RESEARCH ARTICLE OPEN ACCESS

Identification and Analysis of Network Security Risks in Cloud Computing

Sahil Kundu [1], Anirban Bhar[2]

[1]B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
Email: kundubabita991@gmail.com

[2]Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata,India.
Email:anirban.bhar@nit.ac.in

--************************----------------------------------

Abstract:

Cloud Computing is an internet-based resource sharing technology which triggers broad networking sectors. However, over the recent times the advanced programs of cloud computing can also be done in small as well as medium scale sectors. This technology delivers a new model of information and services by means of an existing gris computing technology. In simple words we can say that Cloud Computing is the delivery of computing services such as storage, databases, networking, software, analytics and intelligence over the internet to offer faster innovation and flexible resources. Cloud Computing services provide a vast range of options from basics of storage, networking to natural language processing and AI as well as standard office applications. Apart from this cloud computing offers cloud platforms for customers to create and use web-oriented services. The hardware and software resource sharing are possible in cloud and it is managed and maintained by a third-party cloud service provider. Nowadays cloud computing has become an important and popular Research areas in the field of Computer Science. In the field of cloud computing, there are a lot of open research questions. Some of the most demanded Research topics are: Big Data, DevOps, Cloud Cryptography and cloud load balancing. In this paper, we will discuss on the cloud security issues in various aspects. All tiers of SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS are used in the study (Infrastructure as a Service).

Keywords **—Cloud Computing, Artificial Intelligence (AI), Cloud Security, Cloud Cryptography, Cloud load Balancing**

--************************----------------------------------

I. INTRODUCTION

Cloud computing is a technology which delivers a new model form existing grid technology and is basically based on internet resources sharing and broad networking access. Among all the definitions, the most relevant one is, “a network solution for providing inexpensive, reliable, easy, and simple access to IT resources”. The most important topic or we can say “the hot topic” on cloud computing is the data security and privacy. Many Researches are going on to improve the security of the data in a cloud as the rate of cyber-crime has emerged drastically in the recent years. It is very important for the cloud services to ensure the data integrity, privacy and protection. For this reason, many service providers are using different ways that depend upon nature, type and size of the data. One of the key questions asked while using cloud for storing data is whether to use a third-party cloud service or create an internal organization cloud because sometimes the data is too sensitive to store in public cloud like national security data, security intelligence data or highly confidential data.

Several issues are there related to cloud computing like: vendor lock-in, multi-tenancy, loss of control, service disruption, data loss etc. Cloud services have experienced numerous security incidents in recent years, such as the massive document leak from Google in March 2009, the 22-hour outage of the Microsoft Azure platform in April 2011, and the disruptions to Amazon's EC2 service in April 2011 that had an impact on Quora and Reddit, among other services. The security issues must therefore be resolved. In this we are going to study security techniques used for protecting and securing data, and different types of attacks and techniques to secure cloud model.

II. Previous Work

Several resources have been reviewed in order to comprehend the fundamentals of cloud computing and keeping data securely on the cloud. This part offers a survey of the literature to lay the groundwork for talking about various data security issues. In the literature, a few approaches have been put forth for dealing with security concerns in businesses using cloud computing.

- Popovi and Hocenski discussed the security concerns, conditions, and difficulties that cloud service providers (CSP) must deal with in cloud engineering [1]:

1. Security issues list the challenges that arose with cloud computing implementation.
2. Security standards offer several security templates that cloud service providers must use. A standard for developing new business models is the Open Visualization Format (OVF), which enables a corporation to offer a product on-site, on-demand, or in a hybrid deployment strategy.

- Countermeasures (such as antivirus software and intrusion detection systems) created to lessen well-known security concerns were discussed by Maggi and Zanero [2]. The emphasis is mostly on anomaly-based techniques, which are better suitable for contemporary security technologies than intrusion detectors.
- Subhashini and Kavitha addressed the security risks that the cloud computing faced [3]. They offered practical proof of security risks and problems that came up when service delivery models were implemented in an organisation. The cloud-based service models were created, and empirical validation was done in order to support the environment's safety.
- Bhaduria and Sanyal performs a survey in cloud computing to identify security flaws and issues, and he lists few typical sorts of attacks [4]:

1. A denial-of-service attack prohibits a legitimate user from accessing resources by the attacker.
2. Insider attacks with malicious intent: In this kind of attack, the perpetrator is an insider. Passwords, encryption keys, and other sensitive user data are all readily accessible to this person.
3. Cross virtual machine side channel attacks: These are attacks in which the attacker gains access to the target virtual machine's private data while being on the same physical hardware as it.
4. Attacks that target shared memory: The attacker and the user's shared memory is exploited to carry out unlawful, undesirable actions.

They suggested a technique for automatically identifying these attacks, and they examined its efficacy by simulating attacks in a genuine, live cloud environment. They claim that machine learning models served as the foundation for this model's construction. A support vector machine (SVM) is able to detect the majority of attacks among the models that are taken into account.

- Hu and A. Klein provided a standard to secure data-in-transit in the cloud [5]. For protecting data during migration, a baseline for encryption has been discussed. Robust security necessitates further encryption, but doing so requires additional computing. The benchmark they presented in their work shows equilibrium for the overhead associated with security and encryption.
- Tjoa, A.M. and Huemer examine the privacy issue by preserving data control to the end user to surge confidence [6]. A number of Cloud computing attacks are reviewed, and various countermeasures are suggested.

- Abdelkader and Etriby suggest a cloud architecture-based data security approach for cloud computing. They also developed software to enrich the effort in Data Security model for cloud computing further [7].

III. Risks and Security Concerns in Cloud Computing

A variety of cloud services, including IaaS, PaaS, SaaS, and models including public, private, and hybrid, are used by organizations. There are several cloud security problems with these models and services [9]. Each service model has certain related problems. Security issues are considered in two views first in the view of service provider who ensures that services provided by them should be secure and also manages the customer's identity management. Customer feedback is yet another angle that verifies the service's level of security.

Virtualization:

To fully exploit the resources of the real operating system, virtualization is a technique in which an operating system image that is fully operational is captured in another operating system. Running a guest operating system as a virtual machine in a host operating system necessitates the use of a unique component called a hypervisor [8].

Data in cloud computing is subject to some hazards due to virtualization. A hypervisor being compromised is one potential risk. If a hypervisor is weak, it may become the main target. The entire system, including the data, may be jeopardised if a hypervisor is exploited. The allocation and de-allocation of resources is another risk of virtualization.The possibility of data exposure to the next VM exists if VM operation data is written to memory and it is not erased before memory is reallocated to the next VM. A better virtualization usage strategy can address the aforementioned difficulties.Before releasing resources, they should be used cautiously and the data must be validated.

Storage in Public Cloud:

Data storage in a public cloud raises additional security issues. Cloud computing typically uses centralised storage, which might be a tempting target for hackers. Storage resources are complex systems that combine hardware and software implementations. If a little security breach occurs in the public cloud, data may be exposed. It is always advised to have a private cloud, if possible, for particularly sensitive data in order to minimise such threats.

Multi-tenancy:

The efficient use of resources offered by multi-tenancy keeps costs down. It means sharing of computing resources, services, and applications at the provider's facilities with other tenants existing on the same physical or logical platform. As a result, it compromises data secrecy, causing information to leak, data to be encrypted, and a rise in the likelihood of assaults. By judiciously authenticating people before granting them access to the data, these problems can be avoided.

Insider Attacks:

A cloud model is a multitenant-based paradigm that is managed solely by the provider. This threat materialises within the company. For cloud workers, there are no requirements or providers for recruiting. Therefore, a third-party vendor can easily hack the data of one company, corrupt it, and then sell it to another company.

Outsider Attacks:

This is the one of the major concerning issues in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network they have more interfaces than private network. Therefore, hackers and assailants have an edge in taking use of the API's flaws and may destroy connections. These attacks are less dangerous than insider attacks because the latter can occasionally go undetected.

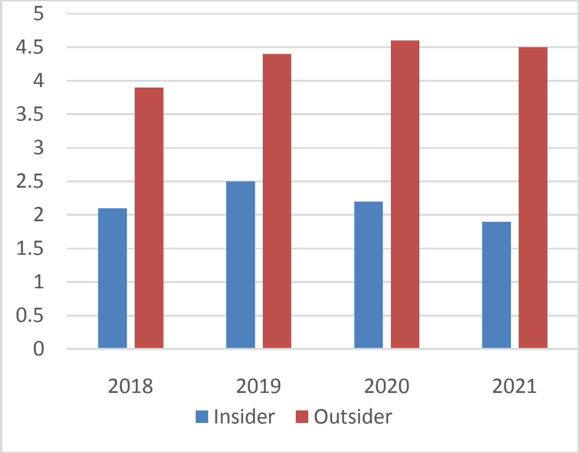

Figure 1: Percentage of Insider vs Outsiders

Loss of Control:

Cloud uses a location transparency model by which it enables organizations to unaware about the location of their services and data. Consequently, a provider can host their services on the cloud from anywhere. In this case organization may lose their data and possibly they are not aware about security mechanism put in place of the provider.

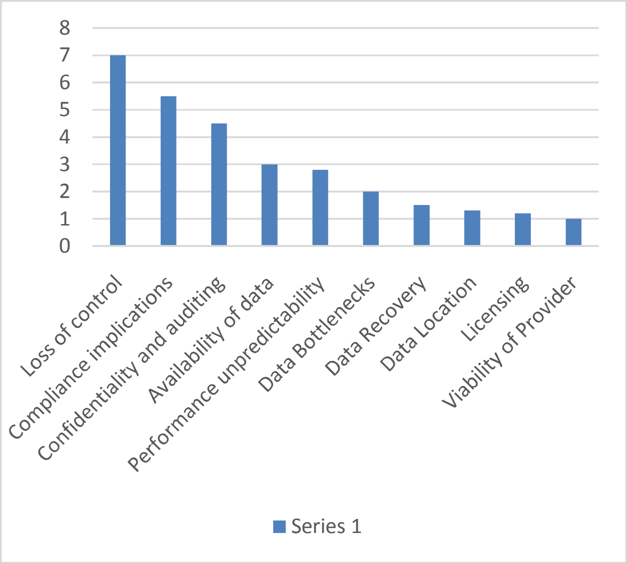

Figure 2: Loss of Control

Data Loss:

Since there are numerous tenants in the cloud, data integrity and safety could not be guaranteed. An organisation may suffer financial and customer count losses as a result of data loss. An notable illustration of this is the upgrading and deletion of data without a backup.

Data at Rest:

Data that is stored in the cloud or that can be accessed via the Internet is referred to as data at rest. This applies to both live and backup data. Since they do not have physical control of the data, enterprises may find it exceedingly challenging to protect data at rest if they are not operating a private cloud. But by maintaining a private cloud with strictly limited access, this problem can be solved [10].

Data in Transit:

Data that is travelling into and out of the cloud is typically referred to as data in transit. This information may be requested for usage at another location in the form of a file or database that is kept in the cloud. Data in transit refers to the state of data when it is being posted to the cloud. Because it must move from one place to another, data in transit is occasionally more vulnerable to dangers than data at rest. The data can be intercepted by intermediary software in a number of ways, and it occasionally has the power to modify the data as it travels to its final location. Encryption is one of the most effective methods for securing data while it is being transmitted.

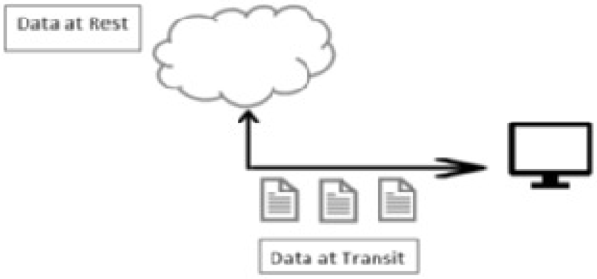

Figure 3: Data in Transit

Network Security:

- Man-in-the-middle assault: In this attack, the attacker establishes a separate connection and communicates with the cloud user over the latter's private network while maintaining complete control.
- Distributed denial of service (DDOS) attacks: In a DDOS assault, a massive amount of network traffic brings down servers and networks, denying consumers access to a specific Internet-based service.
- Port scanning: Information exchange occurs from ports, which are used for port scanning. As soon as the subscriber configures the group, port scanning begins. When you configure the internet, port scanning happens automatically, which goes against the security principles.
- Problem with Malware Injection Attacks: Because so much data is transmitted between cloud providers and customers in cloud computing, user authentication and authorization are required. Attackers may insert malicious code into data transfers between cloud providers and users. As a result, the original user might have to wait until the fraudulently injected job is finished.
- Flooding Attack Problem: In cloud, there are many servers that communicate with one another and transfer data. The requests are processed, the requested jobs are authenticated first, but this authentication requires a lot of CPU utilization, memory and finally due to these servers is overloaded and it passes its offload to another server. Due to all of this, the system's normal processing is halted, and it becomes swamped.

IV. DATA SECURITY MECHANISM IN CLOUD

Authentication and Identity:

Authentication of users and even of communicating systems is performed by various methods, but the mist common is cryptography. Authentication of users takes place in various ways like passwords which is known individually, security token or fingerprint which is unique for every user. When a company uses numerous cloud service providers, one issue with employing traditional identity procedures in a cloud context arises (CSPs). In such a case, synchronizing identity information with the enterprise is not suitable.

Data Encryption:

Different encryption methods can be used for data in transit and data at rest. 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.

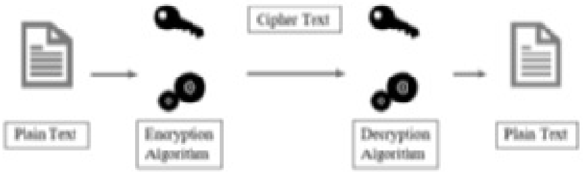

Figure 4: Encryption Technique

Data is encrypted using a variety of cryptographic methods. The level of data protection for ensuring content integrity, authenticity, and availability has grown thanks to cryptography.

There are three basic uses of cryptography:

- Block Ciphers: A block cypher is a data encryption algorithm that produces cypher text by applying a cryptographic key and algorithm to a block of data rather than a single bit at a time. By using this method, it is ensured that messages contain comparable blocks of text are not encrypted in the same manner. Typically, the next encrypted block in a series uses the cypher text from the preceding encrypted block.

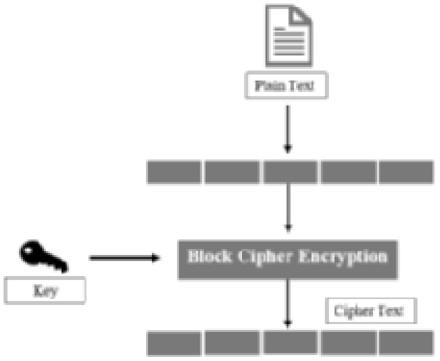

Figure 5: Block Cipher Block-diagram

- Stream Ciphers: This method of data encryption is also known as a state cypher because it is dependent on the cipher's present state. Instead of using blocks of data, each bit is encrypted in this method. Each bit is subjected to an algorithm and an encryption key one at a time. Due to their low hardware complexity, stream cyphers typically perform quicker than block cyphers. However, improper usage of this method might lead to major security issues.

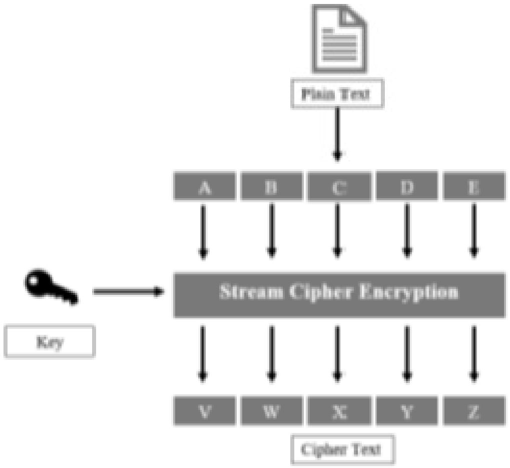

Figure 6: Stream Cipher Block-diagram

- Hash Functions: In this method, an input text is transformed into an alphanumeric string using a mathematical function known as a hash function. The length of the generated alphanumeric string is typically fixed. This method ensures that no two strings can produce the same alphanumeric string. The output string that is created through them may differ greatly even if the input strings are only slightly different from one another.

It is possible for this hash function to be very basic, like the one in equation (1), or highly sophisticated.

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

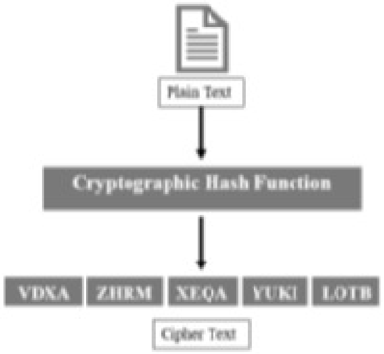

Figure 7: Hashing Block-diagram

Information Integrity and Privacy:

Valid users can access resources and information through cloud computing. Web browsers can be used to access resources, and hostile attackers can also do so. The provision of mutual trust between the provider and the user is a practical solution to the issue of information integrity. Another option is to set up adequate authentication, authorization, and accounting controls so that information access should go through multiple stages of verification to guarantee that resources are being used in a permitted manner. It is necessary to provide some secure access methods, such as SSH-based tunnels and RSA certificates.

Availability of Information (SLA):

Non availability of information or data is a major issue regarding cloud computing services. The information regarding whether or not users can access network resources is provided by a service level agreement. It is a bond of trust between the customer and the provider. Having a backup plan for both the most important information and local resources is one technique to ensure resource availability. This gives the user access to resource information even when it is no longer available.

Secure Information Management:

It is an information security method for gathering data into a single repository. It is made up of agents that run on the systems that need to be monitored, sending data to a server called "Security Console" in the process. The administrator, a human being, who oversees the security console, examines the data and responds to any alerts. Cloud security management becomes significantly more challenging as the user base, dependency stack, and number of cloud security techniques grow. It is also referred as a Log Management. Cloud providers also provide some security standards like PCI DSS, SAS 70.

Malware-Injection attack solution:

With this method, numerous client virtual computers are created and kept in a single storage location. It makes use of the virtual operating system-containing FAT (File Allocation Table). The FAT table contains the application that a client is running. Hypervisor manages and schedules all of the instances. Integrity checking is carried by using IDT (Interrupt Descriptor Table).

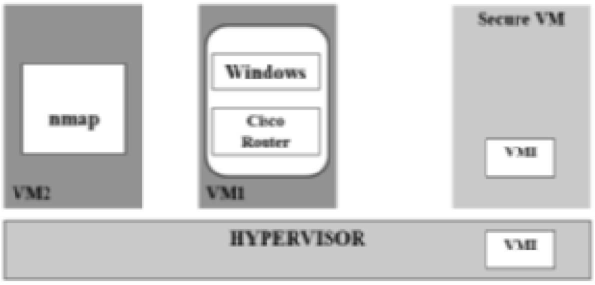

Figure 8: Malware Injection

Flooding Attack Solution:

The entire fleet of servers in the cloud is regarded as one server. One fleet of servers is taken into consideration for system-type requests, one for memory management, and the final one for tasks involving core compute. When one of the servers is overloaded, a new server is brought and used in the place of that server and another server that is called name server has all the record of current states of servers. When one of the servers is overloaded, a new server is brought and used in the place of that server and another server that is called name server has all the record of current states of servers.

V. Future Scope and Conclusions

Future study on this example is something we'd like to see done in an effort to make the cloud security architecture better through the application of AI and machine learning. The number of false positives that take up more time for security professionals is decreased by new AI cybersecurity models. In this situation, AI enables increased effectiveness and resource optimization. Continuous Monitoring is another area of focus. Businesses are able to gather security-related insights, deploy, analyze, and respond with a continuous monitoring method.

Use of cloud computing for storing data is increasing and hence increasing the trend of improving the ways of storing data in the cloud. Data stored or available in the cloud may be at risk if not maintained or protected in right manner. This paper discussed the risks and security threats to data in the cloud and has also provided the ways through which we can protect it and also few points which needs to be improved. In order to determine the risks posed by the hypervisor, virtualization is investigated.

Similarly, threats caused by public cloud, multitenancy, insider and outsider attacks, loss of control, Data loss and Network Security issues have been discussed. One of the major concerns of this paper was data security and its threats and solutions in cloud computing.

The topic of data in various stages and effective methods for encrypting data in the cloud have been covered. The study provided how we could secure our data through various methods and a detailed study on Data Encryption through cryptographic techniques like: Block Ciphers, Stream Ciphers and Hash Functions.

REFERENCES

[1] K. Popovic and Z. Hocenski, “Cloud Computing Security Issues and Challenges,” Proceedings of the 33rd International Convention in MIPRO, 2010, pp. 344-349.

[2] F. Maggi and Stefano Zanero, “Integrated detection of anomalous behavior of computer infrastructures” Network Operations and Management Symposium (NOMS), 2012 IEEE.

[3] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[4] Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. arXiv preprint arXiv:1204.0764.

[5] J. Hu and A. Klein, “A benchmark of transparent data encryption for migration of web applications in the cloud,” 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[6] D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, “Retaining data control to the client in infrastructure clouds,” Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.

[7] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012, May). Enhanced data security model for cloud computing. In 2012 8th International Conference on Informatics and Systems (INFOS) (pp. CC-12). IEEE.

[8] Sangeetha, R., &Silambarasi, M. (2019). Data Security in Cloud Computing. JETIR-International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.

[9] Sharma, S., Gupta, G., & Laxmi, P. R. (2014). A survey on cloud security issues and techniques. arXiv preprint arXiv:1403.5627.

[10] Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016, August). Data security in cloud computing. In 2016 Fifth international conference on future generation communication technologies (FGCT) (pp. 55-59). IEEE.