Survey on Data Security in Cloud Environment

G. Suganya[1] and S. Arumugam[2]

[1]PG Scholar, Department of CSE, Nandha Engineering College (Autonomous), Erode, Tamil Nadu, India

[2]Professor, Department of CSE, Nandha Engineering College (Autonomous), Erode, Tamil Nadu, India

Email: suganyagme@gmail.com[1], arumugamdote@yahoo.co.in[2]

Received date: 10th December, 2017, Accepted Date: 25th December, 2017

Abstract - Cloud computing is a revolutionary technique that migrates current technology and computing concepts into utility-like solutions. Even though the advantages of cloud are distinct, security remains a top issue and influencing people's decisions around cloud. The uncertainty about how security at all levels, led information executives to state that security is their number one concern with cloud computing. This paper provides the comprehensive study of cloud security issues, various algorithms and encryption techniques used to ensure the data security in cloud environment.

Keywords - Cloud computing, Security, Techniques, Issues, Uncertainty

I. INTRODUCTION

Cloud computing has gained interest in various kinds of domains like business, education, research, market, publications etc. It is a technology which has shifted the cost of maintaining large servers which usually are under utilized to third party vendors. Due to this shift many small and medium level organizations deploy their application with just the usage cost(pay-as-you-go).Cloud computing offers three standard models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).The cloud deployment models are Private , Public and Hybrid.

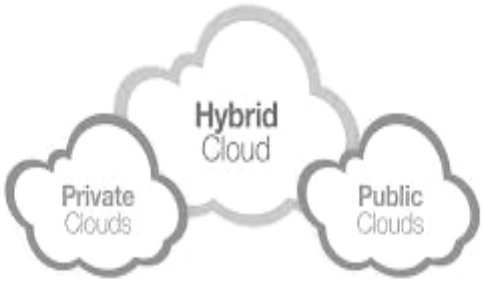

Fig. 1 Cloud Deployment Models

In cloud computing, an increasing number of enterprises and organizations use cloud servers as their system platform. It also has challenges that must be handled before coming to real time. The most captivating part of the cloud computing is the computation outsourcing. More likely, users want to control the privileges of data manipulation over other users or cloud servers. The reason behind this is when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users' control in most cases; other users might be able to infer sensitive information from the outsourced computation. The personal information is at risk since the person is authenticated based on his information in the access control. As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters.

Maintenance and control of the data in cloud is tedious task. The users should have trust on the cloud service providers that their data in cloud is free from breach and the services satisfy the compliance and regulatory measures. The security considerations must be addressed to make the cloud sustainable. This can be achieved by including real time security intelligence, securing the data, preventing threats and attacks. In a cloud environment, there are multiple complex data security challenges to be addressed which include the need to protect confidential data, adhering to regulations [11].

Although virtualization and cloud computing can help companies to break the physical bonds between an IT infrastructure and its users, security threats must be overcome in order to get more benefit fully from cloud computing paradigm. The various Cloud security threats are as follows:

A. Data breaches

Due to the huge amount of data stored on cloud servers, cloud service providers become an fascinating target. The severity of potential damage depends on the sensitivity of the data exposed. Data Breaches involving health information, trade secrets, and intellectual property.

B. Account Hijacking

Cloud services add a new dimension to the threat because attackers can eavesdrop on organization activities, manipulate transactions, and change data. Organizations should restrict the sharing of account credentials between users and services, as well as enable multifactor authentication schemes if available.

C. DoS Attack

Denial-of-service attack (DoS attack) is a an attack where the attacker seeks to make a machine or network resource unavailable temporarily or indefinitely disrupting services to users. Denial of service is typically accomplished by flooding the targeted machine with requests in an attempt to overload systems.

D. Cross Site Scripting (XSS)

Cross-site scripting (XSS) is a type of security vulnerability in web applications. XSS enables attackers to inject client-side scripts into web pages which can be viewed by other users. A cross-site scripting vulnerability is used by attackers to bypass access controls.

