Alyas *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429(Print)
ISSN: 2616-6003(Online)

LGU International Journal for
Electronic Crime Investigation

Research Article Vol. 2 issue 1 January-March 2018

Data Breaches Security Issues for Cloud Based Internet of Things

Tahir Alyas [1], Nadia Tabassum[2], Sagheer Abbas[3] , Atifa Ather[4]
Lahore Garrison University tahiralyas@lgu.edu.pk[1]
Virtual University of Pakistan, nadiatabassum@vu.edu.pk[2]
National college of business Administration & Economics, Lahore, Pakistan dr.sagheer@ncbae.edu.pk[3]
Comsats institute of information technology, atifaathar@ciitlahore.edu.pk[4]

Abstract:

Now a day's Internet of Things (IoT) and cloud computing are latest popular technologies. Both technologies have great role in our life. Their adoption and utilization are relied upon increasingly inescapable and making them vital segments of the Future Internet. A novel worldview where Cloud and IoT are consolidated and would be helpful for large number of application scenarios. Security in cloud computing and IoT truly challenging, needs a watchful comprehension and it includes numerous zones. Protections of cloud situations can be more powerful, versatile and have a superior financially savvy, yet the vast centralization of assets and information is a more appealing focus for aggressors. In this paper, data breaches architecture for the next generation technologies on cloud-based IoT will be introduced which will address the challenging issues of data breaches in cloud base system.

Keywords: Cloud computing, Resource Pooling, Rapid Elasticity, Public cloud, Hybrid cloud.

1 Cloud computing

Cloud computing is a storage medium and the platform where we can store data and files over internet, it is a medium where data remains more secure and threat free, by using cloud system we can access any of our document or website from anywhere through internet. Cloud computing is a system that allow us to compute and arrange our data and information more quickly and securely and it can be accessed by user no matter where he is, the only requirement to accessing data is associated with the availability of internet. [1].

Cloud computing provides users a platform where he can store his data easily and conveniently. Cloud computing is also convenient in a sense that if user wants to share his/her data or information with someone, he can simply allow him/her accessibility without requiring any hard device.

1.1. Cloud Computing Architecture

Cloud computing architecture is the framework or the total design of cloud computing. Cloud actually consist of all the important characteristics of client server websites like it has a front end, back end and the interface that is used by its clients to communicate like internet and cloud internet.

1.2. Essential characteristics of Cloud Computing:

Some of the most important characters of cloud computing is following:

1.2.1. On-Demand Service

On-demand service is a model or technique in which we just provide facility to cloud users so they can get services from services providers irrespective of time and place, providing availability of internet service to user. The user can facilitate from this service for completion of his tasks. The main purpose of this modal is to enhance the liberty of client so he can avail services on his demand at any place or time. To avoid all the issues or any difficulty we just provide this facility to user on his demand, it means any person or organization can get this facility to avail its project that is more depending on the services or the resources required for the maintenance of that organization or company.

1.2.2. Broad Network Access:

Cloud system is just used in broad network area so that everyone can access services. Most of the companies can use this facility to remain updated for clients or other organizations by using the cloud services and anyone can use these services but it is dependent on the network used like whether it is private or public? if you use the private cloud then all the information will be under the members of the private cloud who are sign in to the cloud services but, if it is public network than anyone can access information and can benefits from services provided to the cloud users. Disadvantage associated with public network arises if you just left to log out you id then your project information can leak out and you may have to face many severe issues related to data security

1.2.3. Resource Pooling:

Resource pooling is a technique in which the consumer can acquire and release the resource when it will be required on demand. The PaaS users can get the resource from the resource pool on demand so that the user can make use of this resource and then give it back to the resource pool. It also reduces all the complexities that cloud has to face by using resource-pooling techniques.

1.2.4. Rapid Elasticity:

Rapid Elasticity is one of the characteristics of the cloud computing in which the cloud or cloud service providers provide their users and buyers all the services in a very reliable and flexible manner. Cloud provides their services to users very easily and their users can easily get the services on demand. The cloud users can have extra storage space to have more resources from cloud provider in order to enhance services which was not possible before because system was complicated and less advance. Now if somebody needs to use the cloud system can also get the extra storage space.

