RESEARCH ARTICLE OPEN ACCESS

An evaluation of selective security issues in Internet of Things based on Cloud

Karandeep Kaur
(Department of Computer Science, Guru Nanak Dev University, Amritsar)

--*************************----------------------------------

Abstract:

The implementation of Internet of Cloud needs a broad vision of technology and computing. It requires the incorporation of diverse technologies in order to realize its working. Cloud computing is enabling the use of IoT in wide application areas. Its natural feature of being readily available is showing tremendous advantages in Internet of Things and smart functionalities. However, there are a few aspects of using cloud services in the IoT mainly revolving around data security and access policies. This paper presents a perspective on this side of cloud usage and how it can be handled proficiently. A detailed study and evaluation of selective security issues has been done to help the reader get acquainted with this side of cloud in IoT.

Keywords — **Internet of Things, Cloud computing, Security in cloud, Cloud based IoT, Security issues in IoT**

--*************************----------------------------------

I. OVERVIEW OF INTERNET OF THINGS AND CLOUD COMPUTING

The Internet of Things is the forthcoming concept of Information technology. The idea behind it is the union of web, Information and Communications (ICT) technology and mobile services. It will enable different devices in a model system to interact and coordinate with each other to perform their job efficiently. According to the definition given by ITU, "The IoT describes a worldwide network of billions or trillions of objects that can be collected from the worldwide physical environment, propagated via the Internet, and transmitted to end-users. Services are available for users to interact with these smart objects over the Internet, query their states, as well as their associated information, and even control their actions" [1]. Its main principle is to create a large network which consists of different smart devices and networks to facilitate the information sharing of global things from any place and at any time [2].

The technologies which are widely used in Internet of Things are RFID, WSN, 3S, Cloud computing etc. Radio Frequency Identification (RFID) assigns identifiable tags to various objects and devices. These tags transmit information which is read by a RSID reader and is then used as per the requirements. These tags turn the normal devices into smart devices in IoT [3]. Sensors are also used to collect and interpret the data from various resources. The 3S technology consists of GPS (Global Position system), GIS (Geography Information System) and RS (Remote Sense) which provides the details about the locations of various objects using satellites and sensors etc. and processes that information. Wireless Sensor Network (WSN) facilitates transmission of the data in IoT.

Cloud services which are readily available and location-independent are used to store and compute data generated in IoT. These services may be provisioned where required very easily. Cloud services are best suitable for IoT environment due to various factors like easy availability, managing resource restraints, pay-per-use policy etc. Cloud servers can provide services in the form of software, storage space, computational power, platforms etc. The use of cloud services has its own implications and considerations. The concerns relates to the use of cloud in IoT are covered in this paper. Table 1 discusses the security aspects of cloud in IoT focusing on data storage, access and management perspectives.

II. SECURITY CONSIDERATIONS RELATED TO DATA STORAGE, ACCESS AND MANAGEMENT

Looking at various factors impacting the security of cloud in IoT with respect to the data storage, access and management techniques, the following facts come up.

A. *SECURING COMMUNICATION*

The first requirement of any service based on networks is the security and integrity of data. It has been a constant effort on the part of cloud service providers to improve the level of security in the communication between devices and the cloud. Transport Layer Security (TLS), commonly used by providers, uses encryption methods to provide security. In order to modify the existing TLS for the smart devices in IoT, works are going on by the researchers. Various encryption techniques need to be used by the devices themselves to ensure security [4].

B. *ACCESS CONTROL*

The authentication and authorization of the devices in IoT which connect to the cloud come under the access control provisions. When a device connects to the cloud, it should authenticate itself and after it is established that the device is allowed to do so, the process of authorization is initiated. It will provide access to the cloud as per the authorization rights and privileges of the device. The access control policies are required to manage this access control. Trusted Platform Modules provide services related to management of device access and rights [5].

C. *SENSITIVITY OF DATA*

This is an important aspect when it comes to Internet of Things environment. Sensitive data has to be dealt with caution and should not be available for access to unauthorized users. In IoT the devices that produce data need to be identified and proper measures should be taken. Also, the same device may not produce sensitive data all the time so this also needs to be kept in mind.

D. *DATA PROTECTION ON CLOUD*

This is related to the security of data when it is stored on the cloud. Though TLS is offered by most of the cloud service providers, but that may not be enough when it comes to sensitive data leaks within the cloud by the insiders. This needs to be considered while using cloud in IoT. Also as cloud providers work on the notion of virtualization, measures need to be taken to facilitate the isolation at such levels [6][7]. When the cloud provider can't be trusted, encryption may be done by the smart device itself and it should not rely on cloud only.

E. *DECISION REGARDING CHOICE OF CLOUD*

When a particular field like healthcare generates both sensitive data like patient records as well as not-so-sensitive data like monitoring heart-rate etc., the choice of cloud service is an important concern. The sensitive data needs to be stored on private cloud with complete protection and authorization while the monitoring data may be stored on public cloud. Also, this kind of environment suggests the importance of hybrid clouds which however, has its own security issues when it changes control from private to public cloud and vice-versa.

F. *DATA SHARING WITHIN THE CLOUD*

Along with the security of data stored on cloud, there should be provisions of data sharing within the cloud. For example, a sensor used to monitor patient's heart-beat and another one to monitor its motion may work separately and store their respective data on the cloud, however they need to share the information with each other to ensure smooth working in IoT healthcare. There is a need to have policies which enable this data sharing. A methodology called Information Flow Control (IFC)

Table 1: Security Considerations in IoT of Cloud

Security considerations in IoT of cloud	Solutions and Implications
Securing Communications	Use of TLS, encryption Need for protocols suitable for devices in IoT
Access Control	Access control policies Authentication and authorization
Sensitivity of Data	Sensitive data on private cloud Less sensitive data on public cloud
Data protection on cloud	TLS offered by cloud Encryption by device itself
Choice of cloud	Depends on the kind of data Hybrid cloud a promising solution
Data sharing within cloud	Information Flow Control (IFC) Access policies for sharing
Encryption by IoT devices	Encryption by the device to ensure security Limits the operations of cloud to storage only

has been developed to ensure that such policies are adopted and also complied with [8][9].

G. ENCRYPTION BY IoT DEVICES

To ensure data security, the IoT smart devices which generate the data can encrypt it before sending to the cloud. This can solve many purposes like secure transit of data, preventing data leakages on the cloud, preventing access of cloud to sensitive data, protection from insiders with malicious intent etc. However, the encryption of data can put extra burden on the devices so it should be done only when absolutely necessary. Also, the cloud can't perform other operations like analysis and computations on the encrypted data, so this should also be considered before implementing this policy [10].

CONCLUSION

The paper aims to assess the security consideration of using cloud services in Internet of Things model. The role of cloud in IoT has been discussed and its suitability reasoned. The aspects of security related to data storage, access and management are studied along with their potential solutions. The cloud computing model is the most appropriate for IoT implementation; however some aspects need to be taken care of in order to reap its potential to the most.

REFERENCES

[1] Lei CHEN, Mitchell TSENG, Xiang LIAN. Development of foundation models for Internet of Things. Front. Comput. Sci. China 2010, 4(3): 376–385.

[2] Su-bin SHEN, Qu-li FAN, Ping ZONG. Study on the Architecture and Associated Technologies for Internet of Things. Journal of Nanjing University of Posts and Telecommunications (Natural Science).2009, 29(6):1-11.

[3] ITU. ITU Internet Reports 2005: The Internet of Things, ITU (2005).

[4] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," IETF, Tech. Rep., 1999.

[5] T. Morris, "Trusted Platform Module," in Encyclopedia of Cryptography and Security. Springer, 2011, pp. 1332–1335

[6] S. Soltesz, H. P¨otzl, M. E. Fiuczynski, A. Bavier, and L. Peterson, "Container-based operating system virtualization: a scalable, high performance alternative to hypervisors," in SIGOPS Operating Systems Review, vol. 41, no. 3. ACM, 2007, pp. 275–287.

[7] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," SIGOPS Operating Systems Review, vol. 37, no. 5, pp. 164–177, 2003.

[8] J. Bacon, D. Eyers, T. Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch, "Information Flow Control for Secure Cloud Computing," IEEE TNSM SI Cloud Service Management, vol. 11, no. 1, pp. 76–89, 2014.

[9] T. F. J.-M. Pasquier, J. Singh, and J. Bacon, "Information Flow Control for Strong Protection with Flexible Sharing in PaaS," in *IC2E, International Workshop on Future of PaaS*. IEEE, 2015.

[10] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley Publishing, 2008.