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

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 10, October 2016**

# A Survey on Security Issues in Cloud Computing

D Ramesh[1], B Rama[2]

Research Scholar, Department of Computer Science, Kakatiya University, Warangal, Telangana, India[1]

Asst. Professor, Department of Computer Science, Kakatiya University, Warangal, Telangana, India[2]

**ABSTRACT:** Cloud computing is the pool of resources (hardware and software) that are delivered as a service over a network. Today, cloud computing generates a lot of publicity; it's both promising and frightening. Businesses see its potential with huge concerns. This Emerging computing paradigm offers attractive financial and technological advantages. Cloud services are very exciting and useful, but also have many open security issues and concerns such as information-security in-addition to that trust, expectations, regulations, and performance issues.
Research is currently being done on the different identified issues faced by cloud systems and possible solutions. However there is still a need for better solutions if cloud systems are to be widely adopted. The aim of this research is to examine the major security issues affecting Cloud Systems and the solutions available with the Study of clear and standard format for SLA (service level agreement) because that should not be fully formalized:, Data encryption is very expensive in the cloud computing, so that this methodology proposed some new experimental methods such as encryption techniques using hash function with cryptographic nonce number:, Without intervention of service provider encryption and decryption at sender side only:, about the storage-storage of data also in cipher text, without key it is meaning less for intruders and also providers.

**KEYWORDS:** Cloud computing- Security – Nonce Number-Hash Function.

## 1. INTRODUCTION

Security is considered one of the most crucial aspects in everyday computing, and it is no different for cloud computing due to the gentleness and importance of data stored in the cloud. Cloud computing infrastructures use modern technologies and services, most which have not been fully eva 8p;/luated in addition to security.
Cloud services are very interesting and useful, but have many open security issues. One issue with cloud computing is that the management of the data might not be fully accurate. The risk of malicious insiders in the cloud and the failing of cloud services have received a strong absorption by companies. Security is a troubling concern for cloud computing as shown in a Survey governed by the IDC enterprise panel which confirms that Security is the peak concern of cloud users. Cloud Security is one of the issues that need to be approached for allowing faster growth of cloud computing.

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

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 10, October 2016**

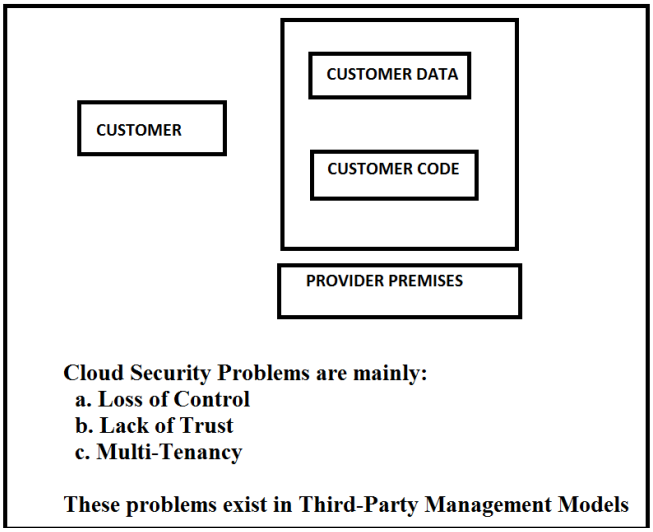


Fig.1: Security Problems in Cloud

Cloud Computing offers some incogitable benefits: unlimited storage, access to lightening quick processing power and the ability to easily share and process information. It have several issues, and most of them are security related. Cloud systems must overcome many risks before it becomes widely adopted, but it can be utilized right now with some adjustments and in the right conditions. People can enjoy the full benefits of cloud computing if we can address the very real security concerns that come along with storing sensitive information in databases scattered around the internet.

One of the main problems that need to be addressed is coming up with a clear and standardized format for the Service Level Agreement (SLA), that fully documents all of the services, what services and processes can be provided by the service provider to back up its assurances. When customers have the right level of expectations and the insecurities are esteemed manageable, cloud computing as a whole will gain ground and take hold as usable technology.

Another major issue of cloud computing is Encryption. Encryption is the main method of ensuring security of data stored in the cloud, but, encryption is computationally expensive. Encryption methods specific to DaaS (Cloud Databases) has been developed and more research is presently being done on Encryption mechanisms for cloud systems, more efficient methods are still needed to provide security in the cloud systems.

