iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** II **Month of publication:** February 2021

DOI: https://doi.org/10.22214/ijraset.2021.33113

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue II Feb 2021- Available at www.ijraset.com

Security Challenges in IOT, Big Data & Cloud Computing Integration

Mrs Bhagyashri S. Nemane[1], Miss Renu D. Pahurkar[2]
[1, 2]*Assistant Professor, Saraswati College Shegaon Maharashtra, India*

Abstract: ***With the growing up advances in communication technologies and in many other sectors, also growing up security and privacy issues. Here we introduced a technology called Cloud Computing (CC) to operate with the Big Data (BD). Thus we proposed a new system for Cloud Computing integrated with Internet of Things as a base scenario for Big Data. It gives focus on the security issues of Cloud computing and big data technologies. Here we also present the security challenges of the integration of IoT and Cloud Computing with the aim to provide an architecture depending on the security of the network in order to reduce their security issues.***

Keywords: Efficiency, Cloud Computing, Big Data, Internet of Things, Security, privacy.

I. INTRODUCTION

The use of big data (BD) analysis tools and services can reduces the problem with security and privacy in everyday life. Big data is a new well liked term, used to describe the rapid increase in volume of data in structured and unstructured form [1]. Accuracy in big data may lead to more certain decisions making, and better decisions can result in greater operational efficiency, cost reduction, and reduced risk [2] [3]. A base technology for another relative to communications technology could be used as cloud computing, internet. The basic idea of the IoT is the spread presence of a variety of things or objects used by people such as radio-frequency identification tags, sensors, actuators, and mobile phones. With unique addressing schemes, these things interact with each other and cooperate with other things near them in order to reach the common goals [4]. The IoT can defined as "the network of physical objects, devices, buildings, vehicles, and other items which are embedded with electronics, software, sensors, and network connectivity, permitting these objects to gather and exchange data" regarding the bibliography [6].Some examples include the restrictions of storage, communication capabilities, energy and processing offered to IoT devices. Those inefficiencies inspire us to combine the functionality of cc and IoT technologies [6].IOT security is the area of strive concerned with protecting connected devices and networks in the IoT. The IoT involves the raising dominance of objects and entities, provided with unique identifiers and the ability to automatically transmit data over a network. Much of the increase in IoT communication comes from computing devices and the embedded sensor systems used in sectors such as industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices [7] [8]. Furthermore, the new technology called cloud computing could be defined as "a distributed information technology (IT) architecture in which client data is processed at the periphery of the network, as close to the originating source as possible". The move toward cloud computing is driven by mobile computing, the decreasing cost of computer components and the absolute number of networked devices in the IoT Moreover, cc describes to data processing power in a fog network instead of holding that processing power in a cloud or a central data warehouse.CC storage solutions offer users and enterprises with various capabilities to store and process their data in third-party data centers .With the aim to offer safer and secure communication over the network, major role is played by encryption algorithms. It is a valuable and fundamental tool for the protection of the data. Encryption algorithm converts the data into encrypted form by using "a key" and only the user have this key to decrypt the data. Regarding the researches which have been carried out, an important encryption technique is the symmetric key encryption. In symmetric key encryption, only one key is used to encrypt and decrypt the data. In this encryption technique the most used algorithm is the AES[11]. Here we can also use the triple des algorithm. Regarding the cc, the characteristics that affected more are "service over internet" and "computationally capable". As a general conclusion, we can observe that those two technologies contribute more each other in many of their characteristics. Here, we present a short survey of IoT and CC with a focus on the security issues of both technologies. Specifically, we integrate the two technologies with the aim to examine the common features, and in order to discover the benefits of their integration. Concluding, we present the contribution of cc to the technology IoT, and it shows how the cc technology improves the function of the IoT Finally, we survey the security challenges of the integration of IoT and CC with the aim to provide an architecture relaying on the security of the network with the aim to improve the security issues.

