International Innovative Research Journal of Engineering and Technology

ISSN NO:2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

A Survey on Issues in Cloud Data Security

Dr.P.Maragathavalli[1], K.Suganthi[2], D.Pavithra[3], S.Rajathi[4], R.Sabitha[5]

[1]Assistant Professor/IT, Pondicherry Engineering College
[2]Student Member/IT, Pondicherry Engineering College

[1]marapriya@pec.edu,[2]suganthik@pec.edu,[3]pavithrad@pec.edu,[4]rajathis@pec.edu,[5]sabithar@pec.edu.

Abstract

Cloud consists of large number of servers. Tremendous amount of information is stored in cloud. There are several issues associated with cloud computing such as storage, scalability and security challenges like confidentiality, integrity and privacy. Ensuring security to the cloud data is an important issue. Considering the security and privacy within the cloud there are certain threats to the user's sensitive on cloud storage. While moving towards the concept of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability. This paper analyzes various security issues in cloud such as confidentiality, integrity, availability and authorization.

Keywords—Authentication, Cloud Computing, Data Security, Security Issues, Privacy.

I. Introduction

Cloud computing security is the set of control-based technologies and policies designed to adhere to protect information, data applications and infrastructure associated with cloud computing use. Because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider. Cloud computing security processes should address the security controls to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and data backup plan in the case of a cloud security breach. Cloud security encompasses a broad range of security constraints from an end-user and cloud provider's perspective, where the end-user will primarily will be concerned with the provider's security policy, how and where their data is stored and who has access to that data. For a cloud provider, on the other hand, cloud computer security issues can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policy. Cloud security is important because it is probably the biggest reason why organizations fear the cloud.

The best strategy for cloud vendor is to send only encrypted files to the cloud. Use the strongest encryption anything less is not worthwhile. We should not depend on the cloud provider or an intermediary to encrypt those files and decrypt them as well as rely on trust. With the cloud, all data and metadata should be encrypted at the edge, before it leaves. It does not matter that the clouds are managed by major, revered companies.

This paper seeks to identify and explore important security issues and challenges facing cloud computing, a now fairly mature technology, along with the methods employed in industry to combat these problems. In order to achieve this goal, we must first understand the concepts behind this technology, as well as its underlying infrastructure. In this paper we will analyze the security challenges such as confidentiality, integrity and privacy. The paper is organized as follows: Section II describes the literature review; Section III describes the conclusion and finally followed by references in Section IV.

II. LITERATURE SURVEY

SI. No.	AUTHORS	TITLE OF THE PAPER	JOURNAL / CONFERENCE NAME	TECHNIQUES OR METHODS USED	PARAMETERS CONSIDERED	DIS-ADVANTAGES
1	Joseph K. Liu, Kaitai Liang & Willy Susilo	Two-Factor Data Security Protection Mechanism for Cloud Storage System	IEEE Transactions on Computers , 2016	Identity Based and Public Key Encryption	Efficiency, Security	Does not enhances the confidentiality of data
2	Sulton Aldossary & William Allen	Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions	International Journal of Advanced Computer Science and Applications, 2016	Identity Based Encryption, Attribute Based Encryption, Public Based Encryption	Efficiency, Availability	Data vulnerability to internal and external threats
3	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, 2016	Public key cryptography	Authenticity	Insiders' attacks are very difficult to identify and also very tough to protect data
4	Yunchuan Sun & Junsheng Zhang	Data Security and Privacy in Cloud Computing	International Journal of Distributed Sensor Networks, 2014	Homomorphic encryption	Confidentiality	Reducing data storage
5	S.Balamurugan & S.Sathyanarayana	Enhanced Security as a Service to Protect Data in Public Cloud Storage	International Journal of Advanced Research in Computer and Communication Engineering, 2016	Security as a Service (SECaaS)	Efficiency, Security	Less interaction with users

In most of the papers mentioned above they used encryption techniques such as Identity Based Encryption (IBE), Public Key Encryption (PKE) and Attribute Based Encryption (ABE). The Identity Based Encryption is a public-key cryptosystem which is based only on valid public key. IBE solutions may rely on cryptographic techniques that are insecure against code breaking quantum computer attacks. The Private Key Generator (PKG) [1] generates private keys for users; it may decrypt and/or sign any message without authorization. This implies that IBE systems cannot be used for non-repudiation. The Public Key Encryption [2] can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key. Because of the computational complexity of asymmetric encryption, it is usually used only for small blocks of data and only protects what it's designed to protect. The Attribute Based Encryption [3] is a public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. ABE systems have few drawbacks such as non-efficiency and non-existence of attribute revocation mechanism. The above mentioned techniques concentrates on the data loss, storage maintenance and data interception. They can be improved by giving additional security to database and authentication issues so that the time can be utilized effectively. By giving additional security, parameters such as confidentiality, integrity and privacy can be improved.

III. CONCLUSION AND FUTURE WORK

Though cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces lot of security challenges. From this paper, we have gained an understanding of cloud computing and what it entails. Building on that understanding we proceeded to outline and examine the various security issues associated with the cloud data. In future, concrete standards for cloud computing security can be developed. To provide a secure data access in cloud environment, advanced encryption techniques can be used for storing and retrieving data from cloud. Also proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.

REFERENCES

[1] Sulton Aldossary and William Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions”, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, (2016), pp. 485-498.

[2] Joseph K. Liu, Kaitai Liang and Willi Susilo, “Two-Factor Data Security Protection Mechanism for Cloud Storage System”, IEEE Transactions on Computers, Vol. 65, No. 6, Jun 2016, pp.92-104.

[3] 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, No. 1, Feb 2016, pp.498-503.

[4] 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, Vol. 13, 2016, pp.1-13.

[5] Ramalingam Sugumar and Sharmila Banu Sheik Imam, “Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage”, Indian Journal of Science and Technology, Vol. 8, No. 23, DOI:10.17485/ijst/2015/v8i23/79210, Sep 2015, pp.1-5.

[6] R. Velumadhava Rao, K. Selvamani, “Data Security Challenges and its Solutions in Cloud Computing”, International Conference on Intelligent Computing, Communication and Convergence, Aug 2015, pp. 204-209.

[7] Aized Amin Soofi, M. Irfan Khan,Fazal-e-Amin, “A Review on Data Security in Cloud Computing”, International Journal of Computer Applications”, May 2014, pp.1-9.

Author Biography

Dr. P. Maragathavalli

She received her B.E. degree in CSE from Bharathidasan University, M.Tech. degree in CSE from Pondicherry University and Ph.D degree in CSE from Pondicherry University. She is working as Assistant Professor in the Department of Information Technology, Pondicherry Engineering College. She is a Life member of ISTE.

K. Suganthi

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

D. Pavithra

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

S. Rajathi

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

R. Sabitha

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.