E. SQL Injection

SQL injection is a code injection technique in which depraved SQL statements are inserted into an entry field for execution. SQL injection must exploit security vulnerability in an application's software.

II. MATERIALS AND METHODS

The following literature survey shows the various techniques and algorithms which have been proposed to heighten the data security in cloud.

A. Achieving Flexible and Self-Contained Data Protection in Cloud Computing [1]

Self-contained data protection mechanism called RBAC-CPABE has been proposed by integrating role-based access control (RBAC) to provide an effective way for protecting outsourced data which is widely employed in enterprise systems, with the ciphertext-policy attribute-based encryption (CP-ABE). Data-centric RBAC (DC-RBAC) model that supports the specification of fine grained access policy for each data object to enhance RBAC's access control capabilities. DC-RBAC and CP-ABE by expressing DC-RBAC policies with the CP-ABE access tree and encrypt data using CP-ABE. Because CP-ABE enforces both access control and decryption, access authorization can be achieved by the data itself.

B. Multi-factor Authentication as a Service for Cloud Data Security [2]

To protect data access by unauthorized users, authentication plays an important role. Authentication is a first step for data security, through which user can establish proof of identities prior data access from system. Multi-Factor Authentication (MFA) scheme has been proposed which integrates more than one factors like knowledge, possession, location and time, for cloud user authentication. The architecture offers security as a service to cloud customers which can help to build trust to adopt cloud infrastructure without any fear to security threats.

C. An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique [3]

Mediated certificateless encryption which is an advanced encryption scheme that offers more security to the cloud data sharing and a steganographic method which enhances the security of data inside the cloud. Steganography approach reduces the falsification of unauthorized users. It provides explicit security to the public cloud. This method in the public cloud solves the key escrow problem as well as certificate revocation problem.

D. Division and Replication of Data in Cloud for Optimal Performance and Security [4]

Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) has been proposed that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

E. Towards Achieving Data Security with the Cloud Computing Adoption Framework [5]

The framework Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. CCAF explains the overview, rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. It

also demonstrated that CCAF multi-layered security can protect data in real-time and it has three layers of security: firewall and access control, identity management and intrusion prevention and convergent encryption.

F. Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption [6]

A semi anonymous privilege control scheme AnonyControl has been proposed to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity.

G. DNA Cryptography An New Approach to Secure Cloud Data [7]

Cryptography is a method in which we protect data or information and transmit it into an unreadable format. A new approach of cryptography that is DNA cryptography has been proposed. DNA can be used to store and transmit data. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, a five carbon sugar and a phosphate group. The nucleotides that make up these polymers are named after the nitrogen base that it consists of; Adenine (A), Cytosine (C), Guanine (G) and Thymine (T).

H. Two-Factor Data Security Protection Mechanism for Cloud Storage System [8]

Two-factor data security protection mechanism allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the Ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the Ciphertext without either piece.

I. An Efficient Fuzzy Self-Classifying Clustering based Framework for Cloud Security[9]

Fuzzy self-classifying clustering based cloud intrusion detection system which is intelligent to gain knowledge of fuzzy sets and fuzzy rules from data to detect intrusions in a cloud environment. The results of proposed approach are compared with other cloud intrusion detection systems based on K means, modified K means, and fuzzy self constructing clustering algorithms. Using each of these algorithms, the intrusion detection training dataset is partitioned into several clusters with similar patterns belonging to same cluster.

J. A Bio-Inspired Model to Provide Data Security in Cloud Storage [10]

The Bio-Inspired security model is an amalgamation of genetic algorithm and attribute based encryption. As per the methodology proposed the data need to be encrypted before being stored on the cloud. This way the cloud service provider is unaware of the data being stored and even if the data is compromised to some third party, there is no information leakage.

III. RESULTS AND DISCUSSION

The following table summarizes different algorithms are working on security parameters at some cases. Each algorithm focuses on improving different parts of cloud environment. The differences are shown in Table I.

TABLE I: DIFFERENT TECHNIQUES & IMPACTS

Sl.	Techniques and Algorithms	Impacts
1	Self-contained data protection mechanism called RBAC-CPABE by integrating role-based access control (RBAC)	Achieves more flexible and fine grained access control. Achieves efficient protection for outsourced data.
2	Multi-Factor Authentication (MFA)	Helps to build trust to adopt cloud infrastructure without any fear to security threats. Provides safe storage and access to cloud data.
3	Mediated certificateless encryption	This method in the public cloud solves the key escrow problem as well as certificate revocation problem.
4	DROPS Methodology	The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack.
5	CCAF multi-layered security	The CCAF multi-layered security can block 9,919 viruses and Trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated
6	Attribute-based encryption	Achieves not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information.
7	DNA cryptography	DNA cryptography secure the data. That will help to make a strong structure for security of data

8	IBE (Identity-based encryption)-based mechanism	Once the security device is stolen or lost, this device is revoked. which will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device.
9	Fuzzy Self-Classifying Clustering	Fuzzy self classifying clustering based CIDS achieves lower error ,less frequent intrusion cannot go undetected.
10	Bio inspired model	It takes less execution time thereby decreasing the latency and increasing the performance of cloud

IV. **CONCLUSION**

The utilization of cloud computing paradigm is continuously growing. Since security is the main concern in cloud computing. The security issues are classified into five categories namely security standards, network, access, cloud infrastructure, and data. The survey describes various security threats associated in cloud and the proposed techniques to enhance the data security. Security standards and techniques must be improved by focusing on various parameters for more secure cloud environment.

ACKNOWLEDGMENT

I am thankful for the timely and consistent cooperation given by my guide Dr. S. Arumugam for preparing this survey. I hope this survey will help to understand various kinds of cloud security threats and techniques available with the aspect of secure cloud platform.

REFERENCES

[1] Bo Lang, Jinmiao Wang and Yanxi Liu, Achieving Flexible and Self-Contained Data Protection in Cloud Computing , IEEE Access, Vol. 5, No. 7, pp. 1510-1523, 2017.

[2] Sajjan Rajani1, Vijay Ghorpade, Madhuri Dhange, Multi-factor Authentication as a Service for Cloud Data Security, International Journal of Computer Sciences and Engineering, Vol. 4, Special Issue - 4, pp. 43-46, 2016.

[3] Mohis M, Devipriya V S, An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique, International Conference on Inventive Computation Technologies (ICICT), DOI: 10.1109/INVENTIVE.2016.7830073, 2016.

[4] Mazhar Ali, Kashif Bilal,, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, Albert Y. Zomaya, DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security, IEEE Transactions on Cloud Computing, Vol. 99, 2015.

[5] Victor Chang and Muthu Ramachandran, Towards Achieving Data Security with the Cloud Computing Adoption Framework, IEEE Transactions on Services Computing, Vol. 9, No. 1, pp. 138-151, 2016

[6] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, pp. 190-199, 2015.

[7] Vinay Kumar and Ashutosh Kumar, DNA Cryptography An New Approach to Secure Cloud Data, International Journal of Scientific & Engineering Research, Vol. 7, No. 6, pp. 890-895, 2016.

[8] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Two-Factor Data Security Protection Mechanism for Cloud Storage System, IEEE Transactions on Computers, Vol. 65, No. 6, pp. 1992-2004, 2016.

[9] Sivakami Raja, Jaiganesh M, Saravanan Ramaiah, An Efficient Fuzzy Self-Classifying Clustering based Framework for Cloud Security, International Journal of Computational Intelligence Systems, Vol. 10, No. 1, pp. 495-506, 2017.

[10] N. Hitaswi and K. Chandrasekaran, A Bio-Inspired Model to Provide Data Security in Cloud Storage, International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds, DOI: 10.1109/INCITE.2016.7857617, 2016.

[11] S.Selvakumar and M. Mohanapriya, Securing Cloud Data in Transit using Data Masking Technique in Cloud Enabled Multi Tenant Software Service, Indian Journal of Science and Technology, Vol. 9, No. 20, pp. 1-5, May 2016.