Security considerations relate to risk areas like external knowledge storage, dependency on the “public” web, lack of management, multi-tenancy and integration with internal security. Compared to ancient technologies, the cloud has several specific options, like its massive scale and therefore the incontrovertible fact that resources happiness to cloud suppliers is fully distributed, heterogeneous and all virtualized. Ancient security mechanisms like identity, authentication, and authorization are not any longer enough for clouds in their current type. Security controls in Cloud Computing are, for the foremost half, no completely different than security controls in any IT surroundings. However, as a result of the cloud service models used, the operational models, and therefore the technologies accustomed modify cloud services, Cloud Computing could gift completely different risks to a company than ancient IT solutions. Sadly, group action security into these solutions is usually perceived as creating them a lot of rigid.

Moving crucial applications and sensitive data to public cloud environments is of great concern for those organizations that are moving on over their data center’s network under their control. To mitigate these considerations, a cloud solution provider should make sure that customers can still have an equivalent security and privacy controls over their applications and services, give assurance proof to customers that their organization are secure and that they will meet their service-level agreements, which they will prove compliance to auditors

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

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 10, October 2016**

## II. RELATED WORK - SECURIITY ISSUES IN CLOUD COMPUTING

The main problems cloud computing faces are conserve confidentiality and integrity of data in aiding data security. The initial solution for these problems is encryption. Still encryption of data also raise new problems. Here is an analysis of some of the major problems faced by cloud systems and some respective solutions.

**a) Trust**

Today the major issue is Trust between the Service provider and the customer in the cloud computing. There is abstaining for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of internal attacks. The only legal document between the user and service provider is the Service Level Agreement (SLA). This document consists all the agreements between the user and the service provider; it contains what the service provider is doing and is willing to do [11]. Still there is currently no clear scheme for the SLA, and as such, there may be services not documented in the SLA.

**b) Legal Issues**

There are several regulatory requirements, privacy laws and data security laws that cloud systems need to be adhere. One of the major problem with adhering to the laws is that laws alter from country to country, and users have no control over where their data is physically located.

**c) Confidentiality**

The data privacy is additionally one in all the key considerations for Cloud computing. A privacy steering committee ought to even be created to assist create decisions associated with data privacy. Requirement: this may make sure that your organization is ready to satisfy the information privacy demands of its customers and regulators. Information within the cloud is sometimes globally distributed that raises considerations concerning jurisdiction, information exposure and privacy. Organizations stand a threat of not complying with government policies as would be explained further whereas the cloud vendors WHO expose sensitive info risk legal liability. Virtual co-tenancy of sensitive and non-sensitive information on identical host conjointly carries its own potential risks.

Confidentiality is preventing the abnormal disclosure of information. Preserving confidentiality is one of the major issues faced by cloud systems, since the information is stored at a remote location that the Service Provider has full access to it. Therefore, there has been some method required to achieve it.

## III. AUTHENTICITY (INTEGRITY AND COMPLETENESS)

Data corruption will happen at any level of storage and with any sort of media; therefore Integrity observation is important in cloud storage that is important for any information center. Data integrity is well achieved in a very standalone system with single information. Data integrity in such a system is maintained via database constraints and transactions. Transactions ought to follow ACID (atomicity, consistency, isolation and durability) properties to confirm information integrity. Most databases support ACID transactions and might preserve data integrity. Information generated by cloud computing services are unbroken within the clouds. Keeping data within the clouds means that users might lose control of their data and rely on cloud operators to accomplish access control.

Integrity is preventing the improper modification of information. Conserve Integrity, like confidentiality is another major issue faced by cloud systems that needs to be controlled, and is also mainly done by the use of data encryption. In a common database setup, there would be many users with wavering amount of rights. A user with a limited set of rights might need to access a subset of data, and might also want to confirm that the delivered results are valid and complete (that is, not poisoned, altered or missing anything) [11].

### *A. ENCRYPTİON*

Encryption could be a key technology for data security, understand data in motion and data at rest cryptography. Remember, security will range from straightforward (easy to manage, low value and quite honestly, not terribly secure) all the thanks to extremely secure (very advanced, costly to manage, and quite limiting in terms of access). You and therefore the provider of your Cloud computing solution have many selections and choices to

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

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 10, October 2016**

contemplate as an example, do the web services APIs that you simply use to access the cloud, either programmatically, or with clients written to those APIs, offer SSL cryptography for access, this can be usually thought-about to be a typical. Once the item arrives at the cloud, it's decrypted, and stored. Is there any choice to encrypt it before storing? Do you wish to fret regarding encryption before you transfer the file for cloud computing or do you like that the cloud computing service mechanically do it for you? These are choices, perceive your cloud computing answer and build your decisions based on desired levels of security.

A cryptographic hash function compresses arbitrarily long messages to digests of a short and fixed length. Most of extant hash functions are designed to evaluate a compression function with a finite discipline in a mode of operation, and the compression function itself is often designed from block ciphers or permutations. This modular design approach allows for ascetic security analysis via means of both cryptanalysis and provable security. We present a survey on the behavior of hash function security and modular design analysis. We concentrate on existing security models and definitions, as well as on the security aspects of designing secure compression functions (indirectly) from either block ciphers or permutations. In all of these directions, we identify open problems that, once solved, would allow for an increased confidence in the usage of cryptographic hash functions.

The main method used for ensuring data security in the cloud is by encryption. It seems like the perfect solution for ensuring data security, still, it is not without its defects. Encryption takes considerably more computational power, and this is multiplied by several factors in the case of databases [11]. Cryptography greatly affects database performance because each time a query is run, a huge amount of data must be decrypted and since the main operation on a database is running queries, the amount of decryption operations quickly become extravagant. There are several approaches developed to handle data encryption; each having its own compromises, some provide better security mechanisms, and some focus on facilitating more operations to the customers. Some of the methods are mentioned below:

### *B. EARLY APPROACHES*

Early approaches have used extensions to the query language that simply adopt encryption before writing to the database and adopt decryption before reading from the database.

### *C. QUERYİNG ENCRYPTED DATA*

There are several methods that were proposed to handle Querying of Encrypted Data, one such method was suggested by Purushothama B.R. and B.B. Amberker in [5].

In the proposed scheme, several cryptographic mechanisms were used to encrypt the data in each cell of each table to be stored in the cloud. When a customer needs to query this data, the query parameters are encrypted and checked against the stored data. No data decryption is done in the cloud, that protects the Authenticity and integrity of the information. When the results of the query is returned (in encrypted form) to the user, then the user decrypts the data and uses it. This scheme also has compelling improvements for select queries over previous related schemes.

### *D. KEY MANAGEMENT*

Since encryption is the main method used to arrange data security, naturally we would be faced with the problem of key management. The keys will not be stored in the cloud, therefore the customer must manage and control a key management system for any cryptographic method used [11]. For simple encryption schemas such as the “Early Approaches” described above, there might not be a problem since a single encryption and decryption key can be used for the entire system. However, atmost any real database requires a more complex system [11]. This simple system to manage keys might even have to take the form of a small database which would have to be a secure local database; which again, may defeat the purpose of moving the original database to the cloud.

### *E. DATA SPLİTTİNG*

Some of the methods have been developed that serve as alternatives to encryption. These methods are generally faster than encryption but have their own limitations.

Data Splitting was initially developed by Divyakant Agrawal and his colleagues. The idea is to divide the data over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

combine the separate data-sets to crack up the original. This method is extremely fast compared to encryption but it aquires at least two separate, but alike service providers.

### *F. MULTİ-CLOUDS DATABASE MODEL (MCDB)*

It is a method which uses multiple clouds and several other techniques to ensure data is split in across clouds in a manner that protects the data Confidentiality, Integrity and ensures Availability.
MCDB provides cloud with database storage in multi-clouds, this model does not conserve security in a single cloud; rather security and privacy of data will be conserved by applying multi-shares technique on multi-clouds. By doing so, it avoids the negative effects of single cloud, abate the security risks from malicious insiders in cloud computing environment and reduces the negative impact of encryption techniques [1].

### *G. MULTİ-TENANCY*

Cloud systems share computational resources, storage, services between multiple user applications (tenants) in order to achieve efficient utilization of resources while decreasing cost, this is ascribed as multi-tenancy, even though the sharing of resources violates the confidentiality of tenants' IT Assets. That implies unless there's a degree of isolation between these tenants, it is very difficult to keep an eye on the data streaming between different realms which make the multi-tenancy model insecure for adoption [2].

### *H. VİRTUAL MACHİNE ATTACKS*

Generally in a cloud, business data and applications are stored and run within virtual machines. These virtual machines(VMs) are usually running on a server with other VMs, some of these can be malicious. Research has shown that attacks against, with and between VMs are possible.

### *I. SHARED RESOURCES*

Assuming the cloud system isn't running on a VM, the hardware is now an issue. Research has shown that it is possible for information to flow between processor cores, which means that an application running on one core of a processor can get access the information of another application running on other. Applications can also pass data between cores.

## IV. RESEARCH CHALLENGES IN CLOUD COMPUTING

Cloud computing analysis addresses the challenges of meeting the necessities of next generation non-public, public and hybrid cloud computing architectures, conjointly the challenges of permitting applications and development platforms to require advantage of the benefits of cloud computing. The research on cloud computing continues to be at an early stage. Several existing problems haven't been totally addressed, whereas new challenges keep rising from industry applications. Some of the difficult research problems in cloud computing are given below.

1. Service Level Agreements (SLA's)
2. Cloud data Management & Security
3. Access Controls
4. Reliability & availability of Service

### *A. SERVİCE LEVEL AGREEMENTS (SLA'S)*

Cloud is organized by service level agreements that permit many instances of one application to be replicated on multiple servers if need arises; addicted to a priority scheme, the cloud could minimize or close up a lower level application. A giant challenge for the Cloud customers is to judge SLAs of Cloud vendors. Most vendors produce SLAs to form a defensive shield against action, whereas providing marginal assurances to customers. So, there are some vital problems, e.g., data protection, outages, and price structures that require to be taken under consideration by the customers ahead signing a contract with a provider. The specification of SLAs can better replicate the customers' desires if they address the specified problems at the correct time. Number of essential queries associated with SLA are time period i.e. are they planning to be up 99.9% of the time or 99.99% of the time? And additionally how will that distinction appulse your ability to conduct the business? Is there any SLA related to backup, archive, or preservation of

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

information. If the service account becomes indolent then do they keep user data? If yes then however long? Thus it's a vital research area in cloud computing.

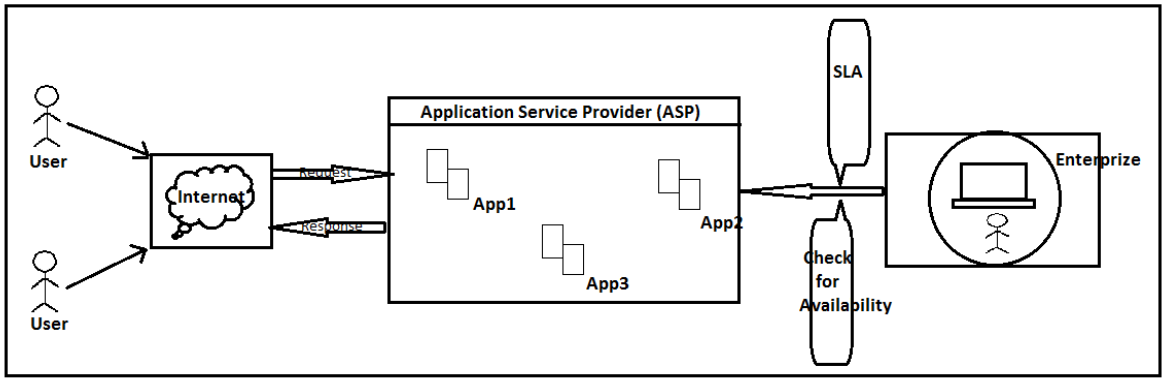


Fig.2 SLA Management in Cloud Computing

Fig2 Enterprises developed the web applications and deployed on the infrastructure of the Third-Party Providers. These Providers get the require hardware and make it available for application hosting. It necessitated the enterprizes to enter into a Legal Agreement with the Infrastructure Service Providers to guarantee a minimum quality of service (QoS).

***B. CLOUD DATA MANAGEMENT***

Cloud data will be terribly massive (e.g. text-based or scientific applications), disorganized or semi-organized, and usually append-only with rare updates Cloud data management is a esteemed research topic in cloud computing. Since service providers usually don't have access to the physical security system of data centers, they need to admit the infrastructure provider to achieve full data security. Even for a virtual non-public cloud, the service provider will solely specify the security setting remotely, without knowing whether or not it's totally implemented. The infrastructure provider, during this context, should attain the objectives like confidentiality, irritability. Confidentiality, for secure data access and transfer, and irritability, for attesting whether security setting of applications has been altered or not. Confidentiality is typically achieved using cryptographic protocols, whereas irritability will be achieved using remote attestation techniques. However, in an exceedingly virtualized setting just like the clouds, VMs will dynamically migrate from one location to another; thus directly using remote attestation isn't ample. During this case, it's crucial to create trust mechanisms at each architectural layer of the cloud. Software package frameworks like Map Reduce and its numerous implementations like Hadoop are designed for distributed processing of data-intensive tasks, these frameworks usually operate Internet-scale file systems like GFS and HDFS. These file systems are totally different from traditional distributed file systems in their storage format, access pattern and application programming interface. Specifically, they do not implement the standard POSIX interface, and so introduce compatibility problems with legacy file systems and applications. Many research efforts have studied this drawback

*C.* ***ACCESS CONTROLS***

Authentication and identity management is additional vital than ever. And, it's not extremely all that completely different. What level of password strength and change frequency will the service provider invoke? What's the recovery methodology for password and account name? How are passwords conveyed to users upon a change? What about logs and therefore the ability to audit access? this can be not all that totally different from however you secure your internal systems and data, and it works the same means, if you employ robust passwords, modified off times, with typical IT security processes, you'll shield that component of access.

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

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 10, October 2016**

### *D. RELİABİLİTY & AVAİLABİLİTY OF SERVİCE*

The challenge of reliability comes into the image once a cloud provider delivers on-demand software as a service. The software package has to have a responsibility quality issue so users will access it below any network conditions (such as throughout slow network connections). There are some cases known due to the irresponsibleness of on-demand software package. One of the examples is Apple's Mobile 'I' cloud service that stores and synchronizes information across multiple devices. It began with a distracting start when several users weren't ready to access mail and synchronize information properly. To avoid such issues, providers are turning to technologies like Google Gears, Adobe AIR, and Curl, which permits cloud -based applications to run locally, some even permit them to run within the absence of a network connection. These tools allow net applications access to the storage and process capabilities of the desktop, forming a bridge between the clouds and therefore the users own laptop. Considering the employment of software package like 3D play applications and video conferencing systems, reliability continues to be a challenge to attain for an IT answer that's based on cloud computing.

## V. CONCLUSION

One of the most important security worries with the cloud computing model is that the sharing of resources. Cloud service providers got to inform their customers on the extent of security that they provide on their cloud. In this paper, we tend to first discuss models of cloud computing, security problems and analysis challenges in cloud computing. Data security is main issue for Cloud Computing. There are many alternative security challenges as well as security aspects of network and virtualization. This paper has highlighted of these problems with cloud computing. We tend to believe that thanks to the complexity of the cloud, it'll be troublesome to attain end-to-end security. New security techniques got to be developed and older security techniques required to be radically tweaked to be ready to work with the clouds design. Because the development of cloud computing technology continues to be at an early stage, we hope our work can offer a higher understanding of the look challenges of cloud computing, and pave the means for any analysis during this area.

## REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C, Kramer D, Karl W, "Scientific Cloud Computing: Early Definition and Experience", 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.
[3] R. L Grossman, "The Case for Cloud Computing", IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.
[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing", Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.
[6] AlZain, M., Soh, B, & Pardede, E. " A New Approach Using Redundancy Technique to Improve Security in Cloud Computing". IEEE. 2012.
[7] Behl, A., & Behl, K. "An Analysis of Cloud Computing Issues". IEEE, 109-114, 2012.
[8] Bracci, F, Corradi, A., & Foschini, L, " Database Security Management for Healthcare SaaS in the Amazon AWS cloud". IEEE, 2012.
[9] Wang, J., Zhao, Y, Jiang, S, & Le, J. " Providing Privacy Preserving in Cloud Computing". IEEE ICTM, 213-216, 2009.
[10] Purushothama. B & Amberker, B. "Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation". 2013.
[11] Weis, J, & Alves-Foss, J. "Securing Database as a Service. IEEE Security and Privacy", 49-55, 2011.
[12] Wikimedia (2016, September 14)," Data as a Service", Retrieved from Wikipedia: http://en.wikipedia.org/wiki/DaaS.