An Extensive Review on Cloud Computing and Data Security Concern

Debasis Ghosh[1], Manoj Singh Bisht[2]

[1]*Associate Professor,* [2]*Assistant Professor*

Amrapali Institute of Technology and Science, Haldwani , India

Abstract-The term "Cloud computing" includes but not limited networking, virtualization, distributed computing, software and web services. A cloud comprises of a few components such as server, data-center and clients. It incorporates high availability, scalability, flexibility, reduced overhead for users, reduced cost of ownership, fault tolerance on demand services etc.

In modern era of communication, cloud computing has emerged as one of the most promising and evolving areas of computer science and IT industry. As on demand service cloud delivers infrastructure, platform, and software. Cloud provides several data centers at different geographical locations for availability service and reliability. Users can subscribe services and deploy applications at competitive cost from any location. Cloud computing is a globalized concept and there are no b orders within the cloud. Computers used to process and store user data can be deployed anywhere on the globe, depending on where the capacities that are required are available in the global computer networks used for cloud computing. The data can be stored remotely in the cloud by the users and can be access using thin clients as and when required. In order to store critical information many organizations are using cloud storage due to attractive features of cloud computing.

During the last decade, cloud computing has passed a long way from a term mainly known to Information Technology (IT) professionals and computer scientists to a buzzword, widely-known and recognizable by ordinary users.

The data and information that is saved on the Cloud is important to people with noxious intent so security is very important in cloud environment. So understanding the security measures that the Cloud provider uses is very important. The key thing that must be managed is the efforts to set up security that the cloud provider recently has set up.

Objective to improve the key management and data security in cloud computing based on advanced algorithm. Our proposed review examination work help to understand challenges and solution in cloud computing against various attacks and security threat in cloud computing.

Keywords : Cloud computing, data security, secure cloud, public cloud, private cloud, hybrid cloud.

I. INTRODUCTION

Cloud Computing, in a simple words, means Internet based Computing. Since the Internet can be thought of as clouds, and therefore the term cloud computing is used. Process execution and computation is done through the Internet. The users who use Cloud can have access to any resource and database with proper authority through the Internet anytime from anyplace and for as long as they need it, without having to worry about any management or maintenance of actual resources. Besides, resources and databases in cloud are usually very scalable and dynamic.

Indeed, cloud technologies, to a greater or lesser extent, are now days involved in almost every area of our daily life and economy ubiquitous cloud services are rapidly transforming the way wed business, maintain our health, educate and entertain ourselves.

Presently days, the huge information is put away on the web called as clouds. With use of distributed storage clients can store their information on the web. Cloud computing offers different types of assistance to the user. Data storage is one of them. But it is observed that there is very big problem of data stealing through the internet. More is the problem of data leaking & attacks on the data on clouds. The intention of this paper is to attain data security of cloud storage and to put together equivalent cloud storage security strategy. These strategies are combined with the outcomes of existing data by considering the security risks & user data on cloud storage & move towards the appropriate security technique , which is based on properties of cloud storage system.[2].

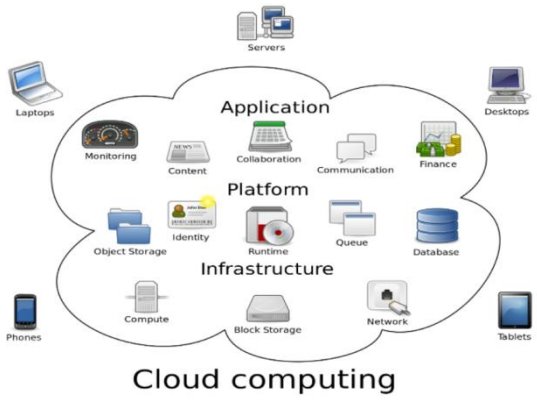

Fig.1.1 Cloud computing delivery model.

A model of cloud computing delivery has been shown in fig. 1.1 [11].

Cloud services are turning into an fundamental part of many associations. Cloud providers have to cling to security and privacy policies to guarantee their users' data remains confidential and secure. Despite the fact that there are some ongoing efforts on developing cloud security standards, most cloud providers are implementing a mish mash of security and privacy controls. This has prompted disarray among cloud providers regarding what safety efforts they ought to anticipate from the cloud administrations, and whether these measures would follow their security and consistence necessities. A comprehensive study has been conducted to review the potential threats faced by cloud consumers and have determined the compliance models and security controls that should be in place to manage the risk[3].

One of the most important security challenges Within the context of Cloud Computing, is to manage and assure a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mechanisms, processes and policies. The objective of controls on security in Cloud computing is, for the most part, similar to security controls in any IT environment from a functional security management perspective. The adaption and reuse of existing conventional security the board regions that must be improved for explicit Cloud registering prerequisites (e.g., dynamic reconfiguration, appropriated services, and so forth.) [4].

There are distinctively 3 components of the cloud:

a. Clients

Clients refer to the devices that the end users utilize to interface with the cloud when they require the services of the cloud. They can be PCs,laptops, smart phone mobile cell phones and so on. Thin clients are the PCs that don't contain interior hard drives and basically show the information from the servers. Thick customer is a typical computer that associates with the cloud utilizing internet browsers like Internet Explorer, Mozilla Firefox and so on. Thin clients have emerged as a popular solution because of their lessened price and enhanced information security. In-formation security is better in case of thin clients as the processing of data and storage takes place directly on the server without involving the client.

b. Data Center

It is an agglomeration of servers where the application to which the users have subscribed is placed. It can be stored anywhere and can be accessed via the internet. A superior solution is to use virtual servers through a single physical server. A software can be installed that permits multiple instances of virtual servers to run whenever the physical server is accessed.

c. Databases

The information or data is stored at these places in the cloud. The storage units can consists of several servers stored in a single place like the Facebook’s data storage or it can extend over a widespread area with several servers around the world connected with each other.

A classic definition of security—in terms of its basic characteristics—specifies it in terms of the CIA triad; the acronym “CIA” stands for confidentiality, integrity and availability three key requirements for any secure system. They are defined as follows [10]:

1. Confidentiality: It is the capacity to conceal data from those individuals unauthorized to see it. It is the premise of numerous security components ensuring data as well as different assets.

2. Integrity: It is the capability to guarantee that information is a precise and same as the original one [10].

3. Availability: It ensures that a resource is readily accessible to the authorized user upon the user’s request.

II. LITERATURE REVIEW

According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now operate on the cloud. However, like any new technology adoption, cloud computing adoption opens new forms of security risks. In 2018 [1] D. R. Bharadwaj, A. Bhattacharya and M. Chakkaravarthy explores security issues related to cloud computing and proposes a cloud-native scalable security solution for the cloud. The paper investigates some of the key research challenges of cloud security solutions to secure the dynamic cloud environment and provides a practical solution to overcome the challenges that the cloud providers and consumers face securing their data and valuable assets.

With utilization of cloud storage services users can store their data on the internet. Cloud computing provides various services to the users. Data storage is one of them. But it is observed that there is very big problem of data stealing through the internet. A. Markandey, P. Dhamdhere and Y. Gajmal [2] introduced more is the problem of data leaking & attacks on the data on clouds. The intention of this examination is to attain data security of cloud storage and to put together equivalent cloud storage security strategy. These strategies are combined with the outcomes of existing data by considering the security risks & user data on cloud storage & move towards the appropriate security technique , which is based on properties of cloud storage system. The examination will go in to subtle elements of information assurance strategies and methodologies utilized all through the world to guarantee most extreme information insurance by diminishing dangers and dangers. Accessibility of information in the

cloud is helpful for some applications yet it postures hazards by presenting information to applications which may as of now have security provisos in them. Also, utilization of virtualization for distributed computing may chance information when a visitor OS is keep running over a hypervisor without knowing the unwavering quality of the visitor OS which may have a security proviso in it. The research work will likewise give a knowledge on information security perspectives for Data-in-Transit and Data-at-Rest [2].

In many organizations cloud services are becoming an essential part. To ensure their users' data remains confidential and secure cloud providers have to adhere to security and privacy policies. Though there are some ongoing efforts on developing cloud security standards, most cloud providers are implementing a mish-mash of security and privacy controls. This are creating huge confusion among cloud consumers as to what security measures they should expect from the cloud services, and whether these measures would comply with their security and compliance requirements. A. Hendre and K. P. Joshi,2015 [3] have conducted a comprehensive study to review the potential threats faced by cloud consumers and have determined the compliance models and security controls that should be in place to manage the risk. Based on this study, developed an ontology describing the cloud security controls, threats and compliances. They also developed an application that classifies the security threats faced by cloud users and automatically determines the high level security and compliance policy controls that have to be activated for each threat. The application also shows old or previous cloud providers that support these security policies. Cloud consumers can utilize system to formulate their security policies and find compliant providers even if they are not familiar with the underlying technology.

M. Kretzschmar, M. Golling and S. Hanigk,2011 [4]Within the context of Cloud Computing, one of the most important security challenges is to manage and assure a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mechanisms, processes and policies. The fundamental objective of Security controls in Cloud computing is, for the most part, no different than security controls in any IT environment from a functional security management perspective. The adaption and reuse of existing traditional security management areas that have to be enhanced for specific Cloud computing requirements(e.g., dynamic reconfiguration, distributed services, etc.), is introduced. Based on the collection of various Inter-Cloud use cases and scenarios within the private and public sector like DMTF (Distributed Management Task Force), NIST (National Institute of Standards and Technology), GICTF (Global Inter-Cloud Technology Forum) and ENISA (European Network and Information Security Agency) analyzed and summarized the range of requirements for security management. As these requirements are not yet fulfilled by current security management approaches, derived a set of security management areas that describe all identified functional aspects. This set will work as a base of our future development towards security management architecture for the Inter-Cloud.

J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, [5] Data sharing in cloud computing enables multiple participants to freely share the group data, which improves the efficiency of work in cooperative environments and has widespread potential applications. However, within a group how to ensure the security of data sharing and how to efficiently share the outsourced data in a group manner are impressive difficulties. Note that key agreement protocols have played a significant function in secure and efficient group data sharing in cloud computing. In this examination, by taking advantage of the symmetric balanced incomplete block design (SBIBD), a novel block design-based present key agreement protocol that supports multiple participants, which can flexibly extend the number of participants according to the structure of the block design in a cloud environment. Based on the introduced group data sharing model, present general formulas for generating the common conference key IC for multiple participants. Note that by benefiting from the (v, k + 1, 1)-block design, the computational complexity of the introduced protocol linearly increases with the number of participants and the communication complexity is greatly reduced. Additional, similar to Yi's protocol the fault tolerance property of our protocol enables the group data sharing in cloud computing to withstand different key attacks.

J. Dangur and S. M. Jaybhaye,[6] In Cloud computing system data owner stores the data files remotely to utilize the cloud resources. Though data sharing in cloud computing is most common approach used in most communication network because of the different advantages but it also having some difficulties. This scheme involves three general approaches. Treebased Group Diffie-Hellman (TGDH) based group key agreement, proxy re-encryption and proxy signature. The introduced framework tries to reduce the overhead of uploading as well as downloading of the files in the cloud storage. The proxy signature technique is used which allows the group leader to effectively grant the permission to one or more selected group members. The proxy re-encryption is introduced which substitutes most computationally demanding operations to Cloud storage Servers without disclosing any sensitive information or data. The enhanced TGDH scheme permits the group to update the group key pairs using Cloud Servers which does not require all the group members to be online. Introduced

scheme provides more efficient, flexible and secured framework for group communication in cloud.

With the popularity of group data sharing in public cloud computing, the privacy and security of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party because of its semi-trust nature, and thus the traditional security models cannot be straightforwardly generalized into cloud based group sharing frameworks. In this examination, K. Xue and P. Hong [7] reported a novel secure group sharing framework for public cloud, which can effectively take advantage of the cloud servers' help but have no sensitive data being exposed to attackers and the cloud provider. The framework combines proxy signature, enhanced TGDH and proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members. The enhanced TGDH scheme enables the group to negotiate and update the group key pairs with the help of cloud servers, which does not require all of the group members been online all the time. By adopting proxy re-encryption, most computationally intensive operations can be delegated to cloud servers without disclosing any private information. Extensive security and performance analysis shows that our presents scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

III. SYSTEM MODEL

In such a case computing services can be utilized from various or huge resources, rather than remote servers or local machines. There is no standard dentition of Cloud computing. Generally it consists of bunch of distributed servers known as masters, providing demanded services and resources to different clients known as clients in a network with scalability and reliability of datacenter.

3.1 Cloud Components

A classical Cloud computing system consists of 3 main elements such as clients, datacenter, and Distributed servers. Each element has a definite purpose and plays a specific role [10].

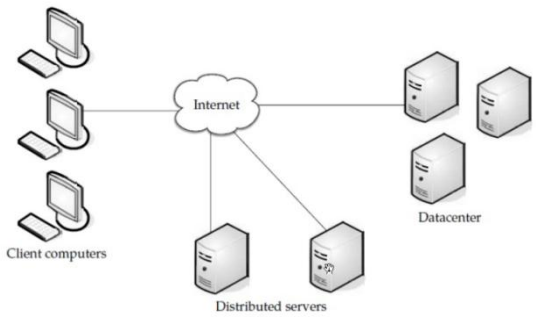

Fig.3.1 Components of cloud

3.2 Type of Clouds

- Public Clouds: A public cloud is a model of cloud computing in which a service provider makes resources, such as applications and storage, available over the internet on a pay-per usage basis. To satisfy increasing demands in a cost-efficient way, the organization requires having an integration of the private and a public cloud [9].
- Private Clouds: A private cloud is a model of cloud computing that is implemented within the corporate firewall, under the control ofthe IT department with limited resources [9].
- Hybrid Clouds (combination of both private and public clouds: A hybrid cloud, as the name implies is composed of a minimum of one private cloud and a minimum of one public cloud. Ideally, this model allows a business to get the advantages of measurability and cost-effectiveness supplied by the public cloud model while retaining the privacy, security and policy of the private cloud model [8]

3.3 Virtualization

It is a very use full concept in context of cloud systems. Virtualization means not real but works a real ”something which isn’t real”, but gives all the facilities of a real. It is the software implementation of a computer which will execute different programs like a real machine [10].

Virtualization is related to cloud, due to utilizing virtualization an end user can use different services of a cloud. The remote datacenter will provide different services in a full or partial virtualized manner [10].

IV. CONCLUSION

In this examination the major aspects of security and privacy in CC has been explored based on prior work in the domain. A brief introduction of cloud computing its architecture various type of cloud has been drafted along with categorization of various security and privacy issues in cloud computing system. The separation of issues has proven useful, resulting in a better organization of this literature survey. Next, there is possibility to divide a security and privacy issues into problems and solutions the literature review of the security and privacy problems and solutions within this categorization framework, an customized solution can be driven in future work

REFERENCES

[1] D. R. Bharadwaj, A. Bhattacharya and M. Chakkaravarthy, "Cloud Threat Defense – A Threat Protection and Security Compliance Solution," 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 2018, pp. 95-99, doi: 10.1109/CCEM.2018.00024.

[2] A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018, pp. 633-636, doi: 10.1109/GUCON.2018.8675033.

[3] A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, 2015, pp. 1081-1084, doi: 10.1109/CLOUD.2015.157.

[4] M. Kretzschmar, M. Golling and S. Hanigk, "Security Management Areas in the Inter-cloud," 2011 IEEE 4th International Conference on Cloud Computing, Washington, DC, 2011, pp. 762-763, doi: 10.1109/CLOUD.2011.83.

[5] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.

[6] J. Dangur and S. M. Jaybhaye, "Framework for secure data sharing in dynamic group using public cloud," 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, 2016, pp. 199-204, doi: 10.1109/CAST.2016.7914966.

[7] K. Xue and P. Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459-470, 1 Oct.-Dec. 2014, doi: 10.1109/TCC.2014.2366152.

[8] Peter Mell and Tim Grance. The nist definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2009

[9] G. Mangal, P. Kasliwal, U. Deshpande, M. Kurhekar and G. Chafle, "Flexible Cloud Computing by Integrating Public-Private Clouds Using OpenStack," 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, 2015, pp. 146-152, doi: 10.1109/CCEM.2015.26.

[10] Ram Prasad Padhy, PGoutam Prasad Rao, “Load balancing in cloud computing systems”, Phd thesis, National Institute of Technology, Rourkela, 2011

[11] Z. Gilani, A. Salam, and S. Ul Haq, "Deploying and managing a cloud infrastructure : real world skills for the CompTIA cloud+ certification and beyond," Wiley, Jan. 2015