ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

A Survey on Various Security Techniques to Secure Cloud Data

Shilpa M Yadawad[1], Gowramma B.H.[2]

Assistant Professor, Department of Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[1]

Assistant Professor, Department of Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[2]

ABSTRACT: Cloud computing is group of services such as storage, network, hardware and software which can be provided to user on pay –as- you –use basis. The security of data in the cloud is important, since the cloud applications data loss and leakage is very high these days. The data is accessible from anywhere at any time and it is important to make a secure cloud system so that confidentiality and integrity are to be achieved. In this paper we are discussing about the basic cloud computing services, data security issues that are faced by providers and customers and it also explores the different solutions to secure the data in cloud.

KEYWORDS: Cloud Computing, Data Security Issues, Different Data Security Solutions.

I. INTRODUCTION

Cloud computing hosts several services by sharing the processing resources, data for computing, virtual machines, storage and other services on demand basis. Its main intention is to provide affordable and scalable on-demand computing structure with superior quality of service levels. Cloud computing allows you to access all your documents and applications from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate. Cloud computing is internet dependent computing technology, but the Internet is not a place where providers can have complete control over it. Because of the security issues, cloud computing is not concerned with some users. As a virtual environment cloud computing has its special security threats which are completely different from threats in physical systems. in the complex multi-tiered applications, multiple parties such as customers, partners, and internal and external users will share the information inside the database. The security of all the data managed by these systems becomes crucial. Damage and misuse of sensitive data stored in the database not only affect a single user also affect entire organization. Various international and national organizations are developing and offering many cloud computing services but they have not properly considered the implications of accessing, processing and storing the data in a distributed shared environment. This paper focuses on different methods to secure the data in cloud data centres.

Paper is organized as follows. Section II describes cloud computing service models. Data types and data security challenges in cloud have been discussed in Section III. Section IV presents Different Data Security Techniques in cloud. Finally, Section V presents Conclusion.

II. RELATED WORK

While adopting data into the cloud the data security measuresare identified by many security challenges and how to handle thesechallenges. So many methods have been implemented to face these security challenges and to secure dataefficiently and effectively in cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

DeepanchakaravarthiPurushothama and Dr.SunithaAbburu[3] The main objectives of this paper are, to prevent data access from unauthorized access, itpropose a distributed scheme to provide security of the data in cloud which can be achieved by using homomorphismtoken with distributed verification of erasure-coded data. Proposed scheme perfectly stores the data and identifies any tamper at the cloud server and also performs tasks like data updating, deleting, appending. It also provides a process to avoid Collusion attacks ofserver modification by unauthorized users.
Mahima Joshi, Yudhveer Singh Moudgil[2] This paper consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. It describes, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve the goal.
D. Manivannan and R. Sujarani [1] This paper focuses on a security solution for protecting of data-at rest,specifically protecting the sensitive data that resides in databases by using TSFS algorithm with three keys thus providing more security for database. This algorithm improves the efficiency for executing the queries in database by encrypting only the sensitive data.
GoikarVandana T., JagdaleSupriya K., Parade Priya B., PawarSumedha D. [8] In this paper two technologies named Location-Based-Cryptography, Geo-Encryption Algorithm have been introduced. By using this technology security can be improved in cloud for data accessby providing a new method for a bank or any other particular location by using Location-Based Encryption.

III. ARCHITECTURE OF SERVICE MODELS

The architecture of service model includes three types of services.

- Software as a Service: SaaS is a complete operating environment for user interface, applications and program management. In the SaaS model, the application is provided to the client through a browser and the customer's responsibility begins with data entry and ends with data management and user interactions [8].Eg. GoogleApps, Virtual desktop.
- Platform as a Service (PaaS): This service provides a platform that enables software developers to develop websites without installing any software on the system. It provides virtual machines, operating systems, applications, development frameworks, transactions, and control structures[8].
  Eg. IBM, GoogleAppEngine, Force.com.
- Infrastructure as a Service (IaaS): This service provider manages all infrastructures and also supports various operations like Virtual storage,virtual machine, hardware, servers and networking. It includes the operating system, applications, and user interactions with the system [8].
  Eg.Servers, Network Devices.Fig. 1 shows the cloud computing service models.

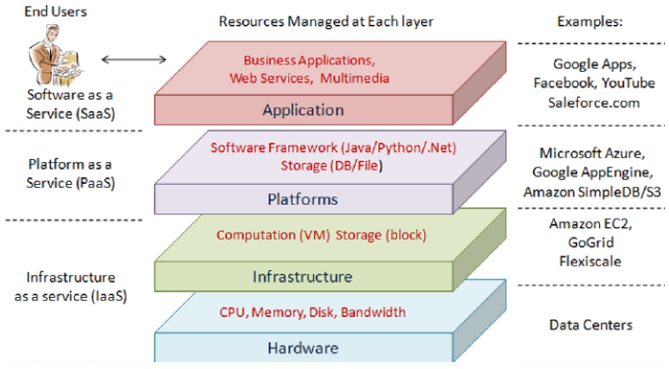

Fig 1: Cloud computing services Architecture.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

IV. DATA SECURITY IN CLOUD COMPUTING

Data security in cloud computing involves more than data encryption. Requirements for data security depend upon on the three service models SaaS, PaaS, and IaaS. Two states of data normally have threat to its security in clouds; Data at Rest and Data in Transit [10]. Fig. 2 Show the different types of data in cloud.

1. Data Types

i) Data at Rest

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data.Sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data [10].

ii) Data in Transit

Data in transit is the data which is moving in and out of the cloud. It can be in the form of a file or database stored on the cloud and can be requested for use at some other location. Whenever, data is uploaded to the cloud, the data at time of being uploaded is called data in transit. Data in transit can be very sensitive data such as user names and passwords and can be encrypted at times. However, data in unencrypted form is also data in transit. Data in transit is sometimes more exposed to risks than the data at rest as it has to travel from one location to another [10].

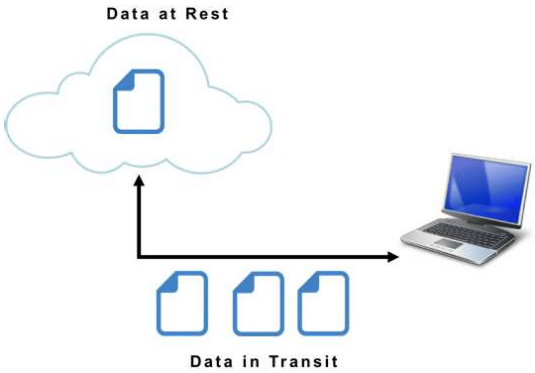

Fig 2: Data in rest and Data in Transit.

Confidentiality and Integrity of data is based upon the nature of data protection mechanisms, procedures and processes.

2. Data Security Challenges in Cloud

i) Account and provision stealing: Cloud Account hijacking is done by unauthorized users which deal with hackers gaining access to your account. It comes under the category of phishing, fraud, software victimization, manipulation of software vulnerabilities like buffer overflow attacks, etc. The major concerns in hijacking is illegal control of user account, influence of data, providing false and business harming responses to clients, and transmit customers to a wrong sites [11].

ii) Authentication mechanism: Authentication for the valid user or the system is the primary factor which is concerned in both the old and current standards. Cloud Service Provider request clients to accumulate their account details in the cloud and infinitely Cloud service provider have access to those data this leads to privacy issues. There are many copies of account will point to multiple authentication processes for all cloud service, the customer needs to switch their authentication mechanism which redundant actions ahead to abuse of the authentication mechanism[11].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

iii) Privileged user access: When vulnerable data is handled outside the enterprise, or by non-employees, it imply that organizational managers are less instantaneous aware of the nature and level of risk and that they have no direct facility to control these risks. It is exactly the case that reliable companies' employees are capable of creating mistakes. Privileged users cannot access all information at anytime or anywhere. Conventional methods for securing networks are inadequate for privileged users due to that powerful claim are lacking, it require rigid access control and management [11].

iv) Malicious attacks from management internally: Sometimes the architecture of cloud computing environments poses risks to the privacy and security of the customers. Although it happens rarely, this risk is very difficult to deal with. Examples include the administrators and managers of cloud service providers who can sometimes act as malicious agents and threaten the security of the clients using cloud computing applications [10].

v) Lock-in: Another hurdle is inadequate standards of data format, a lack of operating methods and shortage of tools which collectively cause compromised portability between the services and applications, even between service providers. Consequently, the customer has to be dependent wholly and solely on the vendor [10].

vi) Insecure or incomplete data deletion: In instances where clients request data to be deleted either partially or completely, this raises the question of whether it will be possible to delete the desired part of their data segment with accuracy. This makes it harder for the clients to subscribe to the services of the cloud-computing [10].

vii) Data interception: Unlike with tradition computing, the data in cloud computing is segmented and distributed in transit. This poses more threats due to the vulnerability and fragility of the computing technology and, in particular, sniffing and spoofing, third party attacks and reply attacks [10].

V. DATA SECURITY TECHNIQUES IN CLOUD

1.Data Storage Security by Token Correctness and Data Error Localization:

In cloud storage system, companies stores their data in the remotely located data server. Accordingly, correctness of the data is assured. Even though sometimes unauthorized person may modify or delete the data which leads to server compromise and/or random Byzantine failures. The cloud storage systems propose an effective and flexible distributed scheme with explicit dynamic data support for file distribution across cloud servers. By computing homomorphic token using universal hash function which can be perfectly integrated with the verification of erasure-coded data. As well as it identifies misbehaving servers. Finally, the procedure for file retrieval and error recovery based on erasure correcting code is outlined [3].

i) **Token correctness**: It achieves assurance for data storage correctness and data error localization, using pre-computed token.Before sharing file distribution using pre-computes a certain number of shortest verification token are generated that will ensure security for a block of data in a file in cloud storage. When the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. After getting assurance of the user it again asks for authentication by which the user is confirmed to be the authenticated user. Upon receiving assurance, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. All servers operate over the same subset of the indices, the requested response values for integrity check must also be a valid code word determined by a secret matrix. Suppose the user wants to challenge the cloud server's t times to make sure the correctness of data storage then he must pre-compute the verification tokens for each function, a challenge key and a master key are used. To generate the i^{th}token for server j, the user acts as follows.

The details of token Generations are shown in Algorithm 1[3].

- Derive an arbitrary value i and a permutation key based on master permutation key.
- Calculate the set of randomly-chosen index.
- Calculate the token using encoded file and the arbitrary value derived.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Algorithm 1 shows Token Pre-computation

Block of data is represented as l;
No. of .blocks is denoted as n;
Let f be the function and t be the token;
Index per proof is denoted as r;
Generate M k and C k ;
For point G (j); j->1, n execute
/*j server position*/
For round i->l ,t execute
/*i block index*/
Derive i = f (i) and k (i) from master key. Compute v(j)
End for
End for
Store all the vis locally.
End procedures

ii) Correctness Verification and Error Localization:Error localization is a key requirement for eradicating errors in storage systems. Error localization only provides binary results about the storage state across the distributed service in predecessors. The response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate potential data error(s). Specifically, the procedure of the i^{th} challenge response for a cross-check over the n servers is described as follows:

- The client reveals the i as well as the i^{th}key k (i) to each servers
- The server storing vector G aggregates those r rows
- Specified by index k(i) into a linear combination R
- Upon receiving R from all the servers, the user takes away values in R.
- Then the user verifies whether the received values remain a valid codeword determined by secret matrix.

Because all the servers operate over the same subset of indices, the linear aggregation of these r specified rows (R (1)i , . . . ,R(n)i) has to be a codeword in the encoded file matrix. If the above equation holds, the challenge is passed. Otherwise, it indicates that among those specified rows, there exist file block corruptions. Once the inconsistency among the storage has been successfully detected, we can rely on the pre-computed verification tokens to further determine where the potential data error(s) lies in. Note that each response R(j) i is computed exactly in the same way as token v(j) i , thus the user can simply find which server is misbehaving by verifying[3].

2) Cryptographic Storage Security

The core components of a cryptographic storage service can be implemented using a variety of techniques, some of which were developed specifically for cloud storage.

i) **Searchable Encryption**

At a high level, a searchable encryption scheme provides a way to encrypt a search index so that its contents are hidden except to a party that is given appropriate tokens. More precisely, consider a search index generated over a collection of files (this could be a full-text index or just a keyword index). Using a searchable encryption scheme, the index is encrypted in such a way that;

(1) Given a token for a keyword one can retrieve pointers to the encrypted files that contain the keyword.

(2) Without a token the contents of the index are hidden. In addition, the tokens can only be generated with knowledge of a secret key and the retrieval procedure reveals nothing about the files or the keywords except that the files contain a keyword in common [2].

- **Symmetric searchable encryption**

SSE is appropriate in any setting where the party that searches over the data is also the one who generates it. The security guarantees provided by SSE are, roughly speaking, the following:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

i)Without any tokens the server learns nothing about the data except its length.
ii) Given a token for a keyword w, the server learns which (encrypted) documents contain w without learning w. (Encrypted) documents contain w[2].

- **Asymmetric searchable encryption (ASE)**

ASE schemes are appropriate in any setting where the party searching over the data is different from the party that generates it.
The security guarantees provided by ASE are the following:
i) Without any tokens the server learns nothing about the data except its length.
ii) Given a token for a keyword w, the server learns which (encrypted) documents contain w [2].

- **Efficient ASE (ESE)**

ESE schemes are appropriate in any setting where the party that searches over the data is different from the party that generates it and where the keywords are hard to guess[2].

ii)Attribute-based Encryption

It allows the specification of a decryption policy to be associated with a cipher text. A user can then encrypt a message under a public key and a policy. Decryption will only work if the attributes associated with the decryption key match the policy used to encrypt the message. Attributes are qualities of a party that can be established through relevant credentials [2].

iii) Proofs of Storage

A proof of storage is a protocol executed between a client and a server with which the server can prove to the client that it did not tamper with its data. The client begins by encoding the data before storing it in the cloud. From that point on, whenever it wants to verify the integrity of the data it runs a proof of storage protocol with the server. The main benefits of a proof of storage are that (1) they can be executed an arbitrary number of times; and (2) the amount of information exchanged between the client and the server is extremely small and independent of the size of the data. Proofs of storage can be either privately or publicly verifiable. Privately verifiable proofs of storage only allow the client (i.e., the party that encoded the file) to verify the integrity of the data. With a publicly verifiable proof of storage, on the other hand, anyone that possesses the client's public key can verify the data's integrity [2].

3) Data Encryption Using TSFS Algorithm

TSFS (Transposition, Substitution, Folding, Shifting)[1] is an efficient light-weight data encryption algorithm, which is also symmetric - key block encipherment algorithm, for symmetric encryption. Same key is used for encryption and decryption and security is dependent on the length of the key. This technique uses three keys for the process of encryption and decryption. For providing effective and more security for the database these three keys are expanded into 12 sub keys by using the key Expansion Technique.

If user wants to encrypt private data that can be seen and altered only by user itself, a randomly generated working key will be used to encrypt the private data with a conventional encryption algorithm. After the data entered by the user immediately that data is encrypted by using the algorithm and the encrypted data is stored in the database. This algorithm is working for both numbers and characters and also it accept the alphanumeric data also (for example the account number is asdf40985490). if decimal point numbers are entered then that number is multiplied by 100 and then applied to the algorithm. Why we multiply by 100 means because for Indian Rupees the Pisa columns have only two integers so that for covert the decimal point numbers to normal numbers, we use this technique. After the algorithm encrypted the data and the data is divide by 100 then it stored in the database. Thus the decimal point number is stored in the same data type in the form of cipher text. The strength of this algorithm is it gives more security to data. Since the numbers of keys are more the key combination increases and makes the guessing of keys harder [1].

4) Security of Data in Cloud Using Location

In this technique Data Encryption and decryption algorithms are discussed with extra security layer which uses user's location and geographical position by Antispoof GPS system. It gives the location of the user for accessing data through latitude, longitude and altitude accurately. Label can be given to data which is stored on cloud and Index table

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

contains these labels and refers to users' geographic location and timeframe. Label and data stored on cloud can be added manually or automatically. This technique can be used to secure bank data stored on cloud [8].

Following are the steps for Geo-Encryption Algorithm:

1. Compute GeoLock by using recipientsPVT(Position, Velocity and TIME) information.
2. GeoLock is then XOR with the session key (Key_S) to form a GeoLocked session key.
3. Encrypt result by using asymmetric algorithm and send to receiver.
4. GeoLocks are computed using an AntiSpoof GPS receiver. 5. Compute PVT → GeoLock mapping function.
6. Check for PVT. If PVT values are correct then resultant geolock will XOR with GeoLocked key and we get session key.
7. Compute decryption by using resultant session key.

Following are the steps which are taken to get access the data on cloud:

1. First, user enters username and passwords. This username and password collectively called label. This client label is sent to cloud.
2. Searching for the similar label and retrieving it is done on cloud.
3. After that the information corresponding to the label will be retrieved (that information contains user location and timeframe within which data can be access.)
4. By using this information and geo-encryption algorithm encryption of data takes place. And this encrypted data is send to the user.
5. Users computer receives that encrypted data.
6. Anti-spoof GPS is used to measure the user's location and delivers the location to the user's computer.
7. Then calculate the geolock code by using the mapping table.
8. Geolock XOR Encrypted key=Session key.
9. And finally decryptsthe data by using this session key.

VI. CONCLUSION

Cloud computing is a marvellous technology which provides various services to the users. Data storage is one such service of cloud computing technology where users can store their data in a remote data centre. It is very important to provide security for data in cloud to avid unauthorized access and data leakage. Hence Data security is one of the key issues in cloud computing. This paper figure out different service models of cloud computing, numerous data security issues and also discusses various proposed technique in securing cloud data.

REFERENCES

[1] D. Manivannan and R. Sujarani, "Light Weight and Secure Database Encryption using TSFS Algorithm," Proceedings of the International Conference on Computing Communication and Networking Technologies, IEEE, 2010.
[2] Mahima Joshi, Yudhveer Singh Moudgil "Secure Cloud Storage" International Journal of Computer Science & Communication Networks, Vol. 1(2) , Oct-Nov 2011.
[3] DeepanchakaravarthiPurushothama and Dr.SunithaAbburu "An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No. 1, March 2012.
[4] Ahmed E. Youssef and ManalAlageel , "A Framework for Secure Cloud Computing," , International Journal of Computer Science Issues, Vol. 9, Issue 4, No. 3, July 2012.
[5] Sh. Ajoudanian and M. R. Ahmadi, "A Novel Data Security Model for Cloud Computing," International Journal ofEngineering and Technology, Vol.4, No.3, June2012.
[6] Nidal M. Turab, Anas Abu Taleband Shadi R. Masadeh, "Cloud Computing Challenges and Solutions," International Journal of Computer Networks & Communications, Vol.5, No.5, September 2013.
[7] Navia Jose, Clara Kanmani A, " Data Security Mode Enhancement in Cloud Environment," Journal of Computer Engineering Vol. 10, Issue 2 , March– April 2013
[8] Jeyachandran, A., & Poongodi, M. (2018). Securing Cloud information with the use of Bastion Algorithm to enhance Confidentiality and Protection. *International Journal of Pure and Applied Mathematics*, *118*(24).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

[9] GoikarVandana T. , JagdaleSupriya K., Parade Priya B., PawarSumedha D."Improve Security of Data Access in Cloud Computing using Location," International Journal of Computer Science and Mobile Computing, Vol.4, Issue.2, February-2015.

[10] JahangeerQadiree andMohdIlyasMaqbool, "Solutions of Cloud Computing Security Issues," International Journal of Computer Science Trends and Technology,Vol. 4, Issue 2, March - April 2016.

[11] Ahmed Albugmi, Madini O. Alassafi and Robert Walters, Gary Wills "Data Security in Cloud Computing" Fifth International Conference on Future Generation Communication Technologies(FGCT),2016

[12] G.ShanmugasundaramV.Aswini, G.Suganya "A Comprehensive Review On Cloud Computing Security" International Conference on Innovations in information Embedded and Communication Systems (ICIIECS), 2017