A Survey on Security Challenges in Cloud Computing

A.Vikram*, G.Gopinath**
*Computer Science and Engineering, Bharathidasan University, Tiruchirappalli.
Email: vikram.aug1984@gmail.com
**Director, Institute for Entrepreneurship and Career Development (IECD)
Bharathidasan University, Tiruchirappalli.

ABSTRACT:
Cloud computing is an Internet-based computing solution which provides the resources in an effective manner. A serious issue in cloud computing is security which is a major hindrance for the adoption of cloud. The most important threats of cloud computing are identified and understood in this survey. Cloud Computing has transformed the software support for large systems from server to service oriented paradigm. This drift has evolved new challenges for design and delivery of services over heterogeneous needs and environments. This brings about risks and challenges for systems. The systems over internet are vulnerable to performance and security risks**,** integrating and deploying data with cloud applications without enforcing any access management will elevate privacy and confidentiality concerns. Different data owners store data in heterogeneous format based on their need. This leads to the data interoperability problem. Thus the concept of Network Security can be applied over the cloud network, where several encryption algorithms are applied to provide integrity on the data. The performance is a complex evaluation but risks that are related to privacy can be handled at different levels of abstraction in cloud model. This paper addresses the security problem, challenges and analyzes the available measures to handle.
Keywords **— Cloud Computing, Cloud security, Security challenges, Network level security, Application level security.**

I. INTRODUCTION

Cloud Computing provides us means of accessing the applications as utilities over the Internet. It allows us to create, configure, and customize the applications in online. Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application. Cloud computing offers platform independency, as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications viz. mobile, a collaborative one. There are some services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

A. Deployment Model

Deployment models defines the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.

1) Public Cloud

The public cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

2) Private Cloud

The private cloud allows systems and services to be accessible within an organization. It is safer because of its private nature.

3) Community Cloud

The community cloud allows systems and services to be accessible by a group of organizations.

4) Hybrid Cloud

The hybrid cloud is a combination of public and private cloud, in which the problematic activities are performed using private cloud while the non-critical activities are performed using public cloud.

B.Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Anything-as-a-Service (XaaS) is yet another service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service. The Infrastructure-as-a-Service (IaaS) is the most primitive level of service.

1) INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

2) PLATFORM-AS-A-SERVICE (PAAS)

PaaS provides the runtime environment for applications, development and deployment tools, etc.

3) SOFTWARE-AS-A-SERVICE (SAAS)

SaaS model allows using software applications as a service to end-users.

II.RISKS RELATED TO CLOUD COMPUTING

Although cloud Computing is a promising technology with various benefits in the world of computing, it comes with risks. Some of them are discussed below:

A. Security and Privacy

It is the biggest burden about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to cloud service providers. Although the cloud computing vendors ensure highly secured password protected accounts, any sign of security breach may result in loss of customers and businesses.

B. Lock In

It is very difficult for the customers to switch from one **Cloud Service Provider (CSP)** to another. It results in dependency on a particular CSP for service.

1) Isolation Failure

This risk involves the failure of isolation mechanism that separates storage, memory, and routing between the different tenants.

2) Management Interface Compromise

In case of public cloud provider, the customer management interfaces are accessible through the Internet.

3) Insecure or Incomplete Data Deletion

It is possible that the data requested for deletion may not get deleted. It happens because either of the following reasons

- Extra copies of data are stored but are not available at the time of deletion
- Disk that stores data of multiple tenants is destroyed.

III. SECURITY CHALLENGES IN CLOUD COMPUTING

Clouds have been used for various applications including business implementation, collaboration services, online presence, R&D projects, social networking, as business tools etc. With these areas of system developments and usage: risk analysis, estimation, control and treatment become essential. The cloud service provider for cloud makes sure that the customer does not face any issues such as loss or theft of data. The following table gives the security challenges and its associated threats [3,4]. These challenges and threats are also distributed according to Cloud Security Alliance (CSA).

IV. CLOUD SECURITY ISSUES

This section deals with various aspects of security in Cloud Computing.

Table 1 Methods used in Cloud Security Issues

Ref. Num	Author Name	Title	Methods	Advantage	Future work
6	Swetha Tera, S. Ramachandran, and P. Shankar Murthy	Computational Analysis of Encrypted Database to Provide Confidentiality	Crypto Algorithms	It concludes encryption in cloud tasks are very innovative	In future extends some of the SQL functions are not working in the CryptDB, it needs to improve CryptDB by working with all SQL functions with results.
8	Mr.Prasad P.S, Dr.Ali Ahammed G.F.	Attribute-Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing	Attribute-Based Encryption (ABE) Techniques	We proposed a novel structure of secure distribution of Personal Health Records in cloud computing in this paper.	We enhance an existing Multi Authority Attribute Based Encryption scheme to manage on-demand user revocation, efficient, and prove its security.
10	Ganesh mouli Bandari, N. Subhash Chandra	Secure Cloud Storage through Public Auditing and Cryptographic Primitives	third party auditor (TPA),	We propose a privacy-preserving public auditing	we extend that for the further purpose of users and our

	,V.Krishna			system for secured data in Cloud Computing.	privacy preserving public auditing was involved into a multi-user setting

In [6], Cloud user's demands security to their data which are stored in data repositories of cloud service provider. Thus in the cloud network the concept of Network Security can be applied, where many encryption algorithms provides integrity on the data. Thus the algorithms include Symmetric encryptions, Asymmetric encryptions, Hashing algorithms and Digital signatures. These algorithms provide security and it won't be applied on query based data retrieval from databases that certain queries are used to invoke the data. So till now the researchers had proposed several models to provide security to the data in database and are not up to the mark. Thus the operations are done in database which is remotely located, away from user, providing encryption on queries and data together will make an efficient approach. Such mechanisms like Homomorphic encryption, Order-preserving encryption are examined to meet all security issues over a cloud termed as "CryptDB".

In [7], the internet of things permeates more aspects of life, the desire to access one's social network from whatever connected device available will become a requirement. Cloud-*based* personal data will be remotely accessible from any connected device is evitable. The solution of this paper is to secure and assessable private social networks by creating a "Security Box" on which a private social *network* can provide safely distributed access. This access is managed, yet interactions are not burdened by onerous rules and membership overhead, that plague many private networks. The Security Box is a cloud-based private social network security mechanism, implemented on Amazon EC2/S3 cloud. The Security Box network provides multiple levels of security, enhanced *personal* and group encrypted files database, authorization control and 128-bit AES encrypted key management. To apply a Client/Server network model, the resulting private social network whose members enjoy an extensively accessible shared database, suitable protected from unauthorized intrusion.

In [8], Personal health record (PHR) is a patient-centric model of health information exchange and it has to be stored at a third party i.e., cloud providers. There are some concerns like personal health information that can be exposed to third party servers aweless to an unauthorized party. In order to assure the patients' authority over approach to their personal PHRs, it is an assuring method to encrypt the PHRs before outsourcing. These are some issues like flexible access, scalability in key management, privacy exposure and efficient user revocation and it has to be continued to the most significant dispute towards accomplishing fine-grained, cryptographically imposed data access control. Sequentially to have control for data access to PHRs stored in semi trusted severs, a novel patient-centric structure and a suite of methods is proposed in this paper. We leverage attribute-based encryption (ABE) practices to attain scalable and fine grained data access control for personal health records to encrypt each patient's PHR file. In this paper, it will be concentrated on the multiple data owner situation, which it has to be distinct from previous works in secure data outsourcing. It divides the users in the PHR system into several security domains which decreases the key management complexity for owners and users. The patient confidentiality is maintained and it will be guaranteed by exploiting multi-authority ABE. In emergency scenario, the proposed scheme provides dynamic change of access policies. Extensive analytical and experimental results are given which shows the security, scalability, and efficiency of our scheme.

In [9], a computational technology that fulfills a user's requirements of physical and virtual resources and it is a paradigm where jobs are assigned to a composition of connections, software's and services. The cloud computing shares distributed resources via the network in an open environment and it has its own associated risks and threats that compromises integrity and encompasses theft, data leakage and insecure platform. In this paper, we have been researched a few of the popular cloud services providers in terms of security threats they faced in the past. We have also been mentioned a few solutions that will help in improving the security of data in the cloud and increase trust between the customers and the cloud service providers.

In [10], if the user wants to store their data remotely into the cloud and so as to enjoy the on demand of high quality application and services for the shared pool of configurable computing storage of outsourcing data and the users can be relieved from the burden about local storage and

maintenance of data. However, in general the users have no longer physical possession of large size of outsourcing data makes data integrity protection in Cloud Computing a challenging, potentially formidable task for users especially with constrained resources. To enable public availability of cloud stored data for security is of critical importance and they can resort to an external third party to check the honesty of user outsourced data when user needed. To securely introduce an effective third party auditor (TPA), the following of two main requirements have to meet:

1) TPA should have efficacy to audit the cloud data storage without local copy of data demanding, and no need of additional on-line burden to the cloud user.

2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

In this paper they explained that they are combining the public key based Homomorphism authenticate with random masking to achieve the privacy preserving public cloud data auditing system, for to meet all the above requirements.

In [11], however, without the adequate belief and strong integrity assurance, it would be difficult to expect clients to completely turn over control of their computation to the cloud. Thus the securing cloud computation becomes an imperative and challenging task, especially in the aspect of integrity verification. To address this challenge, we have to propose a hassle-free, fixed-rate, and job-based software as a service cloud model along with the integrity verification mechanisms, with particular focus on outsourcing the widely applicable engineering optimization problem, i.e., convex optimization. We aim to construct the efficient integrity verification mechanisms using application-specific techniques. Our security design does not require the use of heavy cryptographic tools and we have to leverage the inherent structure of the optimization problems and make the computation outsourcing proof-carrying to achieve efficient integrity verification. The proposed design provides substantial computational savings on the client side and introduces marginal overhead on the cloud side. We further prove its correctness and soundness. The extensive experiments under the real cloud environment show our mechanisms ensure strong integrity assurance with high efficiency on both the client and the cloud sides and are readily applicable in current practice.

In [12], many users place their data in the cloud. But the fact that users has no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. So the correctness of data, security is a prime concern. This article studies the issue of ensuring the integrity and security of data storage in Cloud Computing. Security in cloud is achieved by signing the data block before sending to the cloud and we are enabling public audit ability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worried free. To securely introduce an effective TPA, the auditing process will have no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy preserving public auditing and we are extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Wide security and performance analysis shows the proposed schemes are probably secure and highly efficient.

In [13], Proving security to multi owner data while preserving data and identity privacy from unauthorized users cloud is still a big challenging issue. In dynamic groups the members may frequently join into it or they may leave at any time, hence there is a need to have a robust system to protect the data from the unauthorized access from the cloud. To provide privacy and security to the stored data in the cloud it has to be encrypted and the decryption keys to be shared to only some set of authorized users only. The new user register into the group the group manages has to provide access permissions to read the existing data present in the cloud. This paper provides the reliability as well as improving the scalability by increasing the count of group managers dynamically. The storage overhead the encryption and decryption keys computation cost of our scheme is independent with the number of revoked users. In cloud these resources are shared among the different geographical locations, in order to preserve security and privacy, the users are divided into some groups and the data decryption permissions are given to the only the set of users present in that particular group. Multiple users share their data in the cloud network. In cloud computing the groups are dynamically changes. As the group members are changing frequently it became a challenge to secure data of multi owners from the revoked users. The users present in other groups are not allowed to access the data from other group members shared information.

V. CONCLUSION

Most of the scare of cloud computing comes from the notion of loss of control of subtle data. The Prevailing control techniques do not sufficiently address cloud computing third party information storage and processing needs. Secure Semantic Data Integrator (SSDI). This system utilizes full potentials of semantic data to make secure data integration possible. SSDI enables the user to share the data emanating from heterogeneous sources, with security setting of their own. This feature maintains the data ownership status which makes data owner and data provider classification noticeable. In this work, we discussed the architecture of the protection systems that elaborates the high level structure of the system. It future elaborates the detailed design of the system along with the core exertion techniques. These techniques should reduce most of today's apprehensions of cloud computing and have the competence to give supportable business intelligence benefits in upcoming years.

REFERENCES

[1] Wentao Liu, Research on Cloud Computing Security Problem and Strategy, 978-1-4577-1415-31121 ©2012 IEEE

[2] NIST defmition of Cloud. NIST 500-292 "NIST Cloud Computing Reference Architecture"

[3] Ms. Disha H. Parekh, Dr. R. Sridaran, "An Analysis of Security Challenges in Cloud Computing", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 4, No.1, 2013

[4] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki,Sugata Sanyal, "A Survey on Security Issues in Cloud Computing and Associated Mitigation", International Journal of Computer Applications (IJCA), June 2012, pp: 47 - 66.

[5] Mircea Georgescu, Natalia Suicirnezov, "Issues Regarding Security Principles In Cloud Computing", The USV Annals of Economics and Public Administration Volume 12, Issue 2(16), 2012.

[6] Swetha Tera, S. Ramachandram, and P. Shankar Murthy "Computational Analysis of Encrypted Database to Provide Confidentiality" International Journal of Computer Theory and Engineering, Vol. 7, No. 2, April 2015.

[7] Yuncheng He "Description of a Cloud Based Private Social Network Security Scheme" International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015.

[8] Mr.Prasad P S, Dr. G F Ali Ahammed "Attribute-Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing" Prasad P S et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5038-5040.

[9] Navan Preet Singh, Bhavkaran Singh Walia" Assay of Data Security in Cloud Computing" Navan Preet Singh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6599-6601.

[10] Ganesh mouli Bandari, N. Subhash Chandra ,V.Krishna "Secure Cloud Storage through Public Auditing and Cryptographic Primitives" International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 2 – Sep 2014.

[11] Zhen Xu, *Student Member, IEEE*, Cong Wang, *Member, IEEE*, Kui Ren, *Senior Member, IEEE*,Lingyu Wang, *Member, IEEE*, and Bingsheng Zhang "Proof-Carrying Cloud Computation: The Case of Convex Optimization" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 11, NOVEMBER 2014

[12] M. Madhavi, O.Srinivasa Reddy, Dr. S.Sai Satyanarayana Reddy "Public Auditing For Secure Cloud Storage with HLA" IJCSN International Journal of Computer Science and Network, Volume 3, Issue 4, August 2014.

[13] Dinesh Babu Junuthla, Mr.CT. Kiran Kanth " Preserving Security and Privacy to Data of Multiple owner group in the Cloud" INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS ISSN 2320-7345.