Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 1, January-2019

STUDY AND ANALYSIS OF DATA SECURITY CHALLENGES IN CLOUD COMPUTING

T.A.Mohanaprakash[1], CH.chandrasekhar[2], M.S.G. Chakravarthy[3], M.Karthik[4]

Associate professor, M.Tech., Computer Science Department, Panimalar Institute of Technology, Chennai. [1]

IV year Students of Computer Science Department, Panimalar Institute of Technology, Chennai.[2, 3, 4]

tamohanaprakash@gmail.com[1]

ABSTRACT-Cloud computing is the growing technology that offers the model for enabling on-demand network access for a pool of public, private computing resources through World Wide Web. These resources include sharing of network, server, storage space, applications and services under the multi-tenancy concept. The characteristics that changes the way of managing and delivering computing services, technologies, and solutions are on demand self-service, network access, pooling of resources, rapid elasticity and scalability. Virtualization is the main idea behind the cloud computing technology.

Keywords— Cloud computing, Data breach, Security services,Service providers

I. INTRODUCTION

Cloud Computing is an emergent field in the area of Computing which is used to maximize the application and computing capabilities without investing a lot of money on infrastructure Cloud computing services include features such as liability, adaptability, dependability, profitability These resources can be scaled in any direction to build the assignment execution **.**

It is fundamentally an internet based computing. Cloud computing is an applied approach and has the potential to experience and change the cost benefits to a less-priced environment. Security is the foremost factor to be focused while adapting to the cloud. The users maintain a lot of personal data confidentially in their computers .While they were using the cloud computing technology these data will be transferred from their computer to the cloud. Therefore the cloud storage should have efficient mechanisms to store these confidential data securely.

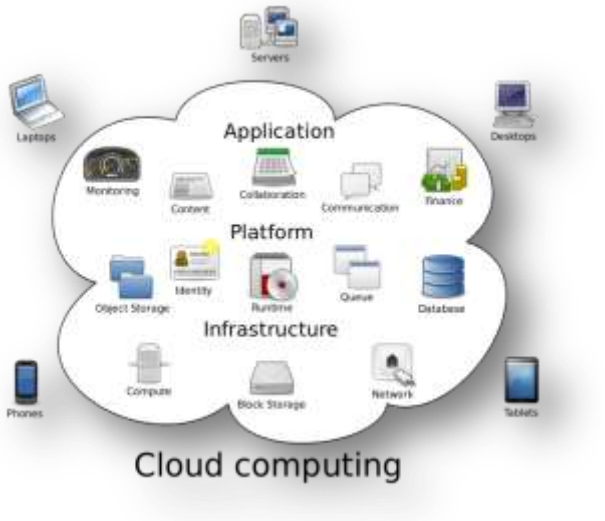

Figure no -1 System model of cloud Computing

II. OVERVIEW OF CLOUD COMPUTING

Cloud computing is a distributed network computing technology. It delivers infrastructure, programming and application as administrations to the client through the internet. The basic concept behind this is virtualization. The accommodation of these clients in a pool of servers is often referred to as Data servers.

Storing or sharing data in cloud environmentswould make data access easier, on-demand availability possible, at much lower cost with an enhanced collaboration capability, integration and analysis cheaper on a shared platform. There are many well-known service providers in the market, such as Google, Amazon, Yahoo, and Microsoft. There are also some vendors who provide cloud services in various deployment models and service models.

III.SECURITY ATTRIBUTE FOR CLOUD SERVICES

The invasion of cloud computing has transformed the way we make use of IT resources. The growth of the cloud service model has offered business-supporting technologies more competently than ever before.

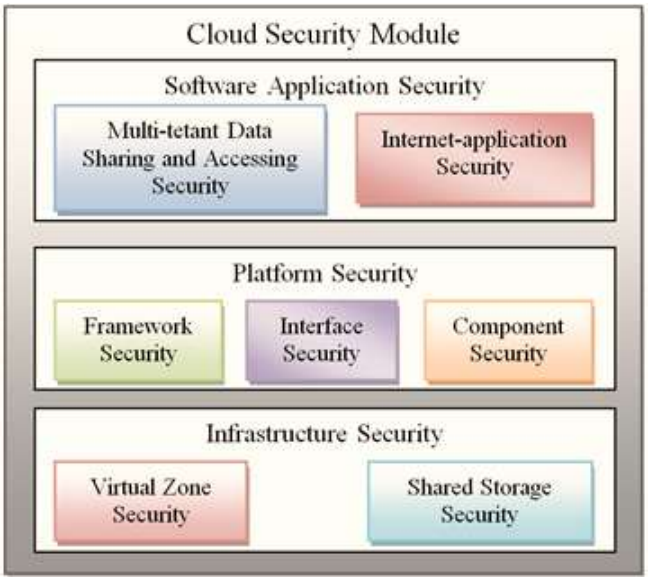

Figure no -2Security model of cloud Computing

Cloud computing has concurrently changed the functions in business and government, and as a result produced new security challenges. The CSA (Cloud Security Alliance) [2] has identified the top nine cloud computing threats for 2013. These threats are recognized as the major threats that can be possible in the modern cloud environment. These threats are as follows according to their rank of severity:

