A COMPREHENSIVE ANALYSIS OF DATA SECURITY AND PRIVACY CHALLENGES IN CLOUD COMPUTING ENVIRONMENT

Smita Sharma
E-Mail Id: sharmasmita34@gmail.com
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh

Abstract - The field of computing is constantly expanding and growing, and cloud computing is no exception. It is gaining attention by offering various computing services such as cloud storage, cloud hosting, and cloud servers to various businesses and academic institutions. From the other end, there are several concerns over cloud security and privacy. In the cloud computing environment, security is still a major issue. With all of the advantages of cloud computing, there are numerous security issues about infrastructure, virtualization, networking, data, and service providers that serve as a major barrier to cloud acceptance in the IT industry. In this paper, various protection and privacy issues related to cloud infrastructure are analyzed.
Keywords: Security, Privacy, Cloud.

1. INTRODUCTION

In cloud computing, a security model is required to manage scalability and multi-tenancy with a necessity of trust. As cloud computing requires pooling tools so that various clients can retrieve them, privacy problems are likely to emerge with information stored or handled in a cloud.
As entities shift with their credentials, data, and technology into the cloud framework, they has to be ready to give up some degree of influence. The entity must have faith in its cloud computing programs and suppliers, but can still authenticate cloud procedures and events. Access control, data protection, compliance, and event planning are the essentials of reliability and authentication. Services and frameworks of cloud computing typically involve: authentication, authorization, data encryption, confidentiality, and multi-tenancy.

2. SECURITY IN CLOUD COMPUTING

To secure its functions, an efficient enterprise should have different layers of security.They are as follows:

2.1 Physical Security

To enable physical access and misuse of resources that have not been certified.

2.2 Personnel Security

Protecting individuals or groups of individuals who are certified to access the operations and records of the company.

2.3 Security operations

Protecting points of interest for particular operations or training arrangements.

2.4 Security of Communication

Secure news, software and content interchanges.

2.5 Network Security

To protect devices, partnerships and substance management systems.

2.6 Data Security

Preserving the privacy, safety of data resources and availability.
Cloud-based systems hide the inner details of software used to develop and operate resources. It is the supplier's responsibility to provide data security and privacy as the client is unable to protect their data at the hardware level. With the support of keys the security factor is taken care of in the context of cloud computing. Critical resources and privacy-related data are therefore very essential for the client for using the cloud. The cloud will guarantee the security and privacy of the customer's sensitive.

Table-2.1 Customer Based Security Requirements

System Level	Service level	Users	Security requirements	Hazards
Application Level	Software -as- a Service	Every individual or company who subscribes to a cloud provider service is responsible for its use.	•Privacy attribute-able to multi-tenant framework •Information security from access to other clients • Access control •Communication safety	•Interception while in use •Rest and travel data alteration •Data disruption •Privacy violation • Impersonation •Session hijacking •Review of traffic

			•Security of software •Availability of services	flow •Network disclosure •Privacy breach
Virtual Level	Platform-as-a- Service Infrastructure -as-a Service	Server refers to an enterprise that utilizes , pays for and charges technology on the cloud infrastructure from the client.	• Access control •Application security •Information security (transit information and information at rest) •Access regulation for cloud services •Safe images •Online cloud safety •Monitoring of communication	•Faults in programming •Software alteration •Software removal • Impersonation •Session hijacking •Network leakage • Link flooding • DDOS •Communication interruption
Physical Level	Hardware used to implement the cloud	The owner refers to an individual or enterprise that owns the assets on the basis of which cloud-based software is deployed	•Legitimate using of cloud computing •Security of Hardware • Availability of hardware •Reliability of hardware •Authenticity of software •Privacy of Network •Privacy of network resources	•Network threats •Connection leakage • DDOS •Hardware disruption •Hardware alteration •Infrastructure misuse •Natural hazards •Hardware extortion

3. CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES

Information is stored within the enterprise in enterprise computing and is completely controlled by the enterprise. The data is saved beyond the location of the customer (on the part of the CSP) in cloud computing. Therefore, in addition to classical security checks, cloud computing must implement additional measures of security to guarantee that information is secure and no data breaches occur due to weaknesses in security.

There are six steps in the information life cycle, according to[4], creating ,saving, using, exchanging, archiving, and deleting. It can switch freely between any stages after the data is created. Data must be secured from its creation to its destruction, throughout all phases of its life cycle. The stage of store and archive is also known as data-at-rest, the stage of use is called as data-in-use, the phase of exchange is called as data-in-transit, and the stage of loss can be called as data-after-delete. These are all self-explanatory steps. In general, encryption is one of the techniques used to prevent unauthorized access in the data transmission process. Data-after-delete is one of the underestimated problems and this is also called data remanence. Data remanence is the physical residual description of the erased data[5]. There can be some physical features that enable the information to be retrieved after a storage media has been deleted[1,2]. Tracing the data path (data lineage) is essential for cloud computing monitoring, particularly in the public cloud, excluding the above stages[3].

