DATA SECURITY IN CLOUD COMPUTING

R.SANGEETHA,
M.M.E.S WOMEN'S ARTS AND SCIENCE COLLEGE,
MELVISHRAM.

M.SILAMBARASI,
M.M.E.S WOMEN'S ARTS AND SCIENCE COLLEGE,
MELVISHARAM.

ABSTRACT

Cloud computing is a model which enables widespread access to a shared pool of resources including the characteristics of scalability, virtualization and many others. The most important service offered by cloud is storage wherein the users store the required data. Security is a concern here as the data is stored on remote server with multi user capabilities. The data is at the risk of unauthorized access thereby reducing reliability and privacy.

The key issue in cloud regarding security is the openness of the host or service providers. A gateway to the hacker is being provided when a test environment is set on a cloud. Cloud allows exchange of information among its services which requires standards. This development of standards is tough due to the interoperability issues. An intruder can provide malicious threat to the cloud data.

The developments of standards are still a concern in security of the cloud. Though there is increasing research done to enhance the security, new issue arises, or the security method becomes inappropriate for the scalable services. Program clustering and slicing for user efficiencies is difficult for the same reason.
To enhance the issues of cloud security such as

- **Data privacy.**
- **Data integrity.**
- **Prevent unauthorized access to the cloud.**
- **Managing interoperability.**

Keywords- Data security, Privacy protection, Cloud Computing.

I. INTRODUCTION

The Cloud computing will be the most important in Internet of Services, and Computer infrastructure. Both applications and resources are delivered to the Internet as services only on demand in the cloud computing environment. Cloud Computing is cost-effective, very flexible, and it provides delivery platform to either business or consumer IT services over the Internet. Cloud Computing is not considered as application oriented but service oriented. There are two basic types of functions in Cloud computing. They are **Computing** and **Data Storage**.

Computing security is one that is more important to be addressed nowadays. A major concern in adaptation of cloud for data is security and privacy. C**loud security** refers to a broad set of policies, technologies, and controls deployed to protect

information security. Security

securityMELVISHARAM., and, more broadly,

data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network concerns associated with cloud computing

fall into two broad categories: security issues faced by cloud providers (The organizations providing **software, platform, or infrastructure as a service** via the cloud) and security issues faced by their customers (companies or organizations Who host applications or store data on the cloud).

Data security framework for cloud computing networks is proposed [5]. Younis and Kifayat give a survey on secure cloud computing for critical infrastructure [6]. The privacy will be used to study about the tangible threats, and the intangible threats, some issues in data security was privacy of data, protecting the data, availability of data, etc.

The various challenges in the security was loss of data, data threats and malicious attacks from outsiders [7]. By using the cloud security techniques, and the data segregation Chen and Zhao [8] analyzed and presented the issues in the cloud computing environment through the data privacy and security. The most challenging issue in cloud computing is **Data Sharing.**

II. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

Several risks, and security concerns are associated with cloud computing and its data. However, this study will discuss the virtualization, storage in public cloud and multitenancy which are related to the data security in cloud computing [3].

A. Virtualization

Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully. A special function called hypervisor is required to run a guest operating system as a virtual machine in a host operating system [5,10].

Virtualization is a foundational element of cloud computing which help in delivering the core values of cloud computing. However, virtualization poses some risks to data in cloud computing. One possible risk is compromising a hypervisor itself. A hypervisor can become a primary target if it is

vulnerable. If a hypervisor is compromised, the whole system can be compromised and hence the data [11].

Another risk with virtualization is associated with allocation and re-allocation of resources. If VM operation data is written to memory, and it is not cleared before reallocation of memory to the next VM, then there is a potential for data exposure to the next VM which might be undesirable [12].

A solution to above mention issues are a better planning for the use of virtualization. Resources should be carefully used, and data must be properly authenticated before re-allocating the resources.

B. Storage in Public Cloud

Storing data in a public cloud is another security concern in cloud computing. Normally clouds implement centralized storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud [13]. To avoid such risks, it is always recommended having a private cloud if possible, for extremely sensitive data.

C. Multitenancy

Shared access or multitenancy is also considered as one of the major risks to data in cloud computing [14]. Since multiple users are using the same shared computing resources as CPU, Storage and memory etc. it is threat to not only a single user but multiple users.

In such scenarios there is always a risk of private data accidentally leaking to other users. Multitenancy exploits can be exceptionally risky because one fault in the system can allow another user or hacker to access all other data [15]. These types of issues that can be taken care of by wisely authenticating the users before they can have access to the data. Several authentication techniques are in used to avoid multitenancy issues in cloud computing [16].

.

