ISSN 2319-2720

Volume 10, No.4, October - December 2021

International Journal of Computing, Communications and Networking

Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn011042021.pdf

https://doi.org/10.30534/ijccn/2021/011042021

Secured Cloud-Based Internet Of Things Application Reporting System: A Review

Babalola G.O[1], Abiodun A.I[2], Oguntimilehin A[3], Abiola O.B[4]

[1]Afe Babalola University, Nigeria, gbemibabz@abuad.edu.ng

[2,3,4]AfeBabalola University, Nigeria

Received Date : October 12, 2021 Accepted Date : November 15, 2021 Published Date : December 07, 2021

ABSTRACT

Cloud-based Internet of Things environments exhibit different architectures based on the services they provide, thus making it even harder to find 'global' security measures. Many of the security issues in relations to Cloud Computing architecture, governance, portability and interoperability, have been addressed in other systems. The specific characteristics of Internet of Things application in Cloud environments result into new security concerns. Various security models have been proposed to deal with security threats ranging from authentication, access control, lightweight security, data privacy and so on. However, users are not aware of the degree of security integrated with the CloudInternet of Things application system thereby limiting the perceived trustworthiness of such systems. Therefore, the need to provide aCloud-based Internet of Things application reporting system that can predict and monitor the effectiveness of such applications cannot be overemphasized. In this paper, reviews of existing Cloud-based Internet of Things security approaches are presented. This paper is concluded by highlighting the future research direction with respect to improving the acceptability of secured Cloud-based Internet of Things deployment.

Key words: Internet of things, Cloud computing, Security, Cloud of things,

1. INTRODUCTION

Cloud computing represents the delivery of hardware and software resources on-demand over the Internet as a Service. At the same time, the internet of things (IoT) concept envisions a new generation of devices (sensors, both virtual and physical) that are connected to the Internet and provide different services for value-added applications. IoT promises a world of devices and things newly outfitted with Internet smarts that will be able to monitor, communicate and respond when their environments change[5].

The Internet of Things (IoT) paradigm relies on the integration of a large number of heterogeneous devices, which are connected to the internet via different networking protocols. IoT permits the communication between different sensors connected to the Internet and the use of their services towards relevant applications. [11]. Introducing IoT into the internet results in lot of smart objects gets connected to the internet. These objects generate large amount of data that cannot be handled by normal databases. If the objects have very simple interface then they cannot even perform small amount of computation that might be necessary. Hence Cloud concepts are integrated with IoT so that storing and computation is done in the Cloud. Managing huge amount of data can be easily done by combining IoT with Cloud [28].

The two worlds of Cloud and IoT have seen an independent evolution. However, plenty of common advantage is the result of their integration have been identified in literature. On the one hand, the Internet of things can benefit from Clouds' almost unlimited capacity and resources to make up for the technical constraints. Specifically, Cloud computing can provide an effective solution to realize management of Internet services and composition and use of things or data applications. Cloud computing can benefit from the Internet of things, on the other hand, by extending its scope to deal with things in the real world more distributed and dynamic way, and to provide new

services on a large number of real life scenarios. Essentially, the Cloud acts as intermediate layer between the things and the applications, where it hides all the complexity and the functionalities necessary to implement the latter [13].

Various Cloud providers adopt or develop different security models to protect user data. Cloud providers enforce viable security models for access control, privacy, intrusion detection, etc. but users are limited in knowledge of the degree of security in a Cloud resource. Users find it difficult to ascertain the level of security at any time because security level of a Cloud is considered to be dynamically changing in nature, because there is no way to predict when and where an IoTCloud will be threatened. Users including developers need to know how secured their IoT applications are and to what degree. This paper presents a review of previous works related to secured Cloud-based security IoTsystems. Adetailed discussion on the existing security systems is presented including the challenges and future opportunities

2. PREVIOUS WORKS

Cloud IoT application security assessment is not easy because of its complexity, largeness and stiffness. The characteristic of Cloud IoT applications makes security a difficult problem from several points of view. The geographical distribution of resources and users that implies frequent remote operations and data transfers lead to a decrease in the system's safety and reliability and make it more vulnerable from the security point of view.

2.1 Convergence of Cloud and IoT

The convergence between Internet of Things and Cloud Computing reveals a new paradigm that seems to be promising named in the literature in various way such as Cloud of Thing [21] or CloudIoT [3]. The number of Internet of Things devices connected to Internet is growing exponential and, since 2011, has already exceeded the number of people on Earth. They have already reached the 9 billion and are expected to grow more rapidly in the next years until reach the 24 billion in 2020 [16]. Besides the growing number of IoT systems, other aspects reveal several motivations on its integration between IoT and Cloud Computing infrastructures.

