Dr. Ramalingam Sugumar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 3, March- 2018, pg. 44-49 **ISSN: 2321-8363**
Impact Factor: 5.515

A Study on Enhancing Data Security in Cloud Computing Environment

Dr. Ramalingam Sugumar[1], K.Raja[2]
[1]Professor & Deputy Director, ChristhuRaj College, Panjapoor, Tiruchirappalli, Tamil Nadu India
E-mail: rsugusakthi1974@gmail.com
[2] Ph.D Scholar, ChristhuRaj College, Tiruchirappalli, Tamil Nadu, India
E-mail: porusrajak@gmail.com

Abstract

Cloud computing is an Internet-based computing model which provides several resources through Cloud Service Providers to Cloud Users on-demand basis without buying the underlying infrastructure and follows pay-per-use basis. Cloud computing usage has increased rapidly in many companies. Cloud computing is the well-known technology for scaling of extensive data and complex computation. Cloud computing offers many benefits in terms of low cost and accessibility of data. Data security is the major issue in cloud computing. This paper covers various security algorithms related to cloud computing and shows a comparative study on data security algorithms.

Keywords: Cloud computing, Scaling, Data security.

I- Introduction

Cloud computing has been envisioned as the next generation of distributed/utility computing. It is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. 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 deployment models include private cloud, public cloud, community cloud, and hybrid cloud. Nowadays, cloud-computing paradigm can offer any conceivable form of services, such as computational resources for high

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

performance computing applications, web services, social networking, and telecommunications services. In addition, cloud storage in data centers can be useful for users to store and access their data remotely anywhere anytime without any additional burden. However, the major problem of cloud data storage is security. Therefore, cloud data centers should have some mechanisms able to specify storage correctness and integrity of data stored on a cloud.

The rest of this paper is organized as follows. Section 2 Presents an overview of the related work. Section 3 the conclusion, and section 4 references. [1]

II- Related Work

DSCESEA - Technique to improve the classical encryption techniques by integrating substitution cipher and transposition cipher. DSCESEA used first stage the plain text is converted into corresponding ASCII code (Hexa) value of each alphabet, key value range between 1 to 256. The algorithm is used in order to encrypt the data of the user in the clouds. Users can store data on demand or for the applications without keeping any local copy of the data on there machine. Since the user has no control over the data after his session is logged out, the encryption key play the very important role and its primary authentication for the user. [2].

Most of cloud services provided by cloud are non turstable. 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[3].

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.[4]

This work is based an obfuscation technique to make stronger a numerical data in cloud storage. This obfuscation technique is used to encrypt and decrypt the numerical data. This

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

algorithm is an confidentiality system named as SUG-DO (SUGUMARDigits Obfuscation) to enhance the security of data in cloud environment. Windows azure as the implementation tool for this proposed algorithm. [5].

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.[6]

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.[7]

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.[8]

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

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]

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

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]

III- Conclusion

This study deals with various security algorithms. The ultimate purpose of those algorithms is to store the data in secure manner. The results of the previous algorithms are limited to give improved result. Still there is plenty of space to improve the results to extract best service from cloud service providers. The common issue and challenge for cloud computing is the security of the cloud environment, many different methods and models have already been proposed by many researchers. Cloud services providers are now pointed 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] 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", EURASIP Journal on Information Security (2016) 2016.

[2] Dr. R. Sugumar, K. Arul Marie Joycee,"DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm" International Journal of Engineering Research & Technology,Vol. 6 Issue 10, October – 2017.

[3] 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.

[4] 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.

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

[5] Dr. Ramalingam Sugumar , K.Arul Marie Joycee, "Ensure and Secure Data Confidentiality in Cloud Computing Environment using Data Obfuscation Technique", International Journal of Advanced Studies In Computer Science and Engineering , Volume 6, Issue 12 ,December 31 .2017.

[6] 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"

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

[8] 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.

[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.

©2018, IJCSMA All Rights Reserved, www.ijcsma.com