The NIST (2004) identifies confidentiality integrity and availability as the three safety goals for information systems. These three principles are specified as the CIA triad and can be described as follows:

3.1 Confidentiality

Preserving confidentiality limits access to critical information by unauthorized employees and assures that only designated individuals are allowed access. A violation of confidentiality leads to unauthorized data disclosure.

3.2 Integrity

Preserving integrity guarantees that throughout the life cycle the information maintains its reliability, integrity and reliability. A breach of integrity gives rise to unauthorized data deletion or alteration.

3.3 Availability

Availability guarantees that secure and prompt retrieval to information is given to authorized individuals. Violation of accessibility leads to loss of access to a service or interruption of the use of data or information system.

In conjunction to the three significant safety goals mentioned above, few more security principles in the security field are treated important by some. Such principles are authenticity and accountability that can be described as follows:

3.4 Authenticity

The property of authenticity guarantees that an individual is who he appears to be and that an input message received by a device comes from a valid and reliable source. This feature helps the sender and the recipient to check the identities of each other as well as the source of the data.

3.5 Accountability

Accountability feature enforcement enables the identification of the organization that induced an action. Accountability feature, that endorses non-repudiation, detection and prevention of intrusion, etc., enables the user to identify a security breach to the relevant organization liable for the breach and implement a legal action.

3.6 Non-repudiation

Regulation of non-repudiation rights means that a payment recipient is unable to contradict or reject an interaction initiated or obtained by the participant. This feature allows a recipient to illustrate that the claimed sender sent a message received by him and vice versa .

The need to address these security dimensions occurs when it is needed to protect data that passes across a channel of communication and is obtained and compromised by an opponent thereby effecting privacy, reliability, credibility, etc. Cryptographic methods are used to fulfill the CIA triad and the other protection targets.

4. SECURITY ISSUES IN THE CIA TRIAD

Loss in confidentiality, integrity and availability (CIA) can have a major effect on the cloud computing field because information is the key element for any enterprise. Information integrity is the guarantee that digital information is not corrupted and that only authorized clients can access it. Accordingly, integrity includes ensuring the reliability, consistency and trust of data throughout its entire life cycle. Retaining CIA is simpler in enterprise computing, but it is more difficult in cloud computing due to the multi-tenant framework and the infrastructure's decentralized design. The following steps is used in cloud computing to maintain consistent CIA:

- Categorize data once the data is generated, determine sensitive information, determine rules, and create access mechanisms for various data types. In addition, generate data archive strategies and destroy data.
- Store information, along with the recovery and backup plan, with good physical and logical security measures.
- Specify the type of information that can be exchanged, whom and how it could be exchanged, and develop rules for sharing data. Several such regulations are commonly referred to as Service Level Agreements (SLA) in cloud computing.
- Develop a corrective measures plan for data theft or hacking due to network or communication software, security vulnerabilities during transfer.
- Loss of availability can be caused by data loss and lack of availability of data. Cloud computing uses few strategies such as scalability and architecture-level high availability. Various approaches and techniques are practiced at various stages of the information life cycle to enhance data security and privacy relevant to the CIA triad. A few of the main strategies are described below:
- Encryption techniques usually provide protection against cloud service threats, but they cannot protect information from installation failures and code bugs[6]. Hash techniques can be used to evaluate unintended and deliberate changes in results. Yet they demand more space and require more time.
- Auditing of third parties (TPA) can be used to validate data integrity. Most authors recommend that third-party auditors verify the quality of information because they are trained in it [7].
- Do not save encryption keys together with encrypted data .
- Build user-friendly Identity and Access Management (IAM) methods.
- Use replication of data, redundancy, backups and fragile mechanisms to deal with problems of availability
- Also provide a failover approach in event the service continues to fail with the CSP.
- If other approaches are not successful, the data dispersion method may be used to resolve the accessibility problem. Here the information is stored in various clouds as segments and the data can be restored when fragmentation methods are required [8].

5. PROTECTING DATA PRIVACY AND INTEGRITY FROM CLOUD PROVIDERS

Security and integrity are essential considerations for different applications. Cloud computing clients are not only concerned about the confidentiality and security of their data being breached by potential attackers, but also by potential interested cloud providers. Generally, the data is encrypted, before the data is being sent to the server of the cloud provider.

While encrypted data is protected against unauthorized access, the encrypted data cannot be completely beneficial, until they are decrypted.

Fig. 5.1 demonstrates the main architecture for data encryption for privacy protection before transmitting it to the cloud environment. The data will then stay encrypted in the cloud and only customers approved by the data owner will be able to obtain the credentials to obtain the encrypted data. The encrypted data can be decrypted only after being downloaded to an authenticated client device. In such a case, data privacy is not dependent on the server's underlying assumption of confidence or the service level arrangement (SLA). Rather, privacy protection relies on the methods of encryption that are utilized to secure the data.

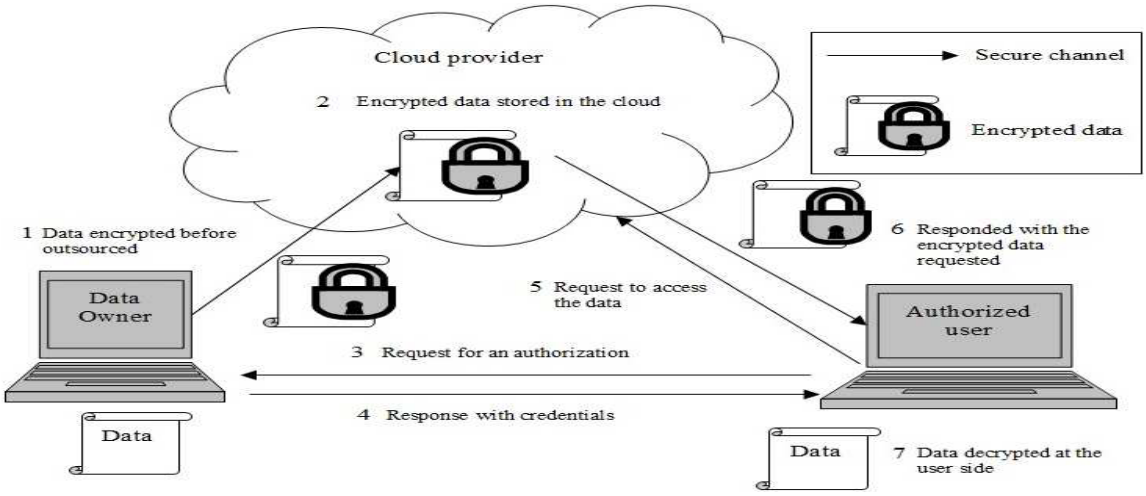

Fig. 5.1 Basic Architecture for Preserving Data Privacy in the Cloud

The initial problems are how to grant the data owner and approved customers can exchange and search the encrypted data and utilize it for certain complex calculations. as per their access permissions. All of these processes should be carried out in a safe manner without revealing any sensitive information to unauthentic organizations, along with cloud providers. New cryptographic methods, secure computing systems, and information-centered security approaches[9] can be effective ways to address a number of security problems in cloud computing.

CONCLUSION

Cloud computing is becoming increasingly common in industries all over the world. Conversely, it is linked with a number of security concerns. Security can be closely related to the development of cloud computing in order to preserve consumers' attention. In this paper, focused have been on the most significant threats to cloud infrastructure that most consumers and companies are concerned with. These threats have been classified into following domains: data threats, network threats, and threats unique to the cloud environment. The paper illustrates the effect of these attacks on cloud consumers and organizations. The security mechanisms that can be used to prevent these risks have been evaluated.

REFERENCES

[1] Herminder Singh & Babul Bansal, “Analysis of Security Issues and Performance Enhancement in Cloud Computing”, International Journal of Information Technology and Knowledge Management, July-December 2010, Vol 2, No. 2, pp. 345-349.

[2] D.H. Patil, Rakesh R. Bhavsar, Akshay S. Thorve, “Data Security over Cloud”, Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012) Proceedings published in International Journal of Computer Applications® (IJCA), 2012.

[3] Gehana Booth, Andrew Soknacki and Anil Somayaji, “Cloud Security:Attacks and Current Defenses”, 8th Annual Symposium on InformationAssurance (Asia’13), June 4-5, 2013, Albany, NY, Pp 56-62.

[4] Zeng, Wenying, "Research on cloud storage architecture and key technologies”, Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human. ACM, 2009.

[5] Pradnyesh Bhisikar, Prof. Amit Sahu, “Security in Data Storage andTransmission in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, IJARCSSE,Pp. 410,Vol. 3, Issue 3, ISSN: 2277 128X, March 2013.

[6] Birendra Goswami, Dr.S.N.Singh, “Enhancing Security in Cloud computing using Public Key Cryptography with Matrices”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 4, Pp.339-344, July-August 2012.

[7] Chow, Richard, et al. "Controlling data in the cloud: outsourcing computation without outsourcing control”, Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, 2009.

[8] Mohamed Al Morsy, John Grundy and Ingo Muller, “An Analysis of The Cloud Computing Security Problem”, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[9] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M.M. A Hashem, “A Newer Us Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”, Applications, Vol. 3, No. 10, 2012.