the help of indigenous compromised node. Secure communication needs to prevent any unauthorized access to the sensitive data. Security threat at the transport layer are handled by TLS(Transport layer security) [11] by encrypting the data link, and

using cryptography in order to provide a secure transmission from both eaves dropping and interference. Where as to maintain the integrity, confidentiality, and authenticity, protection of the data is provided at the network layer by IP Sec [12]. Data security in IoT is one of substantial issues. Some small devices used by IoT stores basics security mechanism which can cost integrity and confidentiality of the data. In place of TCP/IP, TLS over protocol stack is preferred. TLS is the basic attribute of cloud-provider offerings, and thus can be used to protect integrity and confidentiality of the data [5].

Other than TLS, the data can be secure during the transmission, could it be end-to-end encryption in order to attain higher level of security protection. Also, Access control [13] to the cloud resources should be controlled and action taken on external should be guaranteed, be like accessing any specific record or performing some computation within data, etc.

Authentication and authorization are the important methods to control access to various resources. Authentication refers to verify the right person who claims to be and authorizations rules the kind of action that right person is authorized to take.

In IoT, access control has been a challenge as the interaction between the devices raises the concern over authentication and authorization. Trusted platform modules (TPM) [14] guarantee the device configuration [15] and device identity [16], whose benefits can be associated to the access controlled mechanism.Various heterogeneous devices in IoT communicates and stores their data up in the cloud. The transit of data and its storage via cloud services thus should be secured.

III. Security Challenges in IoT:

Majorly four layers need to be made secured in order to make IoT reliable and secure. Various heterogeneous devices should be monitored to prevent any alteration or loss of data. Security challenges at different layers are discussed below:

1. Application layer: Security compromise at this layer can cause bugs in the program code causing malfunctioning of the application. This could be menacing for numbers of devices grouped as application level entity [17,10,18] .Different level of security is needed for different types of application environment. One of the objectives of application layer is to share data, thus data privacy and its access control always remain a challenge.
2. Perceptual layer: The major security challenges at perceptual layer are at node level. Having low storage capacity and power, these are vulnerable to attacks from hackers. Mainly attacks from the outside network are associated with the data gathering or sensors which brings into the scope of protection for data integrity, confidentiality and authenticity.
3. Network layer: Security mechanism at the network layer is very significant to the IoT. The major security challenge at this layer is with respect to the authenticity and integrity of the data travelling through the network. Moreover, this layer carries huge volume of data. Any malicious attack can cause network congestion. Any attack from any malicious node or a hacker that compromise a device in the network is a crucial issue.
4. Physical layer: At this layer, there is a great requirement of advanced technologies to protect sources and substantial security system. Devices needs to be safeguard from any kind of physical attack, both from personalized perspective or environmental. Hardware failure, physical damage or tampering, loss of power, weather attacks are the common challenges at this layer.

IV. Identification of “things “

In IoT, identifying billion of devices is very difficult task. Major security concerns in IoT involve authentications, identifications and device heterogeneity. We discuss in section II/IV authentication and authorization, the key aspects to access control and thus maintaining the confidentiality and integrity of the data. There are different types of devices in IoT and each device has different security requirement. In this paper, we are concern about the identification of different “things” interconnected and communicating via cloud service provider in the cloud. We broadly discuss the identification of “things” from the tenant perspective i.e. the one that uses the services provided and the one who provide the services.

Identity management has been an area of focus, especially in lately venture services; we have identification management schemes [19] [20], from cloud services to application providers like Google, Amazon, Microsoft Services, etc.