II. LITERATURE REVIEW

For the purpose of this paper we study and analyze previous literature which has been published in the field of Big Data, CC and IoT. The following paragraphs present the papers which contributed significantly in our study. To begin with, there are several works for the Big Data technology. Recently, several studies for BD technologies have been devised [12]. The authors of [12] introduce a multi-objective approach using genetic algorithms. Two objectives, the execution time, and the budget of each node to minimize is the main goal. The contribution of [12] research is to propose an innovative adaptive model to communicate with the task scheduler of resource management. The proposed model periodically queries for resource consumption data and uses to calculate how the resources should be allocated to each task. Through this work, the authors believe that the proposed solution is timely and innovative as it provides a robust resource management where users can perform better scheduling for BD processing in a seamless manner. Moreover in [13] the important concepts of BD technology are highlighted and also there is a discussion about the various aspects of BD. Furthermore, the authors of [13] define what BD and discuss the various parameters of its definition. Thus, in [13] there is a look at the process that involved in the data processing and then reviewing the security aspects of BD and as a result, propose a new system for security of BD. Additionally, an offer of six provocation with the aim to spark conversations about the issue of BD technology. These provocations are the cultural, technological, and scholarly phenomenon that rests on the interplay of technology, analysis, and mythology that dares extensive utopian and dystopian rhetoric. Finally, a multi-stakeholder approach for developing a suitable privacy regulation in the age of BD.This argument developed in five steps:

1) A review of the current academic debate on privacy regulation.
2) An argue that the framework for developing a suitable privacy regulation should not only focus on formal and procedural but should additionally include some important essential aspects to guard users and promote socially beneficial BD applications.
3) An examination of how the process leading to an appropriate regulation might be organized.
4) A discussion of the potential structure of a privacy organization which might conduct multi-stakeholder-dialogues as a preliminary step.
5) A discussion of their findings and suggestions.

Also, there are several works for the BD technology in regard with new technologies. A literature review of BD and its related technologies, such as Cloud Computing (CC) and Hadoop. Also, focuses on the five phases of the value chain of BD technology and as a result examines the several representative applications of BD technology. Furthermore, the important concepts of BD technology are highlighted and also there is a discussion about the various aspects of BD. Thus, the authors define what BD and discuss the various parameters of its definition. Finally, there is a look at process that involved in the data processing and then reviewing the security aspects of BD and as a result propose a new system for security of BD. A framework first offered by an introduction to the MIS Quarterly Special Issue on Business Intelligence. Research that identifies the evolution, applications and emerging research areas of BI&AI. Also, there is a report of a biometric study of critical BI&A publications, researchers and research topics which based on more than a decade of related academic and industry publications.

As regard the Sustainability of the Cloud Computing, also, there are various works and researches that have been made in the field. We try to present those researches from oldest to newest. Initially, the authors strive to compare and contrast Cloud Computing with Grid Computing from different angles, and in addition to give insights into the essential characteristics of both. Regarding the open challenges in the field is another research. The presents vision, and architectural elements, except for the challenges, for energy-efficient management of Cloud computing environments. The authors gives more focus on the development of dynamic resource provisioning and allocation algorithms which consider the synergy between different data center infrastructures, and holistically work to boost data center energy efficiency and performance. More specifically, proposes three things. Architectural principles for energy-efficient management of Clouds is proposed at first. Secondly, proposed some energy-efficient resource allocation policies and scheduling algorithms considering quality-of-service expectations, and devices power usage characteristics. And finally, the authors proposed a novel software technology for energy-efficient management of Clouds. Furthermore,through their work state some major challenges in the field of Sustainable Cloud Computing, count on recent researches that have been made. One of these challenges is that it is unclear which application areas of IT can and will be outsourced to a Cloud. In a more recent work, and as a newer version defines an architectural framework and principles for energy-efficient Cloud computing. The authors, based on this proposed architecture, present their vision, open research challenges, and resource provisioning and allocation algorithms for energy-efficient management of Cloud computing environments. Additionally, the authors conduct a survey of research in energy efficient computing and propose three things that have discussed in their past work.

