Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 10, October 2017, pg.41 – 45

DSICCE: A Survey of Data Security Issues in Cloud Computing Environment

K. ARUL MARIE JOYCEE, Ph.D. Research Scholar,

ChristhuRaj College, Panjapoor, Tiruchirappalli, Tamil Nadu, India

joycedinesh@gmail.com

Dr. R. Sugumar, Professor & Deputy Director,

ChristhuRaj College, Panjapoor, Tiruchirappalli, Tamil Nadu, India

rsugusakthi1974@gmail.com

Abstract: Cloud computing is the well-known technology for scaling of extensive data and complex computation. Cloud computing has increased fast in many companies. Cloud computing offers many benefits in terms of low cost and accessibility of data. Increasing data volume is giving the bigger task of Data Centers (DCs) to provide a better quality of cloud computing. 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. This paper is to survey recent research related to clouds security issues

Keywords - Cloud computing, attack, integrity.

I-Introduction

An emerging computing model in the computer field is known as cloud computing and provides many advantages. Computing model has function of scalability for required cloud and the virtualized resources are used as service on internet. CC is conventional technology in networking field consisting of parallel computing, distributed computing, technologies of network storage, utility computing, load balance and virtualization etc. are combined with other different product.

CC functions on demand access of computing resource (configurable) by setting the software and hardware systems over data center. The green computing is the advanced version of cloud computing helps in high performance design, having efficiency in power consumption and with safe mode of operation. CC possesses three service delivery models (SDM), such as: [12]

Software as a service (SaaS): This allows users of cloud to access the provider's apps (PA) over the internet.
Platform as a Service (PaaS): This allows users to deploy their apps on platform development which service provider of cloud (SPC) provides.
Infrastructure as a Service (IaaS): allows users to rent, storage, processing of network capacity by SPC.

II- Related Work

Most of cloud services provided by cloud are non-trustable. Security vulnerability of online storage systems is one of the non trustable. To solve this problem a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. This scheme is able to support dynamic groups. These dynamic groups are generating a group signature and dynamic broadcast encryption techniques, any cloud user can share data with others securely. The main purpose of this scheme is securely using cloud services storing and sharing by multiple owner groups[1].

The different types of attacks on cloud data and also presents what are cryptography solutions are available to protect the data from the different attacks. Security is addressed by different parameters like authentication, authorization, confidentiality and integrity. Among this, ensuring confidentiality protects the data in cloud storage.[2]

Public auditing scheme which provides a complete outsourcing solution of data – not only the data itself, but also its integrity checking. Start from an overview of our public auditing system and discuss two straightforward schemes and their demerits. Then present the main scheme and show how to extent main scheme to support batch auditing for the TPA upon delegations from multiple users. Finally, discuss how to generalize privacy-preserving public auditing scheme and its support of data dynamics.[3]

The integrity auditing scheme which provides a complete outsourcing solution of data. After introducing notations considered and brief preliminaries, started from an overview of proposed data Integrity auditing scheme. Then, presenting main scheme and show how to extent the proposed scheme to support integrity auditing for the TPA upon delegations from multiple users. Finally, how to generalize integrity auditing keeping data privacy scheme and its support of dynamic data.[4]

Steganography has been considered to be a standard way of sending secret data to the receiver without others being able to identify its immediate presence. Cloud computing has been competitive in fields like cost reduction, flexibility and optimal resource utilization. there is an effort taken to embed Steganography and Cloud Computing, so that, the security level of both can hold together and create a greater safety standard. The pixels are inverted and sent to Five Modulus Method (FMM) or Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT) algorithm based on its size and complexity; the steganography image is then transmitted to the receiver using the SaaS infrastructure. Using the Software as a Service (SaaS) Document Management, the image is stored, and shared to the receiver, which reduces the extra steps of upload and download, sending via email or any other meaning of communication. SaaS is Cost-efficient, secure, and scalable. Hence an efficient usage of its security and resources to create a system that can handle them in Cloud without any necessity to download an application to the network.[5]

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.[6]

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[7]

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.[8]

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. [9]

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.[10]

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.[11]

III- Conclusion

Cloud computing is a combination of several key technologies that have evolved and matured over the years. The common issue and challenge for cloud computing is the security of the cloud environment, many different approaches and models have already been proposed by many researchers. Cloud services providers are now searching for the proper security and privacy mechanisms which would make the cloud atmosphere safe and protected place for their customers and they keep full faith on the cloud service provider. This paper surveys the various security mechanisms for data storage in cloud computing, techniques, benefits and drawbacks.

References

[1] Sawase Akanksha and B.M.Patil, "A Secure Multiowner Dynamic Groups Data Sharing In Cloud", International Journal of Advances in Engineering & Technology, Feb., 2016. ISSN: 22311963.

[2] Dr. S. S. Manikandasaran, "Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555,Vol.6, No1, Jan-Feb 2016.

[3] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE,Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage"

[4] Wale Amol D. ,Vedant Rastogi, " Data Integrity Auditing of Cloud Storage" International Journal of Computer Applications (0975 – 8887) Volume 133 – No.17, January 2016.

[5] Ihssan Alkadi, Sarah Robert, " Application and Implementation of Secure Hybrid Steganography Algorithm in Private Cloud Platform", journal of computer science applications and information technology, Received: October 12, 2016; Accepted: October 16, 2016; Published: January 20, 2017.

[6] 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.

[7] 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

[8] 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

[9] 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.

[10] 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.

[11] 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.

