iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3123

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: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A Brief Survey on Perils of Data Storage in Cloud

Dr. S. Veena[1], Poornima. M[2], Divyalakshmi. M[3]
[1]*Professor,* [2, 3]*Student, Department of Computer Science and Engineering, S. A Engineering College.*

Abstract: ***With the dominance of technology, the size of the data is increasing exponentially day by day. Cloud computing serves as an exceptional solution for storage of this rapidly growing data. Cloud computing technology evolves the delivery of computing services such as servers, storage, databases, networks, software, analytics and many more. As the significance of data elevates, a large number of security issues also arises. A lot of questions remain unanswered when we talk about the security of data stored in cloud. This paper presents a brief survey on the issues involved in cloud data storage. We elaborate the already existing ideas, methodologies and experiments recommended by our forerunners and survey the issues that exist in storage of data. We also try to figure out the necessary solutions for these issues concerning other technologies such as block chain that could act as an efficient replacement for cloud.***
Keywords: Cloud computing, Data storage, Security concerns

I. INTRODUCTION

Cloud computing is being the current hysteria of the industry. Most of the eminent corporates such as Google, Amazon & IBM uses cloud to store and process huge volume of data they generate each day. Cloud computing technology provides a platform for development, hard-disk, hardware and software applications and database. It is a pay-per-use system that charges the users only according to the amount of data they use. Cloud computing has made the applications easy and simpler to find and use. Cloud makes use of virtualized resources to access the pool of resources that are available over the internet. Cloud exhibits various features such as speed, efficiency, flexibility and scalability. Cloud computing models are categorized into four major types, namely public, private, hybrid and community cloud. Public cloud ensures the availability of data and resources anytime irrespective of the geographical location of the user wherein a third party service provider is involved in the maintenance of data and resources. Private cloud is built within an organization that could be used only by the respective authorities who are responsible for processing and managing the data. Hybrid cloud, as the name implies is the combination of both public and private cloud. It is deployed in an organization that deals with both confidential and legitimate data where they are stored in private and public clouds respectively. A community cloud follows the concept of private cloud where a group of people same interests only can access the resources shared in the cloud. We also have three types of cloud service models namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) to lend licensed software, platforms and servers to the users as per the usage. Every coin has two sides and the same holds for technologies too. Cloud computing suffers from various risks and challenges such as data breach, hijacking, attacks, data loss and numerous other threats. This paper elaborates the major threats and risks faced while storing the data in the cloud.

II. SURVEY ON RECENT WORKS AND METHODOLOGIES

Some of the existing survey works and methodologies of data storage in cloud are discussed as follows: Jun-Song Fu[1] et al has proposed a data processing framework that is designed by integrating the data processing functions and the retrieval of data. To store the data in a secure environment which allows dynamic processing and also allows searching, there are many issues in implementing. Marten Van Dijk[2] et al has proposed that cryptography is the best suited remedy for security violations in cloud. They have also proved that none of the cryptographic protocols could implement the classes where the data is being shared by clients.

Adel Nadjaran Toosi[3] et al has analyzed different functionalities of the cloud such as interoperability in an integrated cloud environment. It briefly explains the interoperability of cloud that makes it as an indispensable technology. This paper deals with the challenges and risks faced in cloud realization.

Pekka Nikander[4] et al came up with the idea of implementing Host Identity Protocol (HIP) to improve the internet architecture by introducing a new thin layer. This protocol is said to allow better location anonymity and establishing strong identity among trusted parties. This is said to reduce the worst traffic and scalability routing.

Kajal Rani[5] et al has proposed a desktop application which enables the user to share the data with advanced security. It is also important to restrict the unauthorized access, hacker any kind of denial of services. The objectives of the paper is to minimize the data uploading and downloading time on cloud storage, high quality of services.

Diao Zhe[6] et al has performed a study on the basic characteristics of cloud computing such as virtualization, high reliability, scalability, on demand service and data storage. It also deals with the various layers of cloud such as the storage layer, management layer and the application interface layer. This paper analyzes the various risks involved in the cloud storage including data transmission risk, data storage risk and cloud terminal risk.

Yinghui Zhang[7] et al has proposed a tool to realize secure and fair payment of outsourcing services in general without relying on any third-party, trusted or not, BPay, an outsourcing service fair payment framework based on block chain in cloud computing is introduced. The security and compatibility analysis of this system indicates that BPay achieves soundness and robust fairness.

Ilya Sukhodolskiy[8] et al has presented a prototype of multi-user system for access control to datasets stored in an untrusted cloud environment. Cloud storage, like any other untrusted environment needs the ability to share information in a secure manner. This approach provides an access control over the data stored in the cloud without the provider's participation.

Deepak K. Tosh[9] et al have proposed data provenance based on block chain technology called Block Cloud which has been incorporated with a proof-of-stake (PoS) based consensus protocol called as Cloud PoS. It is difficult to provide provenance for the data that has been generating using several operations held in the cloud environment.

Raluca Ada Popa[10] introduces Mylar, a platform for building web applications, which protects data confidentiality against attackers with full access to servers. Mylar stores sensitive data on the server in an encrypted format, and decrypts that data only in users' browsers.

III. MAJOR SECURITY ISSUES IN CLOUD

Cloud computing has set up an entirely new frontier for accessibility, flexibility and storage. This has led to the rise of security concerns involved in data storage. Few of them are as follows:

A. Data breaches

A data breach is an unauthorized access of confidential data by an untrusted party. It has been reported that over 50 percent of the IT professionals believe that the security measures of their organization to protect the data is low. Furthermore, it was found that this was the case with the companies that utilize cloud rather than those which don't.

B. Data loss

A data loss can occur in cloud by malicious attacks or code injections, natural disasters, etc. Loss of confidential data can be irrecoverable at times. This can be calamitous to businesses that don't have a proper recovery scheme. For example, in the year 2011, Amazon suffered from data loss losing its own customer details.

C. Denial of Service attacks

This type of attack does not perform modification or destruction of data. Rather, it makes the servers and websites unavailable to authorized users. This is also one of the most common attacks in cloud.

D. *Abuse of cloud services*

The extension of cloud computing services has helped both small scale and large scale enterprises to host large volume of data at ease. The unfamiliar storage capacity of cloud has allowed both malicious and legitimate users to inject malwares and unauthorized software such as pirated software, books, videos, etc.

E. Insider threat (or) compromising accounts

A malicious person in an organization may cause severe harm or information loss. This person may be a present, past or contractual worker who may have an authorized access to data thereby leading to devastating situations. Hence, it is necessary to continuously examine the number of accesses by the employees.

IV. SINGLE VS. MULTI-TENANT ARCHITECURE

A tenant is a group of people who are given access rights for the resources in the cloud on a rental basis. Single tenant architecture is the one in which every user have their own instance of the software and independent database. There is no sharing of any instance of the softare among the tenants. It provides highest level of security, data migration and ease of migration to a self hosted environment. Multi-tenancy can be defined as an architecture in which evey single part of the software runs on multiple servers and is capable of serving multiple tenants. Multi-tenancy is different from virtualization in that, the hardware and software components are transformed enabling each application to run in an individual virtual machine whereas in a multi-tenant architecture, multiple

tenants share the same application on the same hardware and on the same operating sytem with the same data storage capabilities. Each tenant data is isolated and is invisible to other concurrent users. Scalability, cost effectiveness and optimized efficiency in performance are some of the advantages of multi-tenant architecture.

V. COMPARISON OF VARIOUS REFERENCES

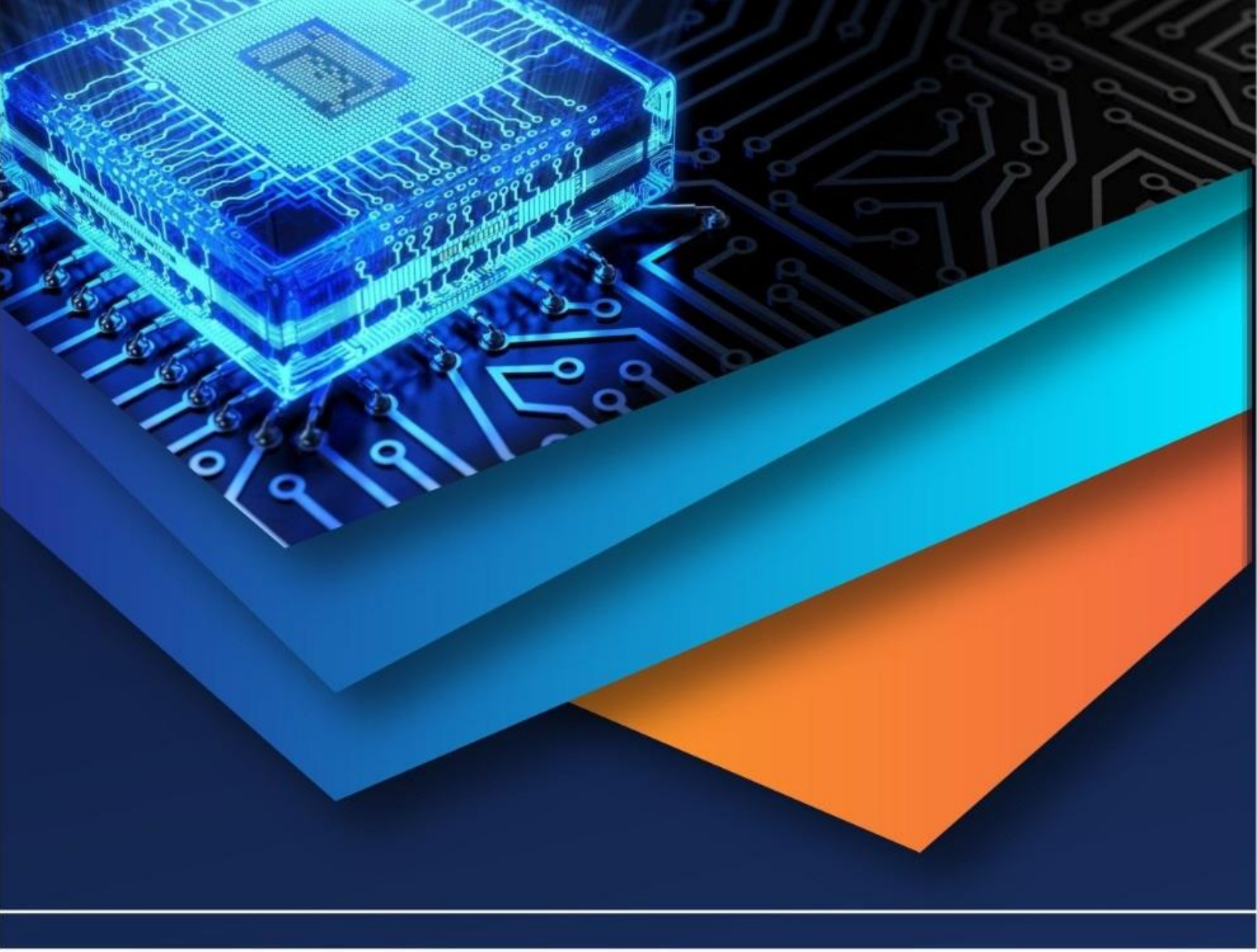
S.NO	TITLE	TECHNLOGIES/ TOOLS USED	MERITS	DEMERITS
1.	Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing	Cloud computing, Fog computing	The hackers cannot eavesdrop on the encrypted data. Improved efficiency of the cloud based data storage.	This scheme doesn't support efficient data search which reduces the functionalities. New index structures need to be designed and added to the framework.
2.	On the impossibility of cryptography alone for privacy-preserving cloud computing	Cryptography, Cloud computing	Centralized provision of computing resources.	Rely on other forms of privacy enforcement.
3.	Interconnected cloud computing environments: challenges, taxonomy, and survey	Cloud computing	Cloud interoperability	Challenges and obstacles faced by Inter-cloud realization are not discussed.
4.	In-depth look at the host identity protocol (hip): providing agile mobility, multi-homing, and security	Cloud computing	Mobility, multi-homing, and baseline end-to-end security	HIP has profound consequences.
5.	Enhanced data storage security in cloud environment using encryption, compression and splitting technique	Cloud computing	Storage security is improved using encryption, decryption and compression	Due to the openness of cloud storage privacy and security problem the better method should be opted. Does not get deployed in the different cloud environment.
6.	Study on data security policy based on cloud storage	Cloud computing, big data	Identifies various risks associated with cloud storage.	Does not provide necessary solutions or suggestions for the problem.
7.	Outsourcing service fair payment based on blockchain and its applications in cloud computing	Blockchain, Cloud computing	BPay achieves soundness and robust fairness if the hash function is collision-resistant and ECDSA is unforgeable. BPay is efficient interms of the computation cost.	The issue of payment fairness based on blockchain technologies in more complex cloud applications such as attribute-based data sharing is not addressed.
8.	A blockchain-based access control system for cloud storage	Blockchain, Cloud computing, Ethereum, Smart contracts.	Implements the access control model of the system to data stored in untrusted environments.	Rejection of the fact and the inability to edit the data.
9.	CloudPoS: A Proof-of-Stake Consensus Design for Block chain Integrated Cloud	Cryptocurrency, block chain, PoS, Cloud computing	The cloud environment is provided with the Block chain-as-a-service	The cloud service provider cannot be eliminated. The validators need to stake their resources for a fixed time which is required to overcome the bottleneck.
10.	Building web applications on top of encrypted data using Mylar	Cloud computing, Mylar	Enables developers to protect confidential data in the face of arbitrary server compromises.	Requires few changes to an application, and that the performance overheads of Mylar are modest.

VI. CONCLUSION

In this paper, we have focused on the major threats involved in storing the data in a highly secure cloud environment. We have also recommended the use of public and private clouds separately for storing common and confidential data respectively instead of using hybrid cloud. We have given a comparison of various methods in a comparison table that helps in better understanding of the concepts. There is no system in the world that is completely secure. Hence, the responsibility equally lies in the hands of the user to carefully cherish the benefits of cloud computing.

REFERENCES

[1] Jun-Song Fu, Yun Liu, Han-Chieh Chao, Bharat K. Bhargava, Zhen-Jiang Zhang, Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. IEEE Transactions on Industrial Informatics.
[2] Marten van Dijk, Ari Juels, On the impossibility of cryptography alone for privacy-preserving cloud computing.
[3] Adel Nadjaran Toosi, Rodrigo N. Calheiros, and Rajkumar Buyya, Interconnected cloud computing environments: challenges, taxonomy, and survey, The University of Melbourne, Australia.
[4] Dr. Pekka Nikander, In-Depth Look at the Host Identity Protocol (HIP): Providing Agile Mobility, Multi-Homing, and Security.
[5] Kajal Rani, Raj Kumar Sagar, Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique, 2nd International Conference on Telecommunication and Networks (TEL-NET 2017).
[6] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, Study on data security policy based on cloud storage, 2017 IEEE 3rd International Conference on Big Data Security on Cloud.
[7] Yinghui Zhang, Robert H. Deng, Ximeng Liu, and Dong Zheng, Outsourcing Service Fair Payment based on Blockchain and its Applications in Cloud Computing, IEEE TRANSACTIONS ON SERVICES COMPUTING.
[8] Ilya Sukhodolskiy, Sergey Zapechnikov, A blockchain-based access control system for cloud storage, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) Moscow, Russia.
[9] Deepak K. Tosh, Sachin Shetty, Peter Foytik, Charles A. Kamhoua, Laurent Njilla, CloudPoS: A Proof-of-Stake Consensus Design for Block chain Integrated Cloud, 2018 IEEE 11th International Conference on Cloud Computing.
[10] Raluca Ada Popa, Emily Stark, Steven Valdez, Jonas Helfer, Nickolai Zeldovich, and Hari Balakrishnan. Building web applications on top of encrypted data using Mylar. 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI '14).April 2–4, 2014 • Seattle, WA, USA ISBN 978-1-931971-09-6



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY