RESEARCH ARTICLE OPEN ACCESS

# Cloud Security and Privacy

Anika Gupta [1], Ruchi Thakur [2], Guneet Deol [3]
Department of Computer Science and Engineering
Punjab Institute of Technology, Kapurthala
Jalandhar, India

## ABSTRACT

Recent advances in virtualization and Networking Technology have given rise to the popularity and success of cloud computing. However, when sharing the data and business application to a third party causes the security and privacy issues to become a critical concern. Nevertheless, cloud computing is becoming increasingly important for provision of services and storing data in the Internet. Though there are several major challenges in securing cloud infrastructures from different types of attacks. The paper focus on four most representative security and privacy attributes (i.e., confidentiality, integrity, availability and privacy-preservability) relationship between them and the vulnerabilities that may be exploited by attackers, the threat models, as well as the defense strategies in a cloud computing.

***Keywords:-***Cloud Computing; Security; Privacy; Trust; Confidentiality; Integrity; Availability; Data Center (CDS's).

## I. INTRODUCTION

Cloud computing have raised large interest in both academia and industry, but it's still an evolving paradigm. With strong interest and investment from industry and government, the cloud is being increasingly exploited by both organizations and individuals [3].Cloud computing provides resource consolidation, consistent management, and costeffective operation from cloud provider's view; for the cloud user, it provides on-demand capacity, low cost of ownership, and flexible pricing. Cloud Computing also characterized in to three service models-IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). Generally, customers (tenants) in the cloud can run different operating systems and applications in their virtual machines and they are very large and complex that causes security vulnerabilities that is more prone to attack by attackers. So there is a need that a service provider can develop techniques to secure its infrastructure and tenant's virtual machine.[5].

***A. Cloud Characteristics and Security*** *Challenges* Four essential features of Cloud computing are [5]-

***1) Self-Service:*** clouds must allow self-service access so that customers can demand, modify, pay, and use services without interference of human operators.

***2) Per-Usage Metering and Billing:*** Services must be priced on a short term basis (e.g., by the hour), allowing users to release (and not pay for) resources as soon as they are not desirable. For these reasons, clouds must employ features to allow efficient trading of service such as pricing, accounting, and bill. Metering should be done accordingly for different types of service (e.g., storage, processing, and bandwidth) and usage.

***3) Elasticity:*** Cloud computing gives the illusion of unlimited computing resources accessible on demand. Therefore users expect clouds to rapidly provide resources in any quantity at any time.

***4) Customization:*** The resources rented from the cloud must be highly customizable. In the case of infrastructure services, it means allowing users to install specialized virtual appliances and to be given privileged (root) access to the virtual servers.

*The three main challenges to build a secure and trustworthy cloud system* [1] -

***1) Outsourcing:*** It includes the contracting out of a business procedure to another business unit, that implies individuals can lose their control over their data and information that will end up being the underlying driver of cloud insecurity. To defeat this issue firstly, the cloud supplier should be dependable by giving trust and secure figuring and information storage room; second, outsourced information and computation might be provable to clients as far as secrecy, honesty.

***2) Multi-tenancy***: It refers to a principle in software architecture where there is a single instance of the software runs on a server, serving multiple tenants. The security issues such as data violation computation breach flooding attack are incurred so, to resolve these issues, create new security mechanisms that deal with the probable risks without changing multi-tenancy paradigm.

***3) Massive data and intense computation:*** Cloud computing can handle mass data storage and intense computing tasks. But traditional security mechanisms may not sufficient due to unbearable computation or communication overhead. So to overcome this new strategies and protocols are required.

### *B. Supporting techniques*

Cloud computing has authority of a collection of existing techniques, such as Data Center Networking (DCN),Virtualization, distribute storage centers(CDS's), MapReduce, web applications and services, etc[1]. *Modern data center* can be used as an efficient carrier of cloud environments. It provides enormous computation and storage facility by composing thousands of machines with Data Center Networking techniques.

*Virtualization* technology is now extensively used in cloud computing to provide dynamic resource distribution like IaaS. With virtualization, multiple OSs can run on the same physical machine without interfering each other.

*MapReduce* is a programming model for processing and generating a large of data sets with a parallel, distributed algorithms on a cluster. MapReduce speeds up the batch processing on huge data, which makes this, become the first choice of computation model for cloud venders[6].

The ecosystem of cloud security and privacy in vision of five security/privacy attributes (i.e., confidentiality, integrity, availability, privacy-preservability), shown in Fig. 1

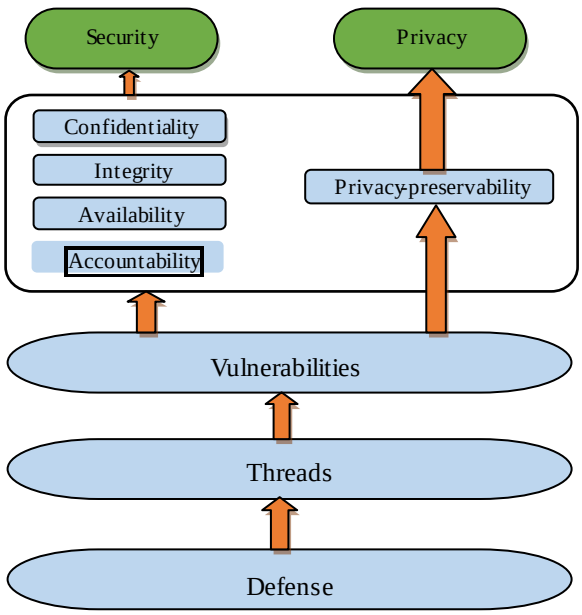


Figure.1. Ecosystem of cloud security and privacy.

## II. CLOUD CONFIDENTIALITY

Confidentiality means the data and computational task of customer should be kept confidential from both cloud provider and other customers. Confidentiality remains as one of the greatest concern in cloud computing security.

### *A. Threats to Cloud Confidentiality*

***1) Cross-VM attack via Side Channels:*** A Cross-VM attack feats the nature of multi-tenancy, which enables that VMs running different OSs may runs on the same physical machine. The timing side-channels is a menacing threat to cloud computing security due to following reasons a) the timing channels pervasively exist and very difficult to control due to the nature of massive parallelism and shared infrastructure; b) malicious customers are able to snatch information from other people without leaving a sign or raising alarms[1][7].

***2) Malicious SysAdmin:*** Cross VM attack is not only threat to cloud confidentiality. Privileged SysAdmin of the cloud provider can do attacks by accessing the memory of a customer's VMs.

### *B. Defense Strategies*

To overcome the cloud Confidentiality, there are many methods:

***1) Co-residency Detection:*** The cross-VM attack is eliminated by co-residency. Cloud customers may require physical isolation, which are even mention in the Service Level Agreements (SLAs). But cloud vendor may be hesitant to abandon virtualization that is helpful in cost saving and resource utilization. Best solution is to share the infrastructure only with "friendly" VMs, which are own by the similar customer or other trustworthy customer.

***2) Retaining data control back to customer*:** While taking into account of the customer's fear of losing the data and information in cloud environments, the best solution is to retain data control for the cloud customers by storing encrypted VMs on the cloud servers.

## III. CLOUD INTEGRITY

As Data Integrity is an necessary in databases in the same way, integrity of Data Storages is an essential in the cloud, it is a major factor that effects on the performance of the cloud. It provides the validity of the data, assuring the consistency or regularity of the data. The integrity in cloud computing

concerns both data integrity and computation integrity. In cloud, the complete storage of data is provided by the enduser that is done at the data centers and the security and integrity of the data depends on the vendor who stores data in the data centers but not the cloud hosts. Therefore only storing data at cloud data stores or data centers doesn't guarantee the integrity of data, but a number of methods should be implemented at each storage level to ensure the data integrity[1].

### *A. Threats to Cloud Integrity*

***1) Data loss/manipulation:*** Data distributed on servers while keeping security and reliability in mind because data may be lost or modified maliciously or unintentionally. Management errors may cause data loss (e.g., while doing backup and restore, data migration) unfortunately that may lead attacks by taking advantage of data owners' loss of control over their own data.

***2) Dishonest computation in remote servers:*** It is difficult to determine whether the computation is executed with high integrity. Since the computation details are not so much transparent to cloud customers, cloud servers may act disloyally and return incorrect computing result. [1].

### *B. Defense Strategies*

***1. Proofs of Retrievability (POR):*** Many solutions have been provided to focus on resolving the issues of integrity. One model is proposed called Proofs of Retrievability (POR) that guarantees remotely and reliable integrity of the data without the retrieving of data file. It is a data encryption mechanism which detects data corruptions and retrieve the complete the data without any damage[8].

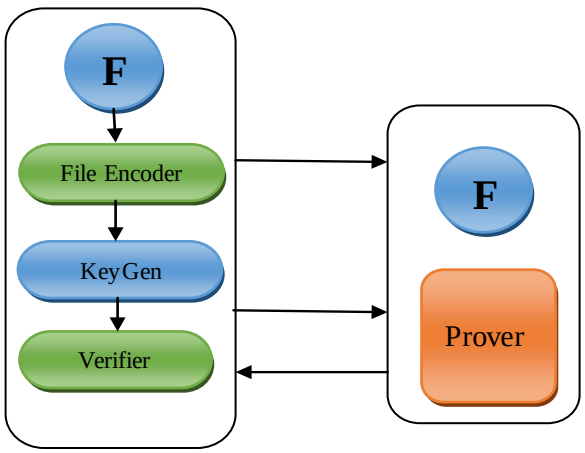


Figure.2. POR Model

***2) Data Encoding Mechanism***: Data encoding is one of the basic methodologies used for the purpose of integration of data being transmitted. The mostly used mechanism of data encoding used in data centers for data integration is based on hash values, means encrypting data using encryption mechanism and then using hash values at server and client side to check the integrity of data being transmitted.

## IV. CLOUD AVAILABILITY

High-availability is, ultimately, the aim of the cloud. It represents the idea of anywhere and anytime access to services, tools and data and enables companies with no physical offices or of global companies with completely integrated IT systems. Availability is also associated with reliability: a service that is on 24x7 but goes constantly offline is useless.

### *A. Threats to Cloud Availability*

***1) Flooding Attack on Bandwidth Starvation:*** In a flooding attack, which can cause Deny of Service (DoS), due to which a huge amount of unwanted requests are sent to a particular service to hinder it from running appropriately. In cloud computing, there are two fundamental types of flooding attacks: Direct DOS (that is, the attacking object is determined, and the accessibility of the targeting cloud service will be fully lost) Indirect DOS (that is the attack is initiate without a specific target).

***2) Fraudulent Resource Consumption (FRC) attack:*** The goal of this attack is to deprive the victim of their long term availability of resources that are publicly accessible that is, attackers, who act as legal cloud service clients, endlessly throws requests to website hosting in cloud 2servers to consume bandwidth, which bill to the cloud client own the website.

### *B. Defense strategy*

***1) Defending the new DOS attack:*** A DOS avoidance strategy called service migration has been developed to remove the Flooding attack. In this a monitoring manager located outside the cloud to detect whether there may be bandwidth starvation by constantly probing the cloud application. When bandwidth deprivation is detected, the monitoring manager will execute application relocation which may discontinue the service for the time being, with it resume afterward. The migration will move the current application to another subnet of which the attacker is unaware.

***2) FRC attack detection:*** The key of FRC detection is to separate FRC traffic from normal activity traffic. There are three detection metrics that together form the criteria for identifying a FRC attack from that of normal web activity [1].

## V. CLOUD PRIVACY

Privacy has been an issue of the highest priority. Privacy is one of the critical concerns to cloud computing because of the customer's data and business tasks reside over the distributed cloud servers which are maintained by cloud supplier. Therefore there are possible risks that confidential data or critical information is disclosed to public. Privacy-preservability as the center trait of privacy and it directly or indirectly influence privacy-preservability including confidentiality, integrity, accountability, etc.

### *A. Threats to Cloud Privacy*

Privacy-preservability is an another form of confidentiality, due to this that they both prevent information outflow Therefore, if cloud confidentiality is still violated, privacy-preservability will also be violated. Similar to other security services, the meaning of cloud privacy is dual purpose: data privacy and computation privacy. The main privacy challenges for cloud computing are: a) Complexity of risk assessment in a cloud environment b) Emergence of new business models and their implications for consumer privacy c) Achieving regulatory compliance[5].

### *B. Defense strategies*

***1) Fully Homomorphic Encryption (FHE)*** to preserve privacy in cloud computing .FHE enables computation on encrypted data, which is kept in the distrust servers of the cloud provider. Data might be process without decryption. The cloud servers have no knowledge about the input data, the processing function, and any intermediate consequence values. Therefore, the outsourced computation occur 'under the covers' in a fully privacy-preserving way [1].

***2) Data indexing solution:*** Privacy issue that is caused by data indexing so to tackle data indexing and to prevent information outflow so the researchers present a three-tier data protection architecture to offer different levels of privacy to cloud customers.

TABLE.1 APPROACHES OF PRIVACY ENFORCEMENT

| **Approach** | **Description** | **Example** |
|---|---|---|
| Information centric security | Data objects have access-control policies with them. | A data outsourcing architecture combining cryptography and access control |
| Trusted computing | The system will consistently behave in expected ways with hardware or software enforcement | Trusted Cloud Computing Platform |
| Cryptographic protocols | Cryptographic techniques and tools are employed to preserve privacy. | Fully Homomorphic Encryption (FHE) and its applications. |

TABLE.2 .A SUMMARY OF RESEARCH ADVANCES IN CLOUD SECURITY AND PRIVACY

| **Attributes** | **Threats** | **Defense Strategies** |
|---|---|---|
| Cloud Confidentiality | 1.Cross-VM attack via side channels<br>2.Malicious SysAdmin | 1.Co-residency Detection<br>2.Retaining data control back to customer |
| Cloud Integrity | 1.Data Loss/Manipulation<br>2.Dishonest Computation in remote servers | 1.Proofs of Retrievability (POR)<br>2.Data Encoding Mechanism |
| Cloud Availability | 1.Flooding Attack on Bandwidth Starvation<br>2.Fraudulent Resource Consumption(FRC) attack | 1. Defending the DoS attack<br>2. FRC attack detection |

## VI. CONCLUSION

The paper has focused on the security and privacy issues in cloud computing based on an attribute-driven methodology. The most representative security/privacy attributes (e.g., confidentiality, integrity, availability, and privacy-preservability) as well as discussed the vulnerabilities, that are exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well.

## REFERENCES


1. Zhifeng Xiao and Yang Xiao, Senior Member, IEEE," Security and Privacy in Cloud Computing", IEEE communications surveys & tutorials, vol. 15, no. 2, second quarter 2013.
2. Hassan Takabi and James B.D. Joshi and Gail-Joon Ahn,"Security and Privacy Challenges in Cloud Computing Environments".
3. Vijay Varadharajan, Senior Member, IEEE, and Udaya Tupakula, Melbourne,Australia),"cloud computing principles and paradigms".
4. Zahir Tari, RMIT University," Security and Privacy in Cloud Computing", 2325-6095/14 © 2014 IEEE.
5. Rajkumar Buyya(The University of Melbourne and Manjrasoft Pty Ltd.,Australia) & James Broberg (The University of Melbourne,Australia),"cloud computing principles and paradigms
6. http://en.wikipedia.org/wiki/MapReduce
7. http://blog.cryptographyengineering.com/2012/10/attack-of-weekcross-vm-timing-attacks.html
8. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5462173&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5462173