III. SECURITY MODELS IN CLOUD COMPUTING

1. Security of Cloud Implementation Models

Basically, the deployment of a cloud is managed in the house (Private Cloud) or over a third-party location (Public Cloud). While, for various reasons, it is deployed as an integrated private-public cloud (Hybrid Cloud). A "Community Cloud" is a fourth type of cloud implementation models, where the infrastructure spreads over several organizations and is accessed by a specific community. The different cloud implementation models.

In **private cloud** configuration an organization may have control over its infrastructure or delegate that to a third party, being physically on-site or off-site. Securing the in-house cloud infrastructure is controllable and requires no need for extra trust mechanisms.

Public cloud implementation is a model in which a service provider, third-party, offers public services on pay-per-use manner. Some benefits of this model are the economies of scale, ability to have short-term usage and greater resources Utilization secure use of the shared public cloud is more challenging compared to private clouds. For that, public cloud suits more incidentals or less vulnerable applications.

With the **hybrid cloud model,** it is possible to integrate the different implementation models while having an adequate balance, and enabling portability of data and services. Though, vulnerabilities are reduced in hybrid clouds, threats still possible over integration points between the different cloud model.

2. Security of Service Delivery Models

Cloud service providers mainly offer three deliveries that are the **SaaS, PaaS, and IaaS**, alternatively called provision and distribution models.

IaaS layer provides the primary infrastructure of the cloud as service to the customers. Infrastructure is the main hardware components and their management software that includes servers, network, storage, file system, and operating systems. Securing the IaaS layer is divided into two main areas, the virtual environment, and the physical environment. Several security requirements need to be present at the virtual level, which includes controlling the access, data encryption, secure communication channels, and virtual protection. On the other hand regarding physical components, it is required to ensure the hardware reliability and preventing physical intrusion.

PaaS is the application deployment level, where developers are supposed to develop their applications and implement them. Though, some authors consider PaaS and IaaS to be at the same layer rather than two. A platform usually enables utilizing development platform, databases and middleware's. Meanwhile, platform providers currently enable a limited number of specific development languages and API's. The security requirements for PaaS are almost the same as those for the IaaS and both share the virtual environment characteristics. The differences in the security measures, if any, are related to the components' level or the role of the service user, a developer or system administrator for instance.

SaaS is usually accessed over the internet by the end users (tenants) as employees, managers, clients, and auditors.

IV. CLOUD SECURITY CONTROLS

Cloud security control is a set of controls that enable cloud architecture to provide protection against any vulnerability and mitigate or reduce the effect of a malicious attack. It is a broad term that consists of the all measures, practices, and guidelines that must be implemented to protect a cloud computing environment. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories:

A. Deterrent controls

These controls are intended to reduce attacks on a cloud system. Don't protect the cloud architecture or infrastructure but serve as warning to a potential perpetrator of an attack.

B. Preventive controls

These Controls are used for managing, strengthening and protecting the vulnerabilities within a cloud. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

C. Detective controls

Detective control is an accounting term that refers to a type of internal **control** intended to find problems within a company's processes. **Detective control** may be employed in accordance with many goals, such as quality **control**, fraud prevention, and legal compliance.

D. Corrective controls

These controls are designed to correct errors or risks and prevent the recurrence of further errors. They begin when undesirable outcomes are detected and keep the "spotlight" on the problem until management can solve the problem or correct the defect.

V. DATA SECURITY AND PRIVACY

Data security in cloud computing involves more than data encryption. Requirements for data security depends 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** which means the data stored in the cloud, and **Data in Transit** which means data that is moving in and out of the cloud.

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

Data Integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen. Data integrity is easily achieved in a standalone system with a single database.

Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions should follow ACID (Atomicity, Consistency, Isolation, and Durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access an authenticated user should have to secure resources controlled by the system.

Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS.

Data confidentiality is important for users to store their private, or confidential data in the cloud. Authentication, and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness. Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly.

The most significant matter is the exposure of data in above mentioned two states.

A. 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. As mentioned earlier, 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. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

B. Data in Transit

Data in transit normally refers to data which are moving in and out of the cloud. This data 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 on the time of being uploaded is called data in transit. Data in transit can be very sensitive data like usernames and passwords, and can be encrypted at times. However, data in unencrypted form is also data in transit [17].

Data in transit is sometimes more exposed to risk than the data at rest because it must travel from one location to another. (See Fig 1). There are several ways in which intermediary software can eavesdrop the data and sometimes can change the data on its way to the destination. To protect data in transit, one of the best strategies is encryption.

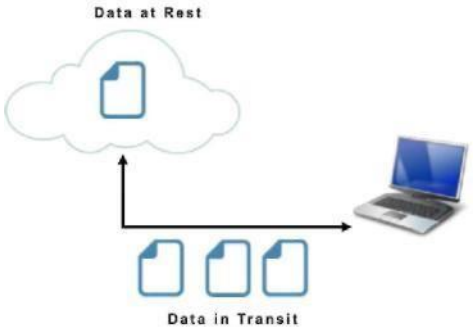

Fig 1: Data at Rest and in Transit.

VI. MANAGING CLOUD SECURITY

There are five basic premises to quantify and manage cloud security.

1) Network Segmentation

Consider a strong zone approach to keep instances, containers, applications, and full systems isolated from each other when possible. This will stop lateral movement in an attack and inappropriate access between systems by any threat actor.

2) Cloud-based Access Controls

All aspects of computing in the cloud should have access control lists. Since services like a database can be instantiated separately, it is more important than it is for one premise to define and implement proper access controls. This includes any virtual infrastructure, operating systems, applications, and even tools used to monitor the environment. The least privilege, or fully closed, security model is a preferred approach. Additionally, just because it is in the cloud does not mean that it should be publicly addressable. Only expose the resources you need to the Internet (if any) and secure the rest.

3) Multi-tenancy in Cloud Computing

While multi-tenancy provides scalability, and segmentation benefits by design, there are also chances of data bleed and irregular boundaries (like reporting or data export) that might not be controllable in the cloud. Consider access controls in a multi-tenant environment and policy boundaries for any account that may have access across tenants.

4) Cloud Access Management

Remember, these are not your computers. Concepts like a crash cart do not necessarily apply. So, you need to manage privileged access to all cloud resources and consider disaster recovery and any failures in your privileged access scope. We manage privileges today on premise with password management solutions and administrator accounts. We need the same concepts in the cloud but do not want cloud administrator rights to be everywhere. This would negate the previous concepts of zones and access control lists. Privileges need to be role based, appropriately delegated, and monitored for usage to ensure the access is appropriate.

5) Cloud Computing Threats and Vulnerabilities

This concept translates one for one from one premise implementations, but may use agents and another integration technologies to determine the premise of vulnerabilities. Once identified, they need to be prioritized using threated intelligence and remediated in a timely fashion. This is old school low hanging fruit that regardless of the computing environment must be done like clockwork to ensure good cyber security hygiene.

VII. PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit can be different. For examples, encryption keys for data in transit can be short-lived, whereas for data at rest, keys can be retained for longer periods of time.

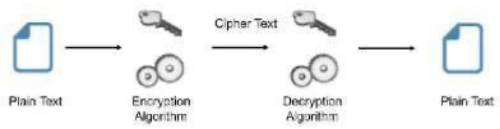

Fig 2: Basic Cryptography Process

Different Cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring contented integrity, authentication, and

availability. In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key as illustrated in Fig 2.

Normally there are four basic uses of cryptography:

A. Block Ciphers

A block cipher is an algorithm for encrypting data (to produce cipher text) in which a Cryptographic key and algorithm are applied to a block of data instead of per bit at a time [27].

In this technique, it is made sure that similar blocks of text do not get encrypted the same way in a message. Normally, the cipher text from the previous encrypted block is applied to the next block in a series.

As illustrated in Fig 3, the plain text is divided into the blocks of data, often 64 bits. These blocks of data are then encrypted using an encryption key to produce a cipher text.

B. Stream Ciphers

This technique of encrypting data is also called state cipher since it depends upon the current state of cipher. In this technique, each bit is encrypted instead of blocks of data. An encryption key and an algorithm is applied to each and every bit, one at a time [28].

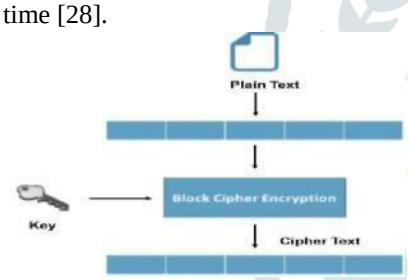

Fig 3: Block Cipher Mechanism

Performance of Stream ciphers is normally faster than block ciphers because of their low hardware complexity. However, this technique can be vulnerable to serious security problems if not used properly.

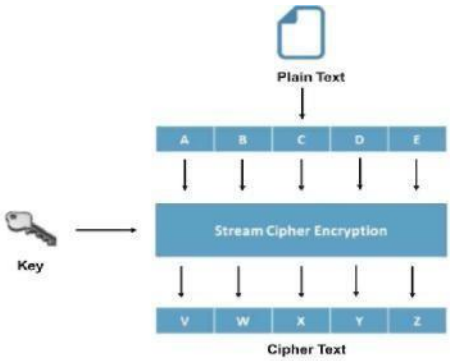

Fig 4: Stream Cipher Mechanism

As illustrated in Fig 4, stream cipher uses an encryption key to encrypt each bit instead of block of text. The resultant cipher text is a stream of encrypted bits that can be later decrypted using decryption key to produce the original plain text.

C. Hash Functions

In this technique, a mathematical function called a hash function is used to convert an input text into an alphanumeric string. Normally the produced alphanumeric string is fixed in size. This technique makes sure that no two strings can have same alphanumeric string as an output. Even if the input strings are slightly different from each other, there is a possibility of great difference between the output string produced through them.

This hash function can be a very simple mathematical function like the one shown in equation (1) or very complex.

$$F(x) = x \bmod 10 \quad (1)$$

Fig 5, below shows the mechanism of hash function cryptography.

All these above-mentioned methods and techniques are widely used in encrypting the data in the cloud to ensure data security. Use of these techniques varies from one scenario to another. Whichever technique is used, it is highly recommended ensuring the security of data in both private and public clouds.

VIII. CONCLUSION

Everyone wants to use the cloud for cost savings and for new

Fig 5: Cryptographic Hash Function Mechanism

business models. But for cloud security, it is very important to understand the different threats that come into play, **sa**ys Derek Tumulak. Cloud is a promising technology for the future IT applications. The main requirement of an organization was reducing data storage and processing cost. The analysis of data and information are the most important tasks in all organizations to make the decisions. So, they will not be transferred by organization to the cloud till there is a trust between the cloud

service providers and consumers. One of the major concerns of this paper was data security and its threats, and solutions in cloud computing. Data in different states have been discussed along with the techniques which are efficient for encrypting the data in the cloud. The study provided an overview of block cipher, stream cipher and hash function which are used for encrypting the data in the cloud whether it is at rest or in transit.

REFERENCES

[1] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology, pp. 285– 295, Springer, Berlin, Germany, 2014.

[2]Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.

[3] R. Velumadhava Raoa,, K. Selvamanib, "Data Security Challenges and Its Solutions in Cloud Computing" in proceedings of the
International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India .

[4] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," in Proceedings of the International Conference on Advanced in
Control Engineering and Information Science(CEIS '11), pp. 2852–2856, chn, August 2011.

[5] A. Pandey, R. M. Tugnayat, and A. K. Tiwari, "Data Security Framework for Cloud Computing Networks," International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178– 181, 2013.

[6] M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.

[7] A. Behl, "Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation," in Proceedings of the World Congress on Information and Communication
Technologies (WICT '11), pp. 217–222, IEEE, 978-1-46739745-2 © 2016 IEEE.

[8] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol.1, pp. 647–651, Hangzhou, China, March 2012.

[9] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in Proceedings of the ACM Workshop on Cloud Computing Security (CCSW '09), pp. 43–53, November 2009.

[10] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms,"Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978.

[11] M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multi-clouds to ensure security in cloud computing," in Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11), pp. 784–791, 2011.

[12] C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data," in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.

[13] S. Kardaş, S. Çelik, M. A. Bingöl, and A. Levi, "A new security and privacy framework for RFID in cloud computing," in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13), Bristol , UK, 2013.

[14] C. Delettre, K. Boudaoud, and M. Riveill, Cloud computing, security and data concealment," in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11), pp. 424–431 Kerkyra, Greece, July 2011.

[15]Towards Analyzing Data Security Risks in Cloud Computing Environments by Amit Sangroya, Saurabh Kumar, Jaideep Dhok,

Vasudeva Varma in Conference on Information Systems, Technology, and Management Bangkok, Thailand, September 2010.

[16]E. Stefanov, M. van Dijk, E. Shi et al., "Path oram:an extremely simple oblivious ram protocol," in Proceedings of the ACM SIGSAC
Conference on Computer & Communications Security, pp. 299– 310, ACM, 2013.

[17]Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud computing system based on trusted computing platform," in Proceedings of the International Conference on Intelligent Computation
Technology and Automation (ICICTA '10), vol.1, pp. 942–945, IEEE,May 2010.

[18]F.Yahya, V.Chang,, J.Walters, and B.Wills, "Security challenges in Cloud Storage," pp. 1–6, 2014.

[19]A. Squicciarini, S. Sundareswaran, and D. Lin,
"Preventing information leakage from indexing in the cloud," in Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD '10), pp. 188– 195, July 2010.

[20]Rahul Reddy Nadikattu, "FUNDAMENTAL APPLICATIONS OF MACHINE LEARNING ACROSS THE GLOBE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.31-40, January 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133453.pdf

[21]Sikender Mohsienuddin Mohammad, "IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf

[22]Rahul Reddy Nadikattu. 2017. The Supremacy of Artificial intelligence and Neural Networks. International Journal of Creative Research Thoughts, Volume 5, Issue 1, 950-954.

[23]Sikender Mohsienuddin Mohammad, "DEVOPS AUTOMATION AND AGILE METHODOLOGY ", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.946-949, August-2017, Available at :http://www.ijcrt.org/papers/IJCRT1133441.pdf

[24]K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp.