International Conference - Innovation-2021-Innovation-2021
International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)
Volume 8, Issue 3, May-June-2021

Data Security in Cloud

Ritesh Hajare[1], Rohit Hodage[1], Om Wangwad[1], Yogesh Mali[2], Faraz Bagwan[3]
[1]Department Computer Engineering, Savitribai Phule, Pune University, Pune, Maharashtra, India
[2]Professor, Department Computer Engineering, Savitribai Phule, Pune University, Pune, Maharashtra, India
[3]Assistant Professor, Department Computer Engineering, Savitribai Phule, Pune University, Pune, Maharashtra, India

ABSTRACT

Data security has been consistent in being a major issue in information technology. In the cloud computing world, becomes specifically critical as the data is situated in different places all over the world.

As per user's concerns about the cloud technology the important factors are privacy protection and data security. In both academics and industries, the topics in cloud computing have been checked by multiple techniques. For the future growth of cloud computing technology in industry, government and business the data security and privacy protection will become more crucial.

Data security and privacy protection challenges are similar to both hardware and software in the cloud architecture. This study is to analyze different security techniques and challenges from both software and hardware aspects to secure data in the cloud and focuses on improving the data security and privacy protection for the trustworthy cloud environment. In this document, we are preparing a relevant research analysis on the existing research work with reference to the data security and privacy protection techniques of cloud computing.

Keywords : Data security, Privacy Protection, Cloud Computing

I. INTRODUCTION

Cloud computing has been emerged as the next generation paradigm in computation. In the cloud computing world, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to fulfill user's requirements. The explanation of “cloud computing” as per the National Institute of Standards and Technology (NIST) states that cloud computing allows unique, convenient. Network access to a shared pool of configurable computing resources like servers, networks, applications, storage, and services and can be provisioned on priority and released with less management effort or service provider interaction on demand.

As per the description, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources

are identical to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure Cloud computing can be looked upon as a new computing archetype that can provide services on demand at a cheap cost. The three renowned and mostly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the similar data is deployed by a cloud service provider, and users can access it through the web browsers. In PaaS, a service provider delivers services to the users with a set of software programs that can resolve the given tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to enhance their business capabilities. Cloud computing is quite similartobut not the same as grid computing.
Grid computing integrates diverse resources together and manages the resources with the unified operating systems to provide better performance computing services, while cloud computing is the combination of computing and storage resources handled by different operating systems to provide services such as large-scaled data storage and top performance computing to users. The overall picture of grid computing has been replaced by cloud computing. Distribution of data isin a new format of cloud computing comparing with the grid computing.

Cloud computing will enable services make the services accessible to be consumed easily on demand. Cloud computing has the features like on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. These achievements of cloud computing have attracted substantial interests from both the industrial world and the academic research world.
Cloud computing technology is currently changing the business strategy in the world. Cloud computing is very promising for the IT applications; however, there are still some concerns to be resolved for personal users and enterprises for data storage and deploy applications in the cloud computing environment. One of the most significant obstacle to adoption is data security, which is accompanied by issues including compliance, privacy, trust, and legal matters.

The characteristic of institutions and institutional evolution is very similar to privacy and security in cloud computing .Data security has been consistent in being a major issue in IT. Data security turns out to be very critical in the cloud computing environment, because data gets scattered in different machines and storage devices including servers, PCs, and different mobile devices like wireless sensor networks and smart phones. Data security in the cloud computing is much more complex than data security in the traditional information systems.

To make the cloud computing adaptive by users and enterprise, the security challenges of users should be resolved first to make cloud world trustworthy.
The trustworthy environment is the basic prerequisite to win confidence of users to get used to such a technology. Discussed the assessment of cloud computing risks. Before the data security concerns are disclosed, the functions of cloud computing are reviewed first. Cloud computing is also known as on-demand service. In the cloud computing world, there is a cloud service provider that facilitates and manages the services.

The cloud provider facilitates all the services over the Internet, while end users use services for meeting their business needs and then pay for the services accordingly. Cloud computing world enables two basic types of functions which includes computing and data storage. In the cloud computing environment, users of cloud services don't need anything and they can get access to their data and complete their computing tasks just through the Internet devices. During the access to the data and computing, the clients don't even know where the data gets stored and which machines performs the computing tasks. Coming to data storage, data safety and security are the primary factors for gaining user's trust and making the cloud technology successfully used. Many data protections and data security techniques have been launched in the research world of cloud computing. However, data security related techniques need to be further improved. Services of cloud computing has been delivered across the entire computing spectrum. Nowadays, organizations and companies are moving and expanding their business by adopting the cloud computing reduce the cost. This can be a contribution to free more man-powers to focus on developing strategic differentiation and business division of labor is transparent.

The concept of cloud has many implementations based on the services from service providers. For example, Google Apps Engine, Microsoft Azure, and Amazon Stack are famous implementations of cloud computing provided by cloud service providers like Google, Microsoft, and Amazon companies. Apart from the rest, the ACME enterprise implemented VMware based v-Cloud for allowing multiple organizations to share computing resources

As per the difference of access scope, cloud can be distributed into three segments: public cloud, private cloud, and hybrid cloud. Public cloud has the similar property of service provider and is accessible in public, private cloud refers to being the property of a company, and hybrid cloud is the blends of public and private cloud. Most of the existing cloud services are delivered by large cloud service companies such as Google, Amazon, and IBM.

A private cloud is a cloud in which only the authorized users have access to the services from the provider. In the public cloud anybody can access the cloud services whereas the hybrid cloud contains the concept of both public and private clouds. Cloud computing can reduce the cost and save organizations time, but trusting the system is more vital because the actual asset of any organization is the data which they share in the cloud to use the required services by putting it either directly or in the relational database or eventually in a relational database using an application.

Cloud computing brings multiple attributes that requires serious attention when it comes to trusting the system. The trust of the entire system relies on the data protection and prevention techniques used in it. By the researchers numerous different techniques and tools have been introduced and tested for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which need attention and are required to be lined up by making these techniques much better and effective. The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information. The resource monitoring, resource management and resource security are the major issues in cloud computing. Currently, to deploy there are no regulations and standard rules. Applications in the cloud and there is a lack of standardization control in the cloud. In cloud numerous novel techniques had been implemented and designed; however, due to the dynamics of the cloud environment these techniques fall short of ensuring total security.

II. METHODOLOGY

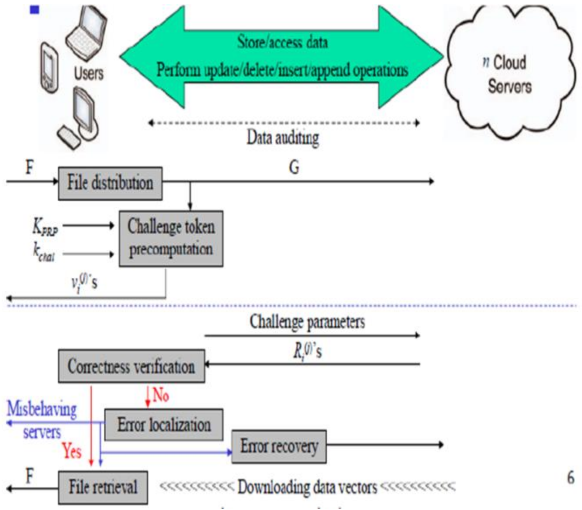


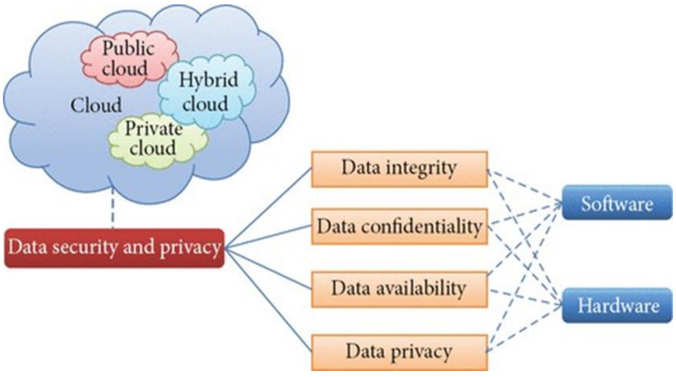
Fig.Error Correction and Error localization

Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operation on data blocks, including: update, delete and append. We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability.

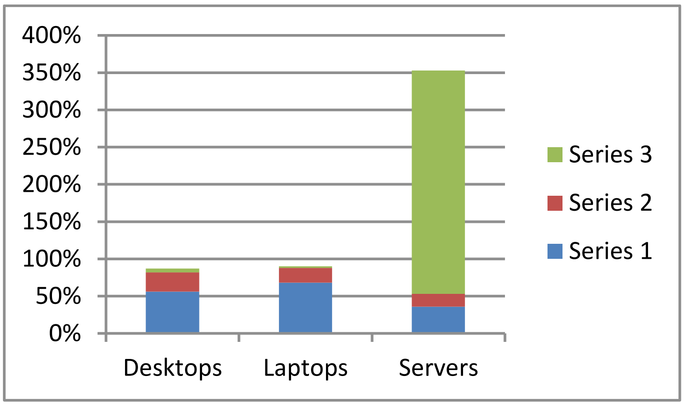
This project drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s) To eliminate the errors in storage systems key

III. RESULTS AND DISCUSSION:

Figures and Tables

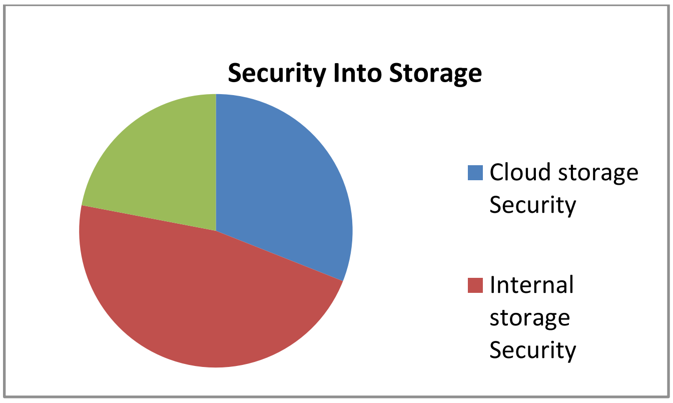


Current and Planned Uses of Storage Devices



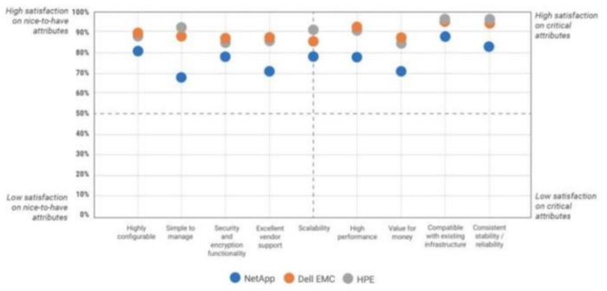
As we can see the Series 3 of servers users are getting more reliable on the Servers. More the storing the data into the Desktops and Laptops.

Importance of Storage Security Array and Internal component Security Array:



As we can see nowadays the 31% Cloud storage security for users are getting more reliable to get their data more secure. More than storing the data into the Portable storage.

Customer Satisfaction for Select Storage Vendors



To dive deeper into Cloud Security pick one over other we have various options decision makers to compare three prominent satisfactions across key consideration factors for users. On the different parameters score very similarly, with high customer satisfaction ratings on key factors such as consistent reliability/stability, compatibility with existing infrastructure, scalability, and high performance.

IV. CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers.

A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

V. REFERENCES

[1]. “Forbes: Cloud computing forecast,” https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts2017/#5c42322c31e8/, 2020.

[2]. “Microsoftonedrive, ”https://products.office.com/en-us/onedrive/online-cloud-storage, 2020.

[3]. C.Wang, N. Cao, J. Li, K. Ren, and W. Lou “Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE Transactions on Parallel and Distributed Systems, vol.23, No.8, Aug.2012.

[4]. S. Karen, “Iot big data security and privacy versus innovation,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1628 – 1635, 2019.

[5]. Z. Lei, F. Anmin, Y. Shui, S. Mang, , and K. Boyu, “Data integrity verification of the outsourced big data in the cloud environment: A survey,” Journal of Network and Computer Applications, vol. 112, pp. 1–15, 2019.

[6]. T. Ye, X. Peng, and J. Hai, “Secure data sharing and search for cloud-edge-collaborative storage,” IEEE Access, vol. 7, pp. 15 963 – 15972, 2019

[7]. J. Wei, W. Liu and X. Hu, "Secure and efficient attribute-based access control for multi authority cloud storage", IEEE Syst. J., vol. 12, no. 2, pp. 1731-1742, Jun. 2018.

[8]. A. Hussain, C. Xu, and M. Ali, “Security of Cloud Storage System using Various Cryptographic Techniques,” International Journal of Mathematics Trends and Technology (IJMTT), vol. 60, no. 1, pp. 45–51, 2018

[9]. Balogh, Z., Turčáni, M.:Modeling of data security in cloud computing. In: IEEE Annual Systems Conference, pp. 1–6.IEEE (2016)

[10]. Namasudra, S., Roy, P.: Secure and efficient data access control in cloud computing environment: a survey.J.Multiagent Grid Syst. 12, 69–90 (2016)

[11]. S. Karen, “Iot big data security and privacy versus innovation,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1628 – 1635, 2019.