Storing data locally and temporarily will not be possible anymore and there is going to be even more a need of storage space. Moreover, this huge amount of data can't be processed locally in the devices and the need of computational capacity is growing.Typically the IoT services are provided as isolated vertical solution in which all components of the applications are tightly coupled to the specific context of application. Bringing IoT services in the Cloud can ease the delivery and the deployment of them by leveraging all the flexibility of Cloud models. In this context, the Cloud Computing facilitates applications development make possible an abstract vision of the IoT systems and offers its services to meet need to decouple the applications from the specific context.

Internet of Things can provide also a platform for the Smart Cities services that are been envisioned in the latter years. Through these platforms can be possible acquiring information from different heterogeneous sensing devices, accessing all kinds of geo-location and IoT technologies, and exposing data extracted from them in a uniform way. Several proposed solution suggest to use Cloud architectures to discover sensors and actuators, to enable their connection and interaction and to create platforms that are able to support ubiquitous connectivity and real-time applications for smart cities [12].

This example do not cover all those aspects in which can be a cooperation between Cloud and Internet of Things but, in all these cases, Internet of Things systems can have many benefits from the usage of an unlimited computational capacity allowing scalability in their applications. Also, elasticity that a Cloud infrastructure provides can face scenarios in which there is a peak of the demand of resource usage from an IoT system or these resources can be released because the demand is poor [20].

2.2 Security Models inIoT Systems

Besides data and resources, the Cloud of Things has to deal with its impact in the business and its consequences. This will create more business opportunities and is making it more attractive for the attackers. The two principal components of Cloud of Things areIoT devices (RFID, Wireless Sensor Network (WSN) etc.) and Cloud infrastructures which are vulnerable to many kind of attacks or theft actions like, for example, disabling network availability,pushing

erroneous data into the network or accessing personal information.

[4] reviewed different security strategies considered by previous researches for IoT systems. The fundamental requirement for any IoT security systems was summarized as follows: Authentication & Authorization, Data Privacy, trust between involved parties, Anonymity, Efficient key management protocol, Context aware security system, Lightweight security technique, Forward secrecy, Hierarchical Access regulation, and Standardized scalable approach. This paper highlighted that while a lot of research has focused on authentication, authorization techniques, there is still need of platform-independent, context-aware, and resource efficient security protocols for comprehensive IoT security. Security issues specific to RFID systems & mobile applications was also described for in-depth study. The National Institute of Standards and Technology contends that security, interoperability, and portability are the major barriers to a broader Cloud adoption [23].

According to [28], the present day Internet of Things (IoT) based on Cloud computing and Big data concepts has become a new area of research. Novel concepts and implementations are being researched every day. The paper presents an overview of trending technologies in Cloud computing and IoT applications. Discussions on these concepts were also included in the paper which covers major advantages, concerns and risks that need to be mitigated. This paper discusses the future internet concepts and how IoT has its influence on future internet. The architecture of IoT, various applications which can be built with IoT and concept of Cloud integrated with IoT leading to new technology called Cloud of things were also discussed.

[10]discusses the architecture of IoTCloud framework and the different APIs available to the users. The paper explains several technical problems involved in the IoT development such as interoperability problem, security, deployment problem, management problems etc. The paper describes the IoT architecture which has components such as IoT Cloud controller, Message broker, Sensors and Clients. IoT Cloud controller is the one which is responsible for controlling system components and providing SOAP messages. The message broker is responsible for routing of messages. Sensors are used to collect the data and which is used by clients. The paper describes different types of message broker, sensors and clients and their functionalities. It also describes about Future Grid. With Future Grid Complex research problems in computer science related to the use and security of grids and Clouds.

According to [11], the emerging trend of Internet of Things (IoT) has spread across almost all components of modern life, starting from smart building, smart city, medical care, wearable devices, automobiles or industries. However, physical things getting attached to the Internet poses new challenges of making the entire system more vulnerable, prone to attacks and misuse. The paper further explained that the heterogeneous nature of all different devices, resource-constrained wireless sensor network nodes make traditional security algorithms inapplicable for IoT scenario. So, IoT systems should consider applying new set of security measures to deal with IoT specific security needs. This paper reviews the major IoT security approaches, namely authentication & authorization, context aware, lightweight protocol design, key management, anonymity, data privacy, trust and standardization.

