JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Study on Research Problems in Data Security in Cloud Computing

M. Vishnupriya

Department of Computer Science, Idhaya College for Women, Kumbakonam, Tamilnadu, India

Corresponding Author: reachtovishnu93@gmail.com

Available online at: www.ijcseonline.org

Abstract— Cloud Computing has attracted considerable attention in both industry and academic. It leads to gain effectiveness deployment, efficiency development and pay on- demand in purchasing and maintaining infrastructure. The resources stored in the cloud are managed by the Cloud Service Provider. Even though, cloud computing provides more advantages to the users, there exists security problem in cloud computing. The data owner who outsources their critical data are unaware of how data being stored in the cloud and who accessing their data. This arises many security issues in cloud computing. This paper discusses several security issues that occur over the cloud and solutions offered by various researches.

Keywords—Cloud Computing, Security issues, Data Security

I. INTRODUCTION

Cloud Computing is an emerging technology. It is used to manipulating, configuring, and accessing the online applications. It also offers virtual data storage, infrastructure and application. It combines both software and hardware based on computing resources delivered as a network service. According to the official NIST definition: “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”[21].

A. CLOUD COMPUTING SERVICESMODELS

Infrastructure as a Service (IaaS)

The infrastructure as a service that provides virtualization computing resources. The cloud infrastructure refers to the hardware and software such as servers, storage and virtualization software. IaaS layer is provides several services that include Computer Hardware, Network, InternetConnectivity, Platform Virtualization, and Utility Computing [22].

Platform as a Service (PaaS)

The computing platform that allows creation of web applications easily without the complexity of maintaining the software [23]. The cloud delivers hardware and software tools. It is used to need for application development. The platform as a service that delivers the application over the Internet. It is provided operating system and networks.

Software as a Service (SaaS)

SaaS as service and provides an application to customers either as a service on demand [23]. The software as a service it required software, operating system, and network is provided on cloud computing. This is mainly accessed through web portal and service oriented architecture.

B. DEPLOYMENTMODELS

Public Cloud

The public cloud as a cloud made available in a pay-as-you-go manner to give the general public.

Private Cloud

A Private Cloud is for single organization. It is an “internal data center of a business or other organization, not made available to the general public”. The resources and applications are managed by the organization itself [22].

Community Cloud

A Community Cloud is “shared by several organizations and supports a specific community that has shared concerns”. It allows system and services to be accessible by a group of organizations.

HybridCloud

A Hybrid Cloud takes shape when a private cloud is supplemented with computing capacity from public clouds. The hybrid cloud is a combination of public and private cloud. The business critical activities are performed using private cloud and the non-business critical activities are performed using publiccloud.

C. CHARACTERISTICS OF CLOUDCOMPUTING

On Demand Self Service

The Computing services such as network, email, applications, or server services can be provided norequired human interaction with each service provider [23]. The cloud service providers providing on-demand self-services contain Amazon web services, Microsoft, IBM and salesforce.com.

Broad Network Access

The resources available over the internet are utilized by standard mechanisms [24].

Resource Pooling

The resources are pooled together to serve multiple customers, with different physical and virtual resources dynamically assigned and reassigned according to the customer demand.

Rapid Elasticity

The cloud is flexible and scalable to submit need. The capability can be elastically provisioned and released in some cases automatically to scale rapidly outward and inward suitable with demand.

Measured Service

The cloud system automatically control and optimize resources apply by leveraging a metering capability at some level of abstraction. The types of service such as storage, processing, bandwidth, and active user accounts. Then the resource usage can be measured, controlled, and reported providing transparency for the provider and user [24].

D. BENEFITS

Expand scalability

It provides on demand scalability means can scale up and scale down resources and manage them.

Less infrastructure costs

No need to spend more money for infrastructure. It provide best service for users, according to their needful. Organisations preserved memory and resources according to their needs [25].

Increase utilization

Many client can share computing service, utilization is more increased in cloud computing.

Improve reliability

We can store more data in cloud, backing up and restoring of data is easier compared to physical device.

Easy reach to resources

Registered user can easily access the data from anywhere and anytime with the help of internet connection.

II. RELATED WORK

NareshVurukonda et al. [1] discussed cloud computing data storage security issues such as data privacy, integrity, recoverability and vulnerability. Identity management and access control issues in cloud computing to ensure data integrity and confidentiality were stated and also service level agreements and legal issues related to data storage were stressed. Finally, the possible solutions for all those issues were analysed by comparing various existing security schemes and techniques.

VelumadhavaRao et al. [2] elaborated data security challenges in cloud based environment. They analysed the security challenges occured in organization related to cloud storage. Various data security problems in cloud such as confidentiality, integrity, locality, breaches and access control were highlighted. Eventually, sseveral security challenges in cloud were also summarized. Finally, the strategies for solving security issues were suggested.

Sultan Aldossary et al. [3] discussed cloud computing security issues such as data security, privacy, availability and integrity. Elaborated data storage issues in cloud computing and the solutions for those issues were analysed. Top threats of cloud computing such as data loss, data breaches, malicious insider, insecure interfaces and APIs were explained. An overview of virtualization security issues were presented. The major data security issues namely data confidentiality, integrity, availability were highlighted, solutions and techniques to overcome the issues were also discussed.

Ahmed Albugmi et al. [4] described security risks and concerns in cloud computing such as virtualization, storage in public cloud and multi- tenancy. Discussion on two states of data and its security threats was made. An overview of encryption techniques for data at rest and data in transmit were explained. Some basic cryptographic techniques such as block ciphers, stream ciphers, and hash functions were also explored. A detailed analysis of existing data security techniques were done to secure the data over thecloud.

PriyaIyer et al. [5] focused on data security and privacy issues in cloud computing. Four cloud security controls namely deterrent controls, preventive controls, detective controls and corrective controls were described. Security issues related to cloud data storage were discussed. Various data security problems in cloud such as data integrity, data confidentiality were highlighted. Techniques to solve those issues such as homomorphic encryption, hybrid techniques, and distributed storage were analysed. Finally, some common security mechanisms were summarized.

Babitha et al. [6] described different privacy protection, data security issues in cloud computing and also provided an overview of various encryption techniques. They used AES algorithm for encryption to increase data security and confidentiality. The proposed model includes Short Message Service (SMS) alert to avoid malicious user access to the data. They analysed this model based on delay and proved this gives the best data security in cloud environment.

AkshitaBhandari et al. [7] proposed a framework for data security both in transmission and storage. The proposed model secured user data while transferring and storing using classification of data, Hashed Message Authentication and Index Building. They stated that this combination of techniques provides greater security to the data. They compared this framework with existing framework and shown it has better execution time.

MrinalKantiSarkar et al. [8] overviewed cloud data security issues and proposed a framework to ensure data storage security in cloud computing. They also discussed proposed key generation algorithm, encryption algorithm and decryption algorithm. They stated that proposed framework has some special features than the existing models. The analysed this model and proved that this framework has feasibility, scalability and efficiency.

PrabuKanna et al. [9] proposed hybrid encryption technique using RSA and ECC to enhance the security of user data. They uses proxy re-encryption algorithm to encrypt the keyword. They compared the proposed algorithm with the existing algorithm and proved that it takes minimum execution time. Two phase encryption has done on user's data to ensure the security of the data stored in the cloudserver.

Shakeeba S. Khan et al. [10] proposed a multilevel encryption technique to eliminate the data privacy issue and to enhance the data security in cloud. The proposed technique combines two different security algorithms such as DES and RSA. It allows only the authorized user to access the data. They stated that this multilevel encryption will provide more security for cloud storage than single levelencryption.

Arockiam et al. [11] proposed a secured confidentiality techniques to ensure the data security stored in the cloud. The proposed technic is based on the symmetric key encryption algorithm. They describes this technique as Security as a Service in cloud, which contains of three security service algorithms such as AROcrypt, MONcryptand AROMONcrypt. AROCrypt algorithm includes security service algorithm and random number generation algorithm. They also compared the proposed technic with other existing techniques and proved that it offers better performance and maximum protection.

Geeta Sharma et al. [12] proposed a scheme for data security in cloud computing. They discussed the limitations of classical cryptography, quantum key distribution. The scheme integrated Advanced Encryption Standard (AES) algorithm with Quantum cryptography. They also compared this hybrid technique with other existing algorithms and stated that this algorithm is suitable for high security applications like government agencies, military etc. because this scheme produces composite keys which are hard to envisage by adversaries.

Boomija et al. [13] proposed a method for secure data sharing in cloud computing. They uses addictive similarity based ElGamal Like encryption which includes proxy re-encryption capabilities to prevent the data from adversaries. They also implemented the method using sample medical data in CloudSim and stated that the proposed model is applicable for content distribution, electronic mail forwarding and monitoring process.

Arul Oli et al. [14] discussed security issues in cloud storage and need for data security. They proposed a novel approach using encryption technique and key management technique for secure cloud storage. They described that the proposed method is used for improving data confidentiality in cloud storage by enhancing dynamic sharing between users. They specified that by protecting the confidentiality of data, the security of the data isenvisaged.

Munwar Ali Zardhar et al. [15] proposed a data classification approach to ensure data confidentiality in cloud computing. They used K- NN data classification technique to classify the data based on cloud security needs. They classified the data in the cloud based on sensitive and non- sensitive data and then secured the sensitive data by using RSA algorithm. They implemented their proposed technique using CloudSim and proved the security of data in cloudstorage.

Yuhong et al. [16] elaborated data security issues in cloud storage and proposed a new framework to ensure data confidentiality in cloud computing. They integrated two techniques such as encryption technique and trust-based technique to achieve secure cloud storage. The proposed framework includes three components such as encryption model, trust model and decision-making model which allows CSUs to encrypt the sensitive data before storing it in the cloud and checks for data correctness from time totime.

KhaleedM.Khan et al. [17] discussed the importance of data confidentiality in cloud computing and proposed an approach for secure transmission of matrix multiplication over cloud networking using randomisation, column-row shifting and size alteration of matrices. They also discussed data hiding protocols and data retrieving protocols.

Arul Oli et al. [18] proposed a confidentiality technique to ensure secure storage in cloud computing. They used obfuscation technique to strengthen the numerical data in public cloud storage. The numerical data gets encrypted before uploading into cloud storage. They used cryptographic techniques and five different mathematical operations to ensure the security of numerical data in cloud computing.

MalekNajib Omar et al. [19] discussed virtualization for cloud computing, security feebleness of cloud computing. The proposed technique used biometric encryption to ensure data confidentiality in biometric data. They stated that biometric encryption uses high level security against confidentiality and privacy issues and it was mainly used for ensuring biometric data in cloud computing.

Jayapandian et al. [20] overviewed the cloud computing client side data security issues. They proposed a new technique to improve security trust on client side data using both Hierarchical Attribute Set Based Encryption and Blowfish encryption. This hybrid encryption done at the client side. They proved by using mathematical model that technique assurances secure end to end transmission of data without any wrongdata.

Table 1.1 Cloud Computing Data Security issues

Author	**Issues**	**Algorithm/Tools /Methods Used**
Babitha et al. [6]	Data security and privacy	AES algorithm and SMS Service to avoid malicious user access
AkshitaBhandari et al. [7]	Data Security	Classification of data, Hashed Message Authentication and Index Building
MrinalKantiSarkar et al. [8]	Data Security	Proposed Key generation algorithm
PrabuKanna et al. [9]	Data Security	Hybrid encryption using ECC and RSA
Shakeeba S. Khan et al. [10]	Data Privacy	Multilevel encryption using DES and RSA
Arockiam et al. [11]	Data Confidentiality	AROCrypt security service algorithm
Geeta Sharma et al. [12]	Data Confidentiality	Integrated Advanced Encryption Standard (AES) algorithm with Quantum cryptography
Boomija et al. [13]	Data Confidentiality	Addictive similarity based ElGamal encryption
Arul Oli et al. [14]	Data Confidentiality	Security framework using Key Generation Scheme
Munwar Ali Zardhar et al. [15]	Data Confidentiality	K-NN data classification technique and RSA algorithm
Yuhong et al. [16]	Data Confidentiality	Integrated two techniques such as basic encryption technique with data correctness verification and trust-based technique
KhaledM.Khan et al. [17]	Data Security	Randomisation, Column-row shuffling and size alteration of matrix
Arul Oli et al. [18]	Data Confidentiality	Obfuscation Technique
MalekNajib Omar et al. [19]	Data Confidentiality	Biometric Encryption
Jayapandian et al. [20]	Data Security	Hybrid encryption using Hierarchical Attribute Set Based Encryption and Blowfish encryption

III. MOTIVATION

Data security is one of the major issues in cloud computing. Here, the data are randomly dispersed and stored in different machines and storage devices. This results in data security such as privacy, integrity, confidentiality and also trust between the user and cloud service provider. Many techniques have been proposed to reduce the various data security issues in cloud storage listed in the table 1.1. However, the existing techniques have not given a full security over the cloud data. The main motivation behind this survey is to find an improved solution for data security over the cloud.

IV. CONCLUSION

Though cloud computing provides many benefits for the data users such as on-demand service, convenient data access etc. Data security is a main disadvantage in cloud storage and transmission. This paper discusses various data security issues in cloud computing and the solution given by researchers to overcome those issues. This survey leads to further research to obtain maximum data protection.

REFERENCES

[1] Nareshvurukonda and B.ThirumalaRao, "A Study on Data Storage Security Issues in Cloud Computing", 2nd International Conference on Intelligent Computing, Communication & Convergence, 2016.

[2] R.VelumadhavaRao and K.Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", International Conference on Intelligent Computing, Communication & Convergence, 2015.

[3] Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", IJACSA International Journal of Advanced Computer Science and Applications, 2016, Vol. 7, Iss.4,pp.485-498.

[4] Ahmed Albugmi, Madini O. Alassafi and Robert Walters,Gary Wills, "Data Security in Cloud Computing", IEEE Fifth International Conference on Future Generation Communication Technologies, 2016, pp.55- 59.

[5] Dr.K.B.Priyalyer, Manisha R, Subhashree R and Vendhavalli K, "Analysis of Data Security in Cloud Computing", IEEE International Conference onAdvances in Electrical, Electronics, Information, Communication and Bio-Informatics,2016.

[6] [6]. Babitha.M.P and K.R.RemeshBabu, "Secure Cloud Storage Using AES Encryption", IEEE International Conference on Automatic Control and Dynamic Optimization Techniques, 2016,pp.859-864.

[7] AkshitaBhandari, Ashutosh Gupta and Debasis Das, "A Framework for Data Security and Storage in Cloud Computing", IEEE International Conference on Computational Techniques in Information and Communication Technologies,2016.

[8] MrinalKantiSarkar and Sanjay Kumar, "A Framework to Ensure Data Storage Security in Cloud Computing", IEEE Annual Ubiquitous Computing, & Mobile Communication Conference, 2016.

[9] G. PrabuKanna and V.Vasudevan, "Enhancing the security of user data using the Keyword Encryption and Hybrid cryptographic algorithm in cloud", IEEE International Conference on Electrical, Electronics and Optimization Techiques, 2016, pp.1-6.

[10] ShakeebaS.Khan and R.R.Tuteja, "Cloud Security using Multilevel encryption algorithms", International Journal of Advanced Research in Computer and Communication Engineering, 2016, Vol.5, Iss.1, pp.70-75.

[11] Dr.L.Arockiam and S.Monikandan, "A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage", IEEE International Journal of Engineering Research & Technology, 2016, Vol.3, Iss.12, pp.1053-1058.

[12] Geeta Sharma and SheetalKalra, "A Noval Scheme for Data Security in Cloud Computing using Quantum Cryptography", IEEE AICTC,2016.

[13] M.D. Boomija and S.V. Kasmir Raja, "Secure data sharing through Additive Similarity based ElGamal like Encryption", IEEE International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics,2016.

[14] S. Arul Oli and L. Arockiam, "A Novel Approach for Ensuring Data Confidentiality in Public Cloud Storage", IEEE International Journal of Computer Applications, 2014, pp.1- 5.

[15] Munwar Ali Zardari, Low Tang Jung and NordinZakaria, "K-NN Classifier for Data Confidentiality in Cloud Computing", IEEE International Conference on Computer and Information Sciences, 2014.

[16] Yuhong Liu, JungwooRyooand SyedRizvi, "Ensuring Data Confidentiality in Cloud Computing: An Encryption and Trust-based Solution", IEEE WOCC,2014.

[17] Khaled M. Khan and MahboobShaheen, "Empowering Users of Cloud Computing on Data Confidentiality", IEEE 3rd International Conference on Cloud Networking, 2014, pp.272-274.

[18] S.ArulOli and Dr.L. Arockiam, "Confidentiality Technique using Data Obfuscation to Enhance Security of Stored Data in Public Cloud Storage", IEEE International Journal of Advanced Research in Electronics and Communication Engineering, 2016, Vol.5, Iss.1, pp.169-174.

[19] MalekNajib Omar, MazleenaSalleh and MajidBakhtiari, "Biometric Encryption to Enhance Confidentiality in Cloud Computing", IEEE International Symposium on Biometrics and Security Technologies, 2014,pp.45-50.

[20] N.Jayapandian, Dr.A.M.J.Md.ZubairRahman and Rahman, "ImprovedCloud

[21] Security Trust on Client Side Data Encryption using HASBE and Blowfish", IEEE Online International Conference on Green Engineering and Technologies, 2016.

[22] [21]. Manjeet Singh, "Study on Cloud Computing and Cloud Database", IEEE International Conference on Computing, Communication and Automation, 2015, pp.708-713.

[23] [22]. A.VithyaVijayalakshimi, N.Veeraragavan and Dr.L.Arockiam "A Study on Cloud Data Security Issues", Research Journal Misbah, 2015, Vol.15, pp.15-25.

[24] [23]. Harshitha. K. Raj, "A Survey on Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, 2014, Vol.4, Iss.7, pp.352-357.

[25] [24]. S. Arul Oil, S. Monikandan and Dr.L.Arockiam "A Framework for Data Confidentiality in Public Cloud Storage", Research Journal Misbah, 2015, Vol.15, pp.8- 14.

[26] [25]. JasleenKaur, AnupmaSehrawat and NehaBishnoi, "Survey paper on Basics on Cloud Computing and Data Security", International Journal of Computer Science Trends and Technology (IJCST), 2014, Vol.2, Iss.3, pp. 16-19.