1. Data Breaches

The theory of data breach is that any malicious person or unauthorized person gets access into a corporate network and snip the sensitive and confidential or trustworthy data.

2. Data Loss

Another severe risk is the potential incapability to avoid data loss because the companies treat their data as a treasured asset.

3. Account Hijacking

In Account Hijacking a malicious interloper makes use of the stolen credentials of the user from cloud to seizure computing services and tries to peak into other's transactions, enclose fake information, and distract users to offensive web sites which have resulted in legitimate issues for cloud service providers.

4. Insecure APIs

If the Application Programming Interfaces used by the users to communicate with the cloud services are fragile or not sufficiently safeguarded, accidental or malicious attempt to encroach upon them may expose the data available in cloud to numerous security threats associated with inflexible access control, scalability and restricted monitoring and related issues.

5. Denial of Service

DoS has become a very serious threat in recent days this occurs because organizations and 24/7 services are indispensable. Temporary access to the data warehoused in the cloud to the authenticated users by attacking the server by sending thousands of request it become unable provide response to the regular users.

6. Malicious Insiders

A person who intervenes into the cloud network to damage the organizations confidential data and assets, harm valuable brands, penalize financial damage, stop yield is known as a malicious insider.

7. Abuse of Cloud Services

This threat is the prominent issue for service providers of cloud than consumers of cloud, but it has a key role in a number of serious consequences for those providers. It takes an attacker year's altogether to crack an encryption key using his own limited hardware, but by using an array of cloud servers, he might be able to hack it in minutes in the cloud services.

8. Insufficient Due Diligence

CSA's basic guidance for organizations is to make sure that they have sufficient resources to implement extensive due diligence before diving into the concepts of cloud. Due diligence denotes to the care of a sensible person must take before arriving into an agreement or a contract with another party.

9. Shared Technology Issues

Cloud computing is a sharing technology so it is very challenging to obtain a strong isolation property for an architecture that involves a multi-tenancy concept. It is the concern of the CSP to deliver a scalable service to the user without snooping with the other client system.

IV. SECURITY APPROACHES

In this section, we examine some innovative security approaches that are made use in cloud computing organizations against data breaches. The main problem is that in the presentation of the cloud; the cloud supplier has certain access or control over the information of the cloud client.

Information-centric security: For the ventures to administer data in the cloud, it is necessary to adopt a methodology for shielding the information from within. This approach is called data driven security. The procedure that involves the process of placing the knowledge inside information itself is the idea behind self-insurance. Data needs to act certainly depicting and ensuring, every aspects of its environment. When information checks its preparation and tries to reinvent a protected situation that is confirmed to be utilizing the structure of Trusted Computing (TC).

High-assurance remote server attestation:

In current situation, lack of transparency is keeping organizations from moving their information to the cloud. Information proprietors wish to have a look at how their information is being controlled and stored at the cloud, and to confirm that their information is not being mistreated or spilled, or possibly have an unrecoverable review trail when it happens at present in cloud organization. Currently, cloud suppliers are utilizing manual estimating methods like SAS-70 to fulfill the needs of their customers. The main deal of this issue depends on trusted computing. When a placed stock is in processing condition, a trusted screen is presented at the cloud server to monitor the activities of the cloud server. The trusted screen gives a proof or evidence of consistence to the proprietor who looks for the information, ensuring that specific approaches have not been violated. To assure the trustworthiness of the screen, secured bootstrapping of this screen keeps running next to the functioning framework and applications.

Privacy-enhanced business intelligence:

A diverse approach to control data involves the encryption of all cloud data. The difficulty with this approach is that encryption restricts use of data. Cryptographers have designed adaptable encryption suggestions that take into account the operations involved in encryption of text. The cryptographic primitives, for example, homomorphism encryption (Gentry, 2009) and private data recovery (PIR) (Chor et al., 1998) implement calculations on cipher text without decrypting it. When these cryptographic methods advance, they may open up new conceivable results and directions for research on the development of algorithms of cloud security.

Privacy and data protection:

Privacy is a main drawback in cloud computing environment. It needs to protect identity information, policy components and histories of transaction. By transferring workloads to a cloud infrastructure, personal and confidential information of the customer faces the risk of unauthorized access and may get exposed. All the solutions on the security of cloud must be embedded with mechanisms of privacy protection**.**

Homomorphic encryption:

This encryption scheme offers a mechanism to execute some specific type of computation on cipher-text which is impossible with any other encryption schemes. With the help of this technique, data can be stored in the cloud as cipher-text format by the cloud user. They can perform any necessary actions without decrypting the cipher-text.

Searchable/Structuredencryption: This technique uses encryption as the base. It gives assurance to the cloud users that cloud does not know or acknowledge the data and the computation involved in the data.

Proofs of storage:

It this approach CSP's and its clients come up with a service level agreement. It ensures the data stored in the servers would never be used by the CSP without the permission of client.

Server aided secure computation:

This security mechanism offers the user a server and rights to perform computation on the cipher text without revealing the insides of the original data.

Tools:

Tools comprises of data loss prevention systems, unusual behavior pattern detection tools, format conserving and encrypting tools, user behavior profiling, decoy technology, authentication and authorization technologies. These tools are capable of performing tasks such as detecting the traffic checking in real time, storing and making use of the data for future forensics, and tools can set trap to malicious activity into decoy documents to lessen the issues of data breach.

V.SECURITY CHALLENGES

There are varieties of challenges regarding to security being incurred in the cloud environment. Some are listed below:

Privileged User Access:

If any of the information that is confidential to the client is accessed by other unauthorizedusers then the new membership should be obtained from cloud service provider to access their credentials. If the membership is not obtained then the leakage of information will be increased. The owner of the data has full access rights but neither any of the users does not have any full control access.

MonitoringCompliance:

Cloud providers perform interioraudit to the cloud systems and procedures, but never allow forany external auditing processes. Cloud provider drops out the installation of new security certificates by the clients.

Investigative Support:

Ameticulous request regardingthe unlawfulpermit to the customer data in cloud computing is difficult and troublesome. The access which is unapproved is finished by either inside (internal client) or remotely (external client).

Figure no -3Security challenges of Cloud Computing

Data segregation:

In cloud computing, sharing is important facility which provides users to share their resources and data in a conserved mannersmore than one client can share the data in parallel with every other client.

Recovery:

If the server or the data farm utilized by the cloud provider isbeing floppedby the user andbecause of the specificdisasters or framework disappointments then it is the responsibility of the cloud provider to compromise the customers availing the data services that are being recovered.

VI. FRAMEWORK FOR THE POSSIBLE SOLUTION

Developing an actual model for security in cloud environment involves analyzing the risk associated with data that are being contracted out. The risk can be analyzed in the view of the all possible use rather exploitation of the data, because the reputation of the company can be exploited by misuse of the data. Therefore there should be some labeling of the data according to the risk associated with the data. Then the security model will turn consequently and give more importance to the important confidential data of the organization. The power of cloud computing is infinite and this great power can be used for various cyber related attacks.

There should be some mechanism that provides security both to the cloud clients and service providers. This can be achieved using the Service Level Agreement (SLA) terms, which is being treated as a contract between the Cloud providers and users. This agreement should include all the features of cloud services. Multi-tenancy is the distinguishing character of cloud environment that can make a severe data hazard as the same computing resources are being serviced among the different users. In the aim of achieving a safe and dependable multi-tenant model, separation among the resources are necessary. Restricting the data access and data segmentation is also one way of providing security to the cloud environment. Phishing attacks and in web leaking of data can be prevented from developing a dedicated cloud application. These dedicated applications will act according to the user‘s behavior.ie user’s account access and will find any breaches that may occur.

Account hijacking is one of the most severe security threats as the hijacker may get access to user credentials and user data from different cloud users. The mechanism to prevent this type of hijacking is the two factor authorization which identifies genuine cloud users and provides secure and stable environment. Trapping of attacker’s activity is done by using honeypot security technology which is also considered to be effective in detecting security breach in cloud.

If installed correctly, a honeypot can aid as an early-notice and act as an advanced security surveillance tool, thus lessening the risks from attacks on data of users.

VII.FUTURE RESEARCH DIRECTIONS

Since cloud is one of engaging technology for worthy businessalso, assumption, the analysts are prompted to take part in undertaking the serious issues of cloud security in prospective of data breaching among the cloud clients. There areenormous cloudsimulations proposed by researchers for data safety, data availability, data reliability,securing from misuse, security inspection and so on. We felt the needto characterize these security related researches and directions to motivate the researchers to ensure the security among the cloud environment.

The various research ideas are listed below:

1. Protect Critical Information

The highest priority should be given only to the user’s data which is confidential than focusing on other data. Moreexploration is required to guard the serious informationarrangement by evaluating the legal background andconcerning all laws from all sectors. From the view point of technical2017 International

Conference on circuits Power and Computing Technologies, various new methods are to be evaluated which pose a threat to the security of dangerous information infrastructure.

2.Third party authentication

The user privacy breach is the major security concern involved in the cloud computing. Toresolve the privacy problem, mechanisms have beendeveloped to protect the user data confidentiality and user demanding privacy. However, these mechanisms provide only user level privacycontrol, which can be enriched by providing security for data reliability. Third party authentication mechanism is the one which provides compact security organization for user privacy and data integrity.Future research work can be focused on third party authentication which ensures reliable infrastructure between cloud providers and cloud environment clients.

3. Regulation

Ventures have lost the substantial amount of user information due to data breaches. Various regulations are provided by the industries to prevent the data breaches. The industries have observed different measures, each with its own method for addressing security of the informationSomeprocesses can reducelosses due to data negotiation, but there is no suggestion thatan increase in processes would result in fewer negotiations.It has been verified that following the protocols can avoid data breaches for some extent. Further study is needed toinvestigate and develop guideline which will evade databreaches.

4.Socio-technical approach

The social features related to cloud computing needs to be investigated in such a way that it takes a well-adjusted method to cloud computing databreaches and integrates the end-user. So there is a need for investigation and balance thecollision between social, technical and environmental features enclosed in finding a feasible solution for security breaches.Security monitoring mechanisms can help to overcome databreaches and interrogate security issues. Establishments usevariety of security mechanisms to examine any distrustfulbehavior. e.g. Cloud Watch by Amazon. The development ofnew security features face differentimpediments due todifferent cloud environments used by cloud provider.Therefore there is a need to conduct investigation on the differentcomponents of the cloud and suggest a cross platform solution toprevent data breaches.

5.Service Level Agreement

The data breach risk will be altering based on securitySLAs as well as based on client's architectural resources needs. The prevailing modelscan be prolonged as additional observing tools becomeavailable. It permits a better assessmentamong variousmultiple cloudproviders, pertaining estimation by a user. More inquiry isrequired to detect good secure models which can aid user to select a cloudprovider with low mitigation of security risk.

6. Cryptographic Algorithms

Cryptography dependsonencryption and decryptionmethods of messaging using unique keys assigned to each unique user. The other cryptographic algorithms are also used in security mechanisms.Organizations prefer to implement ECC (Elliptic Curve Cryptography)over RSA algorithm for the protection of user data. However, ECCcannot be used in all possibilities. But it is more critical toselect the necessary cryptographic algorithms. Hence advanceresearch is promoted in this regard.

7. Scheduling Algorithms

Scheduling Algorithms of green IT is necessary and reliable to find the possibilityof giving appropriate systems to DIDS which stopovers the databreach challenges for dissimilar clouds that might be acaptivatinginvestigation area.

8. Mobile computing

The mobile platforms possesscircumscribed memory, speed of low processor and withhigher computational fundamentals makehindrance in the happenings to give best execution on thesephases. It is another exploration issue to investigate in preparing the frame work to induce the cloud infrastructure.

VII.CONCLUSION

Cloud computing delivers vast amount of advantages in data storing and access, where the aids outnumber the weaknesses. Preserving security and privacy in clouds became a foremost challenge and is often seen as weaknesses that hamper broad acceptance of cloud computing. Recently, security is turning out to be a predictable obligatory feature of a cloud computing environment.

Only if we could create security and privacy in clouds, we could endure to value from cloud services. In this paper, we have provided an indication of cloud computing and conversed its security challenges. We have also advised security patterns as a solution to challenge the challenges of cloud security.

In our discussions, we have explained on some important nontechnical features that make the cloud security engineering development very difficult. Therefore, we have presented a simple model for security patterns for cloud environments and well-defined the features of the security pattern system.

VIII. REFERENCES

[1] Chandan Prakash, Surajit Dasgupta. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016- "Cloud Computing Security Analysis: Challenges and Possible Solutions"

[2] R.Barona, E.A.Mary Anita. 2017 International Conference on circuits Power and Computing Technologies [ICCPCT]-"A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats"

[3] Komal Gandhi, Dr. Parul Gandhi. 2016 International Conference on Computing for Sustainable Global Development (INDIACom)-"2016 International Conference on Computing for Sustainable Global Development (INDIACom)"

[4] Priya Anand, Jungwoo Ryoo and Hyoungshick Kim-2015 First International Conference on Software Security and Assurance-"Addressing security challenges in cloud computing – a pattern-based approach"