[25] discusses the services offered by IoT on Integration with Cloud Computing. The paper gives information about different services the IoT provides. These services include: Identity related services, Information aggregation services, Collaborative aware services, and Ubiquitous services. The paper also discusses about the limitations of the deployment of IoT on Cloud.

[27]discussed about the design of an architecture where new generation services collects the data from the outside environment and different management strategies are applied to them. It mainly focuses on the implementation of the architecture based on COT.

[8] realize usage control for grid computational services by making the grid user deploy her application together with a policy. Different from the approach in this thesis, policies are defined for applications rather than data. As data flows are not considered, cooperating applications may circumvent the usage control mechanisms.

[17] aims at preventing “illegitimate secondary dissemination of protected plaintext data by authorized recipients.”It allows unmodified applications to transparently use protected data while ensuring compliance with policies. It builds upon additional hardware and a trusted hypervisor, which is not needed in my approach. Different to DataSafe, [9] also allow

for the enforcement of policy obligations such as deletion of data after a certain amount of time.

Digital Rights Management refers to mechanisms that aim at controlling the usage of copyrighted, read-only, digital information at the data consumer's site. It can therefore be considered a specialization of usage control that focuses on payment-based dissemination[15]. DRM does not provide means for end users to protect their valuable information. While DRM solutions are limited to read-only content, tailored to specific file types and rely on specific applications to enforce digital licenses, the results of this thesis will not be limited in such a way.

Several Trusted Platform Module (TPM) based solutions have been proposed [23]; their basic idea is to measure crucial system components (BIOS, Boot loader, operating system, usage control infrastructure) and verify their integrity using a set of known "good" values. Yet, not much work has been carried out with the goal to use such technologies for securing data-driven usage control infrastructures.

[19] uses sticking policies to data via the back channel model. In this approach, on each system the communication between PEP and PDP is mediated through an application independent PEP (AIPEP). Once data is sent to another system, the AIPEP is responsible for sending the sticky policy to the AIPEP of the receiving system.

[2]addressed the problems of side-channel attacks and noninterference in the presence of multitenancy and resource virtualization. They presented an access control architecture that addresses these challenges. Close to this work is that of [18], who proposed edit automata for enforcing security policies. Edit automata, suppression automata, and insertion automata are features of their work.

3. CONCLUSION

Cloud and IoT have many complementary characteristics arising from the different proposals in literature. As the research community has envisioned, the Cloud can act as intermediate layer between the things and the applications hiding all the complexity of the resources management and the functionalities necessary to implement the IoT system. This intermediate layer will impact future application development. In this paper, a review of different security strategies considered by previous researches for IoT systems was presented. It is observed that existing models do not report or assure users of the level of security mechanism in the system. While a lot of research has focused on authentication, authorization techniques, and so on, there is still need for platform-independent, context-aware, andtrustworthiness, for comprehensive Cloud IoT security. Security issues specific to Cloud IoT systems should also be studied in depth.

REFERENCES

[1]A. Pretschner, M. Hilty, F. Sch¨utz, C. Schaefer, and T. Walter, "Usage Control Enforcement: Present and Future," IEEE Security & Privacy, vol. 6, no. 4, 2008.

[2]Abdulrahman A. Almutairi, Muhammad I. Sarfraz, SalehBasalamah, Walid G. Aref, ArifGhafoor online "A Distributed Access Control Architecture for Cloud Computing" Jun 12, 2012 [Online]

[3] AlessioBotta, Walter de Donato, Valerio Persico, and Antonio Pesca; On the integration of Cloud computing and internet of things. In Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, pages 23{30. IEEE, 2014.

[4] Antara De, H. S. Guruprasad, "A Survey on Securing IoT Systems", Journal of Emerging Technologies and Innovative Research (JETIR) September 2015, Volume 2, Issue 9 JETIR (ISSN-2349-5162)

[5] Charles Cooper (2015): The IoT, Cloud and Security. Available online at

http://www.cio.com/article/2933046/Cloud-security/the-iot-Cloud-and-security.html

[6] Divers S. - SANS Institute, "Information Security Policy A development Guide for large and small companies", November 2007, pp. 43-44.