At the end, the author of [14] discusses a thorough introduction to cloud computing which is realized with emphasis on its advantages for environmental sustainability. Also, a list of challenges in relation to the use of the technology as green technology is presented, and the reasons for using cloud computing for sustainability are explained in his work.

III. SECURITY ISSUES IN IOT & CLOUD COMPUTING INTEGRATION

There is a quick and independent evolution considering the two words of IoT and CC. Initially, the virtually unlimited capabilities and resources of CC with the aim to recompense its technological constrains, such as processing, storage and communication, could be a benefit for the Internet of Things technology. Also, the IoT technology spins out its scope to deal with real world things in a more distributed and dynamic manner and by delivering new services in a large number of real life scenarios, might be beneficial for the use of CC technology. On several occasions, CC can offer the intermediate layer between the things and the applications, hiding all the complexity and functionalities necessary to implement the latter [40]. Through the integration of IoT and CC could be observed that CC can "complete" some gaps of IoT, such the "*limited storage*" and "*applications over internet*". Also, IoT can "complete" some gaps of CC, such the main problem of "*limited scope*". Based on motivations such those referred beforehand, and the important issue of security in both technologies we can assume some motivations for the integration. The security of this integration has a serious problem. When critical IoT applications move towards the CC technology, concerns arise due to the lack of trust in the service provider or the knowledge about service level agreements (SLAs) and knowledge about the physical location of data. Consequently, new challenges require specific attention as mentioned in surveys [14]. Multitenancy could additionally appease security and lead to sensitive information leakage. Furthermore, public key cryptography cannot be applied at all layers due to the computing power constraints imposed by the things. These are examples of topics that are currently under investigation with the aim to handle the big challenge of security and privacy in CC and IoT integration [14]. Subsequently, some challenges about the security issue in the integration of two technologies are listed below :

a) *Heterogeneity*. A big challenge in CC and IoT integration is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications

b) *Performance*. Often CC and IoT integration's applications introduce specific performance and QoS requirements at several levels and in some particular scenarios meeting requirements may not be easily achievable

c) *Reliability*. When Cloud Computing and IoT integration is adopted for mission-critical applications, arises to reliability. When applications are developed in resource constrained environments several challenges related to device failure or not always reachable devices exists

d) *Big Data*. With an estimated number of 50 billion devices that will be networked by 2020, specific attention must be paid to transportation, storage, access, and processing of the huge amount of data they will produce.

e) *Monitoring*. As largely documented in the literature, monitoring is an essential activity in CC environments for capacity planning, for managing resources, SLAs, performance and security, and for troubleshooting .

Additionally, we can realize that IoT technology related to more challenges [4] than the CC technology [3].

IV. PROPOSED SYSTEM

The study of previous works cites us relevant architecture and topology proposals for a Smart Building network, which on several occasions supported and operated in Internet of Things and Fog environments. In this section we will make a comparative analysis study of the some previous works which we have differentiated. Initially, we analyze what each of them deals with. Regarding the Literature Review analysis we realize that not enough works deal with security and privacy issues in Cloud Computing for technologies such as Big Data and Internet of Things.

Thus, we try to develop a new system for Cloud Computing integrated with Internet of Things as a base scenario for Big Data. In order to improve the security issues we would try to establish an architecture relaying on the security of the network. With the aim to eliminate the privacy and security issues a security "wall" is installed between the Cloud Server and the Internet (the various users). This type of network uses all the benefits of the existing topologies (e.g. star, ring etc.) in order to have good communication and to transfer more safely large-scale data (Big Data) through the network. By applying the proposed model we can extend the advances of IoT and Cloud Computing, by developing a highly innovative and scalable service platform to enable secure and privacy services. Through our research we can propose the part of algorithm which extends the security advances of both Cloud and IoT technologies.