IoT comes up with the other considerations too as it involves various things sharing and accessing the data. In cloud the end-users interacts with various services provided by the service provider and many applications hosted by the tenants. In an environment of IoT, many "things" can send data to the service provider. For example, any user could have hundreds of different data sources sending data to the service providers, few of which could transits through dedication channel and other might be uploading to shared resources or applications. Thus, there is a need to identify the "things" after which it can be specified to which tenant or user the "things" belongs, for this TPM [14] mentioned in section III can be used. For example, healthcare system or house monitoring systems have policies specific to the user requirements. Data collected by sensors and transferred to the other devices to be analysed is sensitive data and needs to be hand over to the right person. It should be a matter of concern that the right "things" communicates with right resources or services provided by the service provider, so that the right data should flow to the right service of cloud, also, it is necessary that right course of action should be generated for the right person(could be a tenant or end-user). For example, if a "things" generates relevant data for different application hosted on different platforms then the "things" should be guided to which place and at what time data should be sent. The "things" should know all the aspects for communication between the different cloud services, and should follow the protocols or the policies which determines that the things should interact to which cloud. There are issues associated with the "things which needs to be taken into consideration like how to manage a communication of a user with a sensor, and what could be the transfer policies which governs the data flow. Such all are complex issues which needs consideration. Further, the identity of "things" becomes complicated when the actuators knows which "things" to actuate. The data gathered could be a source of an attack, when this data is processed, could lead to an unusual behaviour of other sub-systems or things in the system. The data collected from these devices can be used to gain user details which may not provide the confidential data but however, can release sensitive information. For example, some one possesses any particulars device could reveals about the medical conditions [21]. Cameron [22] defined seven fundamental laws for digital identities.

V. Trust and transparency

Managing the equilibrium between trust in the service provider and the tenant privacy is a big challenge in IoT. Whenever we go and adopt a new technology then there is a lot of trust and risk related issues to be addressed. The prospective tenant should trust the service provider before committing to the use of cloud service. The tenant relies on provider to ensure; 1) Data security and privacy; 2) Resource availability; 3) Monitoring and repairing of services/resource. Trust and risk are the opposite sides of the same coin and when we look at trust, it becomes important from the notion of accountability and verifiability. Currently, regulatory compliance can be manifest by certification [23]. The automation of the process of certification has been considered [24]-[26] but being a human centred process, certification evaluates the behaviour of a system at the time of audit [5]. Any amendment or arrival of new framework has to undergo the recertification process which could be costly and time taken. From the perspective of security some aspects of compliance could be structured [27], [28]. The amount of trust which can be put up in a cloud service provider consider the following issues; 1) a secure there services; 2) correctly configuring the services; 3) should report any leakage/issues, if any; 4) provided data should be used for the predetermined purpose. To strengthen trust it is necessary to provide some amount of transparency on the top of the services provide by the cloud service provider. Recent developments in hardware technologies [29] bring trust to a new level, providing TPM [14] and remote attestation for cloud computing [30], this strengthens the trust between the cloud service provider and its service user for example, the confidentiality and integrity of the data is guaranteed irrespective of the platform on which data is attended [31]. Further, some visibility or transparency should be provided in the functionality of the service provider could be for the purpose of compliance, or for more general assurance, of data management.

VI. Conclusion

In the last few years, the internet of things (IOT) has gained significant interest; IOT is emerging as a new domain and will continue for the coming years. Despite of much research done in this area, IoT still remains and is facing severe challenges. With the connection and communication between various heterogeneous devices, Security and privacy remains the primary concern. In this paper, we discuss the ongoing challenges in IoT like authentication, identification, integrity and transparency along with security and privacy. We consider the use of cloud services for open data sharing and communication between various "things". Data sharing being a congenital part of IoT, involves severe security and privacy issues, which should be always taken into consideration.

REFERNCES

[1]Aqeel-ur-rehman, sadiq-ur-rehman, Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan: Security and privacy issue in 107, Vol…. No.3, December 2016

[2] A. Zanella, "Interest of things for smart cities," IEEE interest things J., Vol. 1, No.1, pp. 22-32, Feb 2014.

[3] J. Bacon et al. , "Personal and social communication service for health and lifestyles monitoring," in Proc. 1st Int. Conf. Global Health challenges (Global Health' 12) IARIA Data sys 2012, Vence Italy, 2012, pp. 41-48..

[4] Silverajan, B. Harju, J.: Developing network software and communications protocols towards the interest of things. In proceeding of the Fourth International ICST Conference on communication system software and middleware, COMSWARE 2009, Dublin, Ireland, June 16-19, pp. 1-8 ACM, New York 2009

[5] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko and David Eyers; Twenty security consideration for cloud-supported Internet of Things, IEEE INTERNET OF THINGS JOURNAL Vol. 3, no. 3, June 2016.

[6] L. Yousett, M. Butrico, and D. Da Silva, "Towards a unified ontology of cloud computing," in Proc 2008 and computing Environments workshop.

[7] Amazon Inc., "Amazon elastic compute cloud (Amazon EC2)," 2011 Available: http://aws.amazon.com/ec2/

[8]"Window Azure" Available: http://www.windowsazure.com/en-us/

[9] J.E. Smith and R. Nair, "the architecture of virtual machines," IEEE Internet Comput. , May 2005.

