International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
60 – 62

ASIDSDCCE - A Survey on to Improve Data Security and Data Confidentiality in Cloud Computing Environment

Dr. Ramalingam Sugumar
Professor & Deputy Director,
Christhu Raj College, Panjapoor,Tiruchirappalli,
Tamil Nadu India
rsugusakthi1974@gmail.com

***Abstract*—** Cloud computing refers delivery of computing services such as servers, storage, databases, networking, software, analytics and so on. The several organizations providing these computing services are called cloud providers and typically charge for cloud computing services based on usage. The National Institute of Standards and Technology defines cloud computing by five essential characteristics, three service models, and four deployment models. The essential characteristics are on-demand self-service location-independent resource pooling, broad network access, rapid resource elasticity, and measured service. The main three service models are software as service, platform as a service, and infrastructure as a service. The aim of this survey is to improve the data security and data confidentiality through rectifying the problem in cloud computing environment.

Keywords- *Cloud computing, Data security, Data confidentiality, Issues.*

*****

I. Introduction

Cloud computing refers increasingly being adapted by a wide range of users beginning from commercial entities to consumers. A survey by Right Scale [1] found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes2, which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Alteration of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are:

(a) Honored User Access Management,
(b) Controlling Compliance,
(c) Data Setting,
(d) Data Separation,
(e) Data Shield and Recovery,
(f) Investigative Support,
(g) Long-term Viability.

Cryptography [2] refers a method of storing and disguising confidential data in a cryptic Form. However Cloud provides various facility and benefits but still it has some issues regarding safe access and storage of data. Several issues are there related to cloud security as: vendor lock-in, multi-tenancy, loss of control, service disruption, data loss etc.

II. Related Work

Pradeep et al. [3] proposed an ease of data or record sharing at will has compelled most of the physicians to adopt EHR (Electronic Health Record) for record-keeping of patients. It also makes convenient to the other stake holders of healthcare ecosystem such as nurses, specialists and patient. Due to lower costs and scalability of application, the cloud is becoming the infrastructure for most of the EHR but without comprising the privacy of data. Ravikumar et al. [4] discussed cloud computing must employ additional security measures apart from the traditional security checks to ensure that data is safe and no data breaches due to security vulnerabilities such as CIA Related Security Issues, AAC Related Security Issues, Broken Authentication, Session & Access Other Data Related Security Issues. Confidentiality, Integrity and Availability (CIA) losses can make a big impact in the business of the cloud computing because the data is the core component for any business. Data integrity is the assurance given to the digital information is uncorrupted and only be accessed by those authorized users.

Authentication and Access Control (AAC) is the process of verification and confirmation on user's identity to connect, to access and use the cloud resources. Other minor data related security issues can occur through Data location, Multi-tenancy and Backup in cloud computing. Security is

 ISSN: 2454-4248
60 – 62

major concern to the cloud computing. Manish et al. [5] focuses on storing data on the cloud in the encrypted format using fully homomorphic encryption. The data is stored in DynamoDB of Amazon Web Service (AWS) public cloud. User's computation is performed on encrypted data in public cloud. Fully Homomorphic Encryption (FHE) technique allows user to perform multiple types of operations on encrypted data. Only one kind of operation is allowed in a partially homomorphic encryption technique. Nabeel et al. [6] analyzed several threats and potential challenges in cloud computing. Some of the current threats are as follows:

1. Account or Service Hijacking
2. Data Scavenging
3. Data leakage
4. Denial of service
5. Customer Data manipulation
6. VM escape
7. VM Hopping
8. Malicious VM creation
9. Insecure VM migration
10. Sniffing/Spoofing virtual networks

They are identified 8 potential challenges to be faced in future of cloud computing which in lieu is going to affect its adoption as well. These challenges are as follows:

1. Eaves Dropping
2. Hypervisor viruses
3. Legal interception point
4. Virtual machine security
5. Trusted transaction
6. Smartphone data slinging
7. Insecure APIs
8. Shared technology vulnerabilities

Syed et al. [7] discussed different classifications of cloud security attacks targeting a specific cloud service or a particular kind of the cloud system. Thus there is a need for a more comprehensive classification of security attacks across versatile cloud services at each layer. They are proposes a multilevel classification of security attacks for different cloud services and their associated risks at cloud layers. It also discusses provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider. Haritha et al. [8] examined like manner propose two streamlining procedures for report look for, called the Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) count, to speed the interest time. Results show that EnDAS diminishes look time by and also orchestrate development.

The architecture the intrusion detection and prevention is performed automatically by defining rules for the major attacks and alert the system automatically. The major attacks/events includes vulnerabilities, cross site scripting (XSS), SQL injection, cookie poisoning, wrapping. Data deduplication technique allows the cloud users to manage their cloud storage space effectively by avoiding storage of repeated data's and save bandwidth. The data are finally stored in cloud server namely CloudMe. To ensure data confidentiality the data are stored in an encrypted type using Advanced Encryption Standard (AES) algorithm[9].

On the other hand security of the data in the cloud database server is the key area of concern in the acceptance of cloud. It requires a very high degree of privacy and authentication. To protect the data in cloud database server cryptography is one of the important methods. Cryptography provides various symmetric and asymmetric algorithms to secure the data. It presents the symmetric cryptographic algorithm named as AES (Advanced Encryption Standard). It is based on several substitutions, permutation and transformation[10]. A practical efficient revocable privacy-preserving public auditing scheme for cloud storage meeting the auditing requirement of large companies and organization's data transfer. The scheme is conceptually simple and is proven to be secure even when the cloud service provider conspires with revoked users.[11]

The paper is to survey recent research related to clouds security issues. Ensuring the security of cloud computing plays a major role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. Customers are wondering about attacks on the integrity and the availability of their data in the cloud from malicious insiders and outsiders, and from any collateral damage of cloud services. These issues are extremely significant but there is still much room for security research in cloud computing[12]. A secure cloud storage system for data storage and data forwarding functionality. partition the encrypted data and store them on storage server. It will keep the data secure during transmission and data at rest. It will be helping the user to send the data to cloud without hesitation of data being lost [13].

The different techniques along with few security challenges, advantages and also disadvantages. It also provides the analysis of data security issues and privacy protection affairs related to cloud computing by preventing data access from unauthorized users, managing sensitive data, providing accuracy and consistency of data stored.[14]

A novel secure cloud storage system to ensure the protection of organizations' data from the cloud provider, the third party auditor, and some users who may use their old accounts to access the data stored on the cloud. The system enhances the authentication level of security by using two authentication techniques; time-based one-time password (TOTP) for cloud users verification and automatic blocker protocol (ABP) to fully protect the system from unauthorized third party auditor. The experimental results demonstrate the effectiveness and efficiency of the proposed system when auditing shared data integrity[15]. Ramalingam et al. [16,17] discussed several load balancing algorithms and they are proposed a new framework for data security in cloud computing environment. They study deals with the framework for cloud data security mechanisms in cloud computing environment. The Security and confidentiality are major role in storing of data in that

location. Several researchers are work in that area. Cryptographic meethods are used to provide secure communication between the user and the cloud. This proposed work based on encryption and decryption algorithm for secure data storage in cloud computing environment.

III. Conclusion

In this article deals with several cloud computing security algorithms. The aim of those algorithms is to store the data in secure manner in cloud computing environment. The output of the previous algorithms are limited to give improved performance. Still there is plenty of space to improve the results to extract best service from cloud service providers and the user. The general issue and challenge for cloud computing is the data security and confidentiality of the cloud environment. Cloud services providers are now pointed for the proper security and privacy mechanisms which would make the cloud atmosphere secure and threatened place for their customers and they keep full faith on the cloud service provider.

References

[1]. Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", Procedia Computer Science pp.465-472, 2017.

[2]. Akashdeep Bhardwaja, "GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd, Security Algorithms for Cloud Computing", Procedia Computer Science 85 pp.535 – 542, 2016.

[3]. Pradeep Deshmukh, "Design of cloud security in the EHR for Indian healthcare services", Computer and Information Sciences 29, pp.281–287, 2017.

[4]. P. Ravi Kumar, P. Herbert Raj, P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing", Procedia Computer Science 125 pp.691–697, 2018.

[5]. Manish M Poteya, C A Dhoteb, Deepak H Sharmac, "Homomorphic Encryption for Security of Cloud Data", Procedia Computer Science 79 pp.175 – 181, 2016.

[6]. Nabeel Khana, Adil Al-Yasirib, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework", Procedia Computer Science 94 pp.485 – 490, 2016.

[7]. Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad, "Multilevel classification of security concerns in cloud computing", Applied Computing and Informatics 13, pp.57–65, 2017.

[8]. CH. Haritha, P. Praveen Kumar, "EnDAS. Efficient Encrypted Data Search as a Mobile Cloud Service", IJSRCSEIT | Volume 3 | Issue 1 pp.247-253, 2018.

[9]. R. Shobana, K. Shantha shalini, S. Leelavathy and V. Sridevi,"de-duplication of data in cloud", int. J. Chem. Sci.: 14(4), 2016, 2933-2938 Issn 0972-768x.

[10]. VishalR.Pancholi,Dr.BhadreshP.Patel,"Enhancement of Cloud Computing with secure data storage using AES",International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010

[11]. Xinpeng Zhang, Chunxiang Xu, Xiaojun Zhang, Taizong Gu and Guoping Liu, "Efficient Dynamic Integrity Verification for Big Data Supporting Users Revocability", information 2016, 7,31;doi:10.3390/info7020031, www.mdpi.com/journal/information.

[12]. K. Arul Marie Joycee, Dr. R. Sugumar," DSICCE: A Survey of Data Security Issues in Cloud Computing Environment", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.10, October- 2017.

[13]. Kadwe Yugandhara, Jadhav Ashwini, Pagar Pooja, Patil Suchita,Prof.J.S.Pawar,"Secure Data Storage and Forwarding in Cloud Using AES and HMAC", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056.

[14]. Jeevitha B. K., Thriveni J., Venugopal K. R., " Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey",International Journal of Computer Applications (0975 – 8887) Volume 156 – No 12, December 2016.

[15]. Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", El-Booz et al. EURASIP Journal on Information Security (2016) 2016:13.

[16]. Ramalingam Sugumar, "ASLBACC – A Study on Load Balancing Algorithms in Cloud Computing" IJCSMA, Vol.6 Issue. 3, March- 2018, pg. 1-5.

[17]. Ramalingam Sugumar, Arul Marie Joycee, "FEDSACE: A Framework for Enhanced user Data Security algorithms in Cloud Computing Environment", IJFRCSCE, Volume: 4 Issue: 3, pp.49-52, 2018.