[7] D. Nurmi et al., "The Eucalyptus Open- Source Cloud-Computing System," Proc. 9th IEEE/ACM Int'l Symp. Cluster Computing and the Grid (CCGRID 09), IEEE CS, 2009, pp. 124-131.

[8] F. Martinelli and P. Mori, “On Usage Control for GRID Systems,” Future Generation Computer Systems, vol. 26, no. 7, 2010.

[9] Florian Kelbert, “Data Usage Control for the Cloud,” TechnischeUniversit¨atM¨unchen (TUM), Germany, 2013.

[10] G. C. Fox, S. Kamburugamuve, and R. Hartman “Architecture and Measured Characteristics of a Cloud Based Internet of Things”, API Workshop 13-IoT Internet of Things, Machine to Machine and Smart Services Applications (IoT 2012) at The 2012 International Conference on Collaboration Technologies and Systems (CTS 2012) May, 2012.

[11] GeorgeSuciu, AlexandruVulpe, GyorgyTodoran, Janna Cropotova, Victor Suciu “Cloud computing and internet of things for smart city deployments”, 2012

[12] GeorgeSuciu, AlexandruVulpe, SimonaHalunga, Octavian Fratu, Gheorghe Todoran, and Victor Suciu. Smart cities built on resilient Cloud computing and secure internet of things. In Control Systems and Computer Science (CSCS), 2013 19th International Conference on, pages 513{518.IEEE, 2013.

[13]Hone K., Eloff J. H., “Information security policy: what do international information security standards say?”, Proc. of the 8th European Conference on Information Warfare and Security, Computers and Security, vol. 21, Issue 5, 2002, pp. 402- 409.

[14] J. M. AlcarazCalero et al., "Toward a Multitenancy Authorization System for Cloud Services," IEEE Security & Privacy, vol. 8, no. 6, 2010, pp. 48-55.

[15] J. Park and R. Sandhu, “Towards Usage Control Models: Beyond Traditional Access Control,” in Proc. 7th ACM Symp. on Access Control Models and Technologies, 2002.

[16] JayavardhanaGubbi, RajkumarBuyya, SlavenMarusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645{1660, 2013.

[17] Kshetri, N., “Privacy and security issues in Cloud Computing: The role of institutions and institutional evolution”. 2012, Bryan School of Business and Economics, The Univ. of North Carolina at Greensboro, NC27402-6165,USA.

[18] J. Ligatti, L. Bauer, and D. Walker. Edit Automata: Enforcement Mechanisms for Run-time Security Policies. Intl. J. of Inf. Security, 4(1-2):2–16, 2 2005.

[19] M. Harvan and A. Pretschner, “State-Based Usage Control Enforcement with Data Flow Tracking using System Call Interposition,” in Proc. 3rd Intl. Conf. on Network and System Security, 2009.

[20] Marco Distefano. Cloud Computing and the Internet of Things: Service Architectures for Data Analysis and Management, University Of Pisa, Department Of Computer Science. 2015.

[21] MohammadAazam, Imran Khan, Aymen Abdullah Alsaar, and Eui-Nam Huh. Cloud of things: Integrating internet of things and Cloud computing and the issues involved. In Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on, pages 414.IEEE, 2014.

[22] Morsy M. Al., Grundy J. and Müller I., “An Analysis of the Cloud Computing Security Problem”, Proc. APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.

[23] National Institute of Standards and Technology, “Cloud Computing Synopsis and Recommendations”, May 2012, Special Publication 800-146.

[24] National Institute of Standards and Technology, systems, “Guide for developing security plans for federal information systems”, vol. 800-18, February 2006, [Online]. Available from:http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf/.

[25] PriteeParwekar, “From Internet Of Things Towards Cloud Of Things”, International Conference on Computer and Communication

Technology, 15-17 Sept. 2011, Allahabad, pp 329-333, DOI: 10.1109/ICCCT.2011.6075156.

[26] S. Berger et al., "Security for the Cloud Infrastructure: Trusted Virtual Data Center Implementation," IBM J. Research and Development, vol. 53, no. 4, 2009, pp. 560-571.

[27] Salvatore Distefano, Giovanni Merlino, Antonio Puliafito, “Enabling the Cloud of Things”, 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 4-6 July 2012, Palermo, pp 858-863, DOI: 10.1109/IMIS.2012.61.

[28] Suchetha K. N. and H. S. Guruprasad, “Integration of IoT, Cloud and Big data” Global Journal of Engineering Science and Researches, July 2015] ISSN 2348 – 8034 Impact Factor- 3.155