[10] Xu Xiaohui."Study on Security Problems and Key Technologies of The Internet of Things Fifth International Conference on Computational and Information sciences(ICCSEE) ,pp.648-651,2012.

[11] T. Dierks and C. Allen, "The TLS protocol version 1.0," IETF, Tech. Rep., RFC 5246, 1999 [Online] Available: https://tools.ieft.org/html/rfc5246

[12]Huisuo, Jiafu Wan, Caifeng Zou, Jiangi Liu, Security in the Internet of things: A review, 2012 internal conference on computer science and Electronic Engineering.

[13] R.J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Hoboken, NJ, USA: Wiley, 2008.

[14] T. Morris, "Trusted platform module," in Encyclopedia of Cryptography and Security, New York, NY, USA: Springer, 2011, pp. 1332-1335.

[15] M. Hutter and R. Toegl, "A trusted platform module for near field communication," in Proc. Int. Conf. Syst. Netw. Commun. (ICSNC), 2010, pp. 136-141.

[16] C. Lesjak, T. Ruprechter, J. Haid, H. Bock, and E. Brenner, "A secure hardware module and system concept for local and remote industrial embedded system identification," in Proc. Emerg. Technol,. Factory Autom. (ETFA), pp.1-7.

[17] Hi Suo,Jiafu,Caifeng Zoua,Jianqi Liua Wan."Security in the Internet of Things-A Review",International Conference on Computer Science and Electronics Engineering (ICCSEE),pp.407-410,2013.

[18] Kozlo et al.,"Security and Privacy Threats in IoT Architectures",Proceedings of the 7th International Conference on Body Area Networks pp.256-262,2012

[19] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in Proc. 2nd ACM Workshop Digital Identity Manage., 2006, pp.11-16.

[20] R. Morgan, S. Cantor, S. Carmody, W. Hoehn, and K. Klingenstein, "Federated security: The Shibboleth approach," Educause Q., Vol. 27, pp.12-17, 2004.

[21] J. Singh and J. Bacon, "On middleware for emerging health services," J. Internet Serv. Appl. Vol. 5, No. 6, pp. 1-34, 2014.
[22] K. Cameron, The Laws of Identity, Microsoft Corporation, 2005 [Online]. Available: https://msdn.microsoft.com/en-us/library/ms996456.aspx
[23] A. Sunyaev and S. Schneider, "Cloud service certification," Commun. ACM, vol. 56 no.2, pp. 33-36, 2013.
[24] R. Accorsi, D.-I.L. Lowis, and Y. Sato, "Automated certification for compliant cloud-based business processes," in Business & Information Systems Engineering. New York, NY, USA: Springer, 2011, vol. 3 no.3, pp.145-154.
[25] A. Munoz and A. Mana, "Bridging the GAP between software certification and trusted computing for securing cloud computing," in Proc. 9th World Congr. Serv. (SERVICES) , 2013, pp. 103-110.
[26] T. Kunz, A. Selzer, and U. Waldmann, "Automatic data protection certificates for cloud-services based on secure logging," in Trusted Cloud Computing. New Yourk, NY, USA: Springer, 2014, pp. 59-75.
[27] S. A. de Chaves, C.B. Westphall, and F. R. Lamin, "SLA perspective in security management for cloud computing," in Proc. 6th Int. Conf. Netw. Serv. (ICNS), 2010, pp. 212-217.
[28] K. Bernsmed, M.G. Jaatun, P.H. Meland, and A. Undheim, "Security SLAs for federated cloud services," in Proc. 6th Int. Conf. Availability Reliab. Secur. (ARES), 2011, pp. 202-209.
[29] Intel Software guard extensions programming reference, Tech. Rep. 329298-001US, 2013 [Online]. Availabel: https://software.intel.com/sites/default/files/329298-001.pdf, accessed on Jul. 21, 2015.
[30] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, and L.van Doorn, "VTPM: Virtualizing the trusted platform module," in Proc. Secur. Symp., 2006 pp. 305-320.
[31] A. Baumann, M. Peinado, and G. Hunt, "Shielding applications from an untrusted dloud with have," in Proc. 11th USENIX Conf. Oper. Syst. Des. Implement. (OSDI), 2014, pp. 267-283.