1.2.5. Measured Service Problem Statements:

Measured service problem is one of the most critical features of cloud computing in which work on all the problems and all the faults faced by clients occurred from the services provided. Measured service is a term that IT experts apply to distribute computing. To have the total measurement about the usage of the resources used in different places to made much application. The idea of measured service is a definition of cloud computing which is supported by National Institute of Standard and technology or NIST.

1.3. Cloud Service Models:

The most commonly used service models through which the cloud system provides different services to the users consumers are following:

1.3.1. Infrastructure-as-a-Service (IaaS):

Infrastructure is just like a support or foundation which is used to provide these type of services to your customers and cloud users like by using infrastructure u can give resources to the equipment's that are used in different works like virtualization, storage area, networking etc. You can easily offer these resources or facilities to your customers and cloud buyers and users to enhance your services provided to the customers. You can increase your storage area and the network speed provided to the customers so that they can easily use the benefits of the best networking speed available.

1.4 Cloud Deployment Models

1.4.1 Private cloud:

A private cloud is a particular model of circulated computing that incorporates a specific and secure cloud based condition in which simply the foreordained client can work. Likewise as with other cloud models, private fogs will give figuring power as an organization inside a virtualized space using an essential pool of physical handling resource. In private cloud resource pool of cloud services is subject to affiliation for significant control and security [3].

1.4.2 Public cloud:

The most unmistakable model of disseminated computing to various clients is the overall public cloud show, under which cloud organizations are given in a virtualized circumstance, created using pooled shared physical resources and accessible over an open framework, for instance, the web. In public cloud pool resources influencing an unpredictable situations and using shared services.

1.4.3 Hybrid cloud:

A mixture cloud is a consolidated cloud advantage utilizing both private and open clouds to perform specific limits inside a comparative affiliation. All disseminated computing organizations offer certain effectiveness to different degrees; yet open cloud organizations are most likely going to be more affordable and flexible than private clouds. In this way, an affiliation can extend their effectiveness by using open cloud organizations for all non-sensitive operations, simply relying upon a private cloud where they require it and ensuring that most of their stages are faultlessly planned.

1.4.4 Community cloud:

A social order cloud in figuring is a community effort in which system is shared between a couple of relationship from a specific gathering with fundamental concerns (security, consistence, ward, et cetera.), paying little attention to whether administered inside or by an untouchable and encouraged inside or remotely. This is controlled and used by social affairs of affiliations that have shared interest. The costs are spread over less customers than an open cloud (however more than a private cloud), so only a segment of the cost speculation reserves ability of circulated computing are made sense of it.

1.5 IoT Based Cloud system

The Next revolution in the period of figuring will be changing in contrast with customary demand base requirement and things placed everywhere. Many technologies encompasses the human clients will be on the system in one frame or in another frame in the Cloud Computing and Internet of Things structure. Distributed computing and Internet of Things are two distinctive advancements, these are into our everyday life [4].

1.5.1 Data breaches in cloud system

An information break is an episode in which touchy, ensured or secret information has conceivably been seen, stolen or utilized by an individual unapproved to do as such. Information breaks may include individual data or identifiable data exchange mysteries or licensed innovation [5].

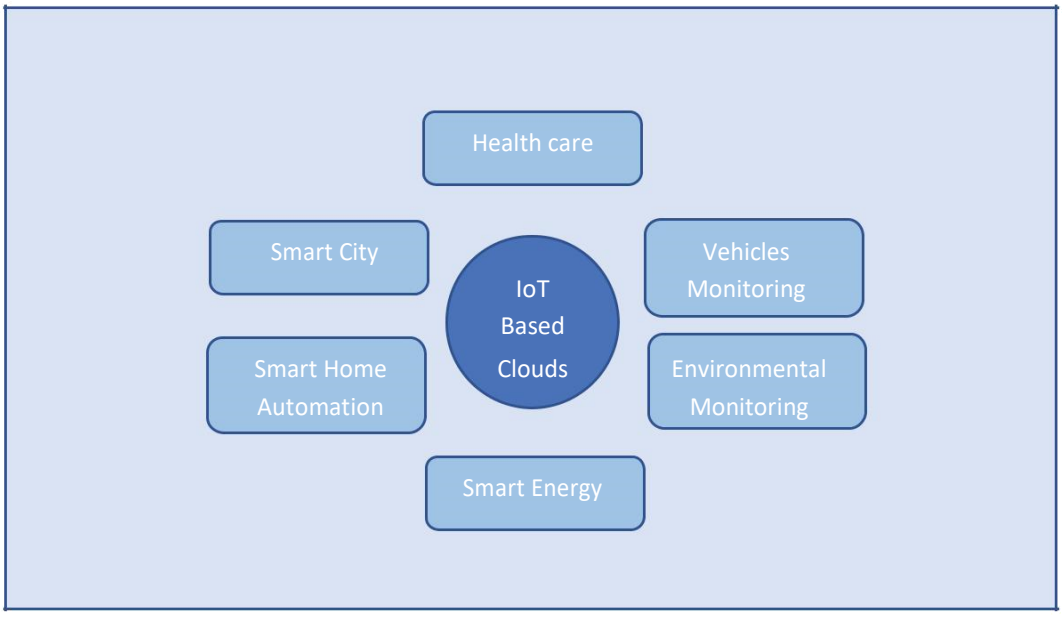

Figure 1. IoT based Cloud System

There are different ways a breach can happen in cloud computing

- Accessing data via malware
- Snuffing private cloud passwords
- employee negligence
- policy failure

An information break happens when there is an "unapproved access to delicate, ensured, or private information". Information ruptures ordinarily have negative outcomes for the business and people included. An information rupture triggers inquiries regarding the earlier cautioning signs, the occasion itself, and the required stance post the information rupture.

1.5.2 Data breach Challenges

The following will be data breaches challenges in IoT based clouds system.

- Privacy
- Security
- Legal aspect
- Social Aspect
- Reliability
- Performance

2 Literature Review

Nowadays, Cloud computing is a proceeding sector that focuses at contributing every type of service on requirement anytime and everywhere. Advancement in this sector has promoted an innovative cooperative cloud in which various inter-dependent clouds offer ascendable services. This paper goal to choose the Trustworthy Service Provider (TSP) by estimating trust based on surroundings assessment from individual authority; these authorities involve third-party feedback, universal consulting feedback and user feedback. As well as, un- fair feedback is clarifying to advance reliability. The multifaceted trust management framework promotes the assortment of a TSP. First of all, to increase the achievement velocity of the job, secondly, to enhance the dignity of the revenue built by the contributor to the users. Thirdly, to increase the standard of service to the users by offering stable service [6].

3 Proposed methodology

Online Reputation networks assist reduce the information imbalance between customers and contributor in Cloud Computing organizations. This paper defines a reputation model that treats with few open problems in up-to-date. First of all, we can provide a peer to peer structure for proceedings with the price of distribution concentrate reputation services, which can be a better design for other organization but not for cloud computing. Secondly, we defined a mathematical model to compute the trust contact from a customer to a contributor. The model too explains trust relationship between updates and peers them to utilize the statistical survey to discover the dependability of their records. Moreover, the reputation and layer.In this environment, various data breaches challenges are there in the form of Privacy, Security, Legal aspect, Social Aspect, Reliability and Performance in IoT based devices like RFID tags, cameras, RFID readers, intelligent sensors, smart meters and intelligent device. These Iot base devices are capable to sense the data breaches and can handle these challenges through security policies layer.

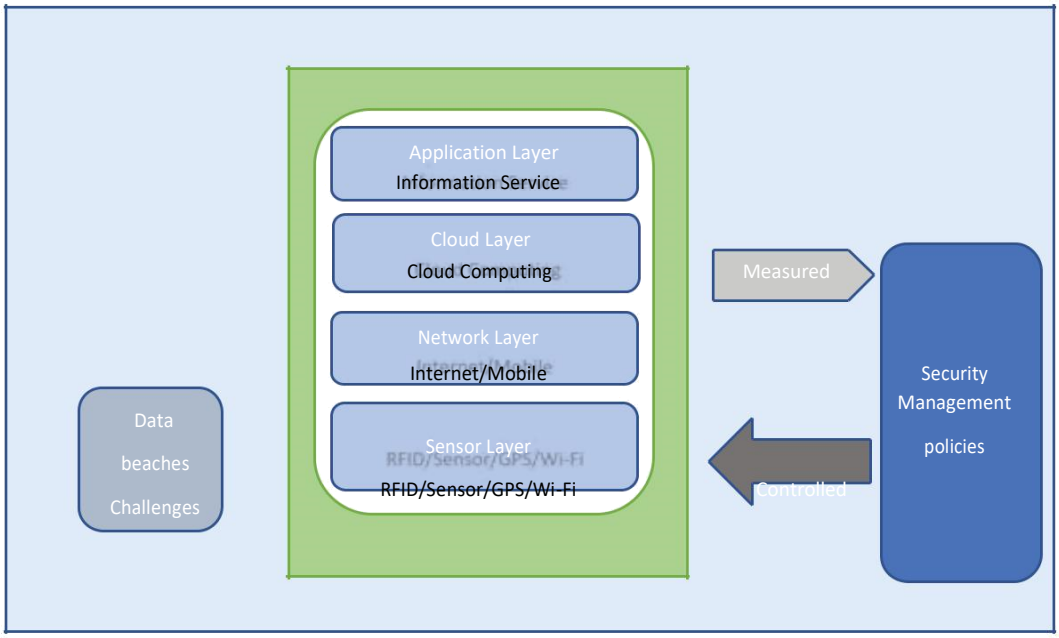

Figure 2. Proposed framework for Data Breaches Security

The middle module is further consisting of four layers, sensor layers, network layers, cloud layer and application layer. Sensing layer is capable to sense the environment of data breaches and communicate it to network layer, this layer will work like bridge between two layers sensing layer and cloud layer. All the data on clouds will route through network layer, the data in cloud can be infrastructure as a service, platform as a service and software as a service or anything as a service will be routed through network layer. In cloud environment, the cloud system management, device management, heterogeneity management, cloud monitoring management, deployment management in clouds can be affected through data breaches security challenges.

Policy and security management are crucial challenge for virtualized network to put up IOT traffic economically and efficiently. Overall, as societies are going to be more reliant on the uninterrupted and genuine working of IT systems, Internet and communication networks, thus the consequences of successful cyberattacks, these malicious, criminal in nature have become very serious. The possible vulnerabilities can be measured like insecure web interface, poor authorization, insecure different networks, poor encryption, privacy related concerns, insecure cloud/mobile interface, less security configurability and poor physical security. The above-mentioned vulnerabilities cab be controlled by measured policies.

4 Conclusion

We proposed a data breach security model for cloud service providers to identify given parameters of most concern to security challenges in IoT Based clouds system. In this model, information leakages for cloud service

providers, empowering clients to recognize parameters are of most worry to them and give a weighting capacity. Multi-characteristic parameters of security issues that are most essential for information break hazard will be shifting in light of security SLAs and in addition in view of customers prerequisites.

5 References

[1] P. R. Pratim , "A survey of IoT cloud platforms," Future Computing and Informatics, pp. 35-46, 2016.

[2] I. Addor and S. Ahamed, "REFERENCE ARCHITECTURES FOR PRIVACY PRESERVATION IN CLOUD-BASED IOT APPLICATIONS," International Journal of Services Computing, pp. 65-79, 2014.

[3] "Integration of Cloud computing and Internet of Things: A survey," Future Generation Computer Systems, pp. 684-700, 2016.

[4] S. Mohanty,, "Everything You Wanted to Know About Smart Cities," IEEE Consumer Electronics Magazine, 2017.

[5] Y. Rahulamathavan and M. Rajarajan, "Assessing Data Breach Risk in Cloud Systems," in *7th International Conference on Cloud Computing Technology and Science*, 2015.

[6] A. Kornfeld Simpson and F. Roesner, "Securing Vulnerable Home IoT Devices with an In-Hub Security Manager," *The First International Workshop on Pervasive Smart Living Spaces*, 2017. [7] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru, "REFERENCE ARCHITECTURES FOR PRIVACY PRESERVATION IN CLOUD - BASED IoT APPLICATIONS (EXTENDED VERSION OF 7398 AT MS 2014)," vol. 2, no. 4, pp. 65–78, 2014.

[8] S. M. Babu, A. J. Lakshmi, and B. T. Rao, "A study on cloud based Internet of Things: CloudIoT," *2015 Glob. Conf. Commun. Technol.*, no. Gcct, pp. 60–65, 2015.

[9] Y. Rahulamathavan, M. Rajarajan, O. F. Rana, M. S. Awan, P. Burnap, and S. K. Das, "Assessing data breach risk in cloud systems," *Proc. - IEEE 7th Int. Conf. Cloud Comput. Technol. Sci. CloudCom 2015*, pp. 363–370, 2016.

[10] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 551–556, 2017.

[11] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, 2017.