V. ADVANTAGES AND BENEFITS OF THE PROPOSED MODEL

Cloud Computing could offer many benefits to people in general, businesses and Small and Medium Enterprises in particular through our proposed model, but additionally and in general use. The five main reasons for adopting a Sustainable Computational Cloud technology with the aim to give it extra boost and competitiveness are listed below:

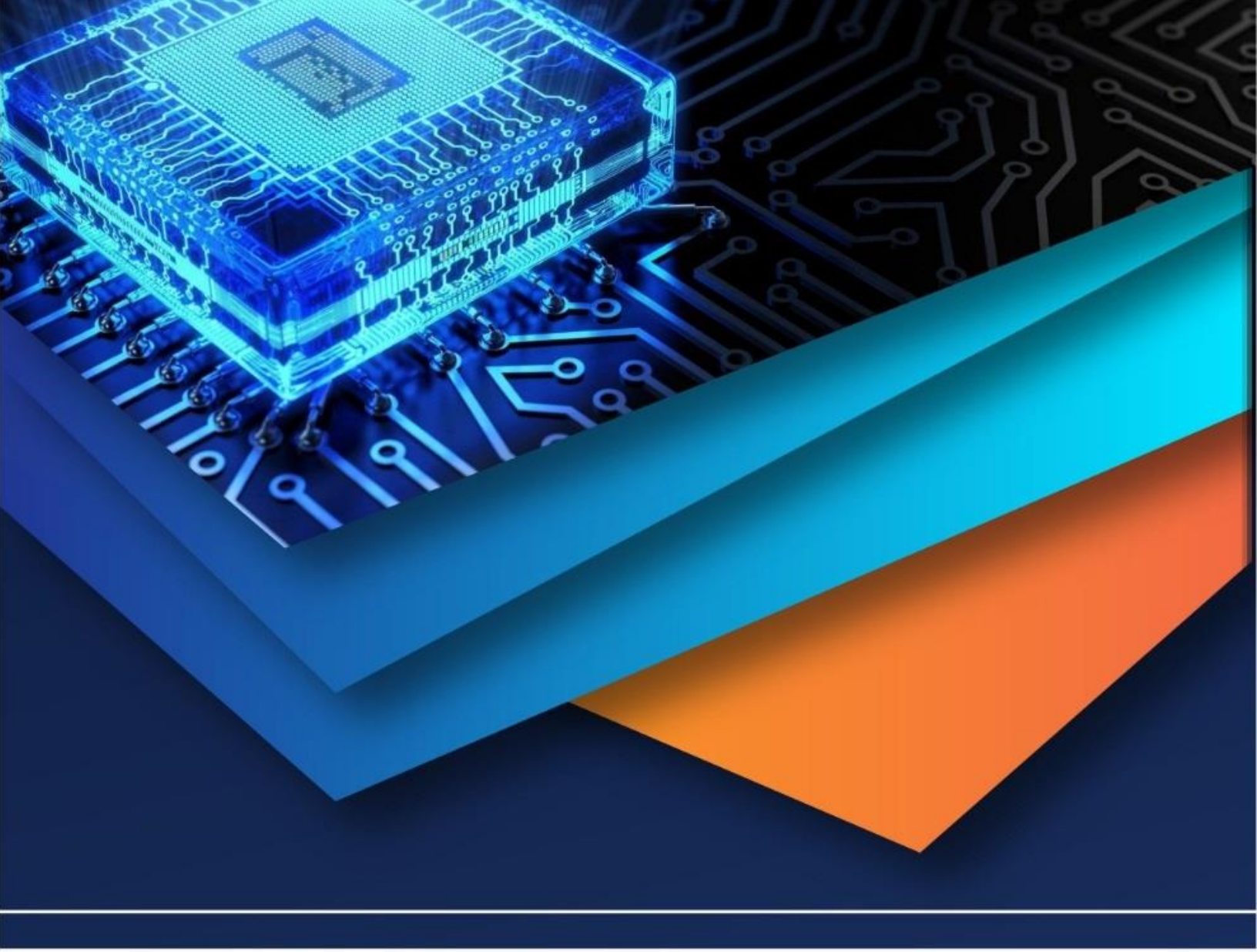
A. Offers software and application solutions without greatly increasing costs as applications run on the Cloud and businesses do not need expensive computing systems. It provides access to Cloud data from anywhere and any device at any given time, giving portability and flexibility to the business. It is backed by state-of-the-art security protocols that ensure enterprise data protection.
B. Provides optimal business performance due to flexibility, mobility and productivity. Regarding the efficiency of Cloud Computing in general, and more specific our proposed model, there are in addition economic and efficiency benefits:
C. Reduces labor costs by 50% in the configuration, operation, monitoring and management of business operations.
D. Improves up to 30% the quality and elimination of software defects.
E. Reduces up to 40% support costs for end users.

VI. CONCLUSION

Thus we come to the conclusion that security and privacy issues grew up by the significant advances in the sector of communications and additionally in other sectors. This work aims to introduce Cloud Computing as a base technology in order to operate and integrate with recent technologies such as Big Data and Internet of Things. Regarding this and depending on the privacy issues in its operation, we proposed a new system for CC which integrated with IoT and operates as a base scenario for BD. The main goal of the interaction and cooperation between things and objects communicate through the wireless networks, in order to fulfil the objective set to them as a combined entity. Also the security challenges of the integration of IoT and Cloud Computing were surveyed through the proposed architecture. At the end, we survey the security challenges of the integration of IoT and Cloud Computing with the aim to provide an architecture relaying on the security of the network in order to improve the security issues. Regarding the future, we plan to make more simulations in order to have a better accuracy in our experimental results. More data transfer scenarios have to be made through the simulators providing results counting not only in data transmission but also in network efficiency and support [14].

REFERENCES

[1] C. Stergiou, K. E. Psannis, “Efficient and Secure Big Data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, pp. 1-20, April 2017.
[2] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, vol. 27, issue: 9, September 2016.
[3] T. Li, J. Li, Z. Liu, P. Li, C. Jia. “Differentially Private Naive Bayes Learning over Multiple Data Sources”, Information Sciences, vol. 444, pp. 89-104, 2018.
[4] C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, “Architecture for Security in IoT Environments”, in Proceedings of 26th IEEE International Symposium on Industrial Electronics, 19-21 June 2017, Edinburgh, Scotland, UK.
[5] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, S. V. Sharma, “Cloud computing for Internet of Things & sensing based applications”, In Proceedings of IEEE 6th International Conference on Sensing technology (ICST 2012), pp. 374–380, Kolkata, India, 18-21 December 2012
[6] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, December 2016.
[7] M. Rouse, "IoT security (Internet of Things security)", IoT Agenda, 01/11/2015. [Online]. Available:http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security. [Accessed 27/07/2017].
[8] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. M. Hassan, A. Alelaiwi, “Secure Distributed Deduplication Systems with Improved Reliability”, IEEE Transactions on Computers, vol. 64, issue: 12, pp. 3569-3579, 2015.
[9] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, Y. Tang, “An ID-based linearly homomorphic signature scheme and its application in blockchain”, IEEE Access, vol. 6, pp. 20632-20640, February 2018.
[10] L. Fan, X. Lei, N. Yang, T. Q. Duong, G. K. Karagiannidis, “Secrecy Cooperative Networks With Outdated Relay Selection Over Correlated Fading Channels”, IEEE Transactions Vehicular Technology, vol. 66, no. 8, pp. 7599-7603, August 2017.
[11] R. Kaur, S. Kinger, "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, March 2014.
[12] I. A., T. Hashem, N. B. Anuar, A. Gani, "Schedule optimization for big data processing on cloud", in Proceedings of 2nd International Conference on Big Data Analysis and Data Mining, San Antonio, USA, 30 November - 1 December 2015.
[13] R. Toshniwal, K. G. Dastidar, A. Nath, "Big Data Security Issues and Challenges",International Journal of Innovative Research in Advanced Engineering (IJIRAE), vol. 2, issue: 2, pp. 15-20, February 2015.
[14] Christos Stergiou, Kostas E. Psannis1, Brij B. Gupta, Yutaka Ishibashi,” Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT”, Article in Sustainable Computing: Informatics and Systems, June 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY