CLOUD CRYPTOGRAPHY

DATA SECURITY ISSUES, SLOUTIONS, COMPONENTS, AND PROTOCOLS

AUTHOR- LAKSHYA AGARWAL

SECTION- K17GZ **ROLL NO.-** A13

EMAIL- LAKSHAYAGARWL3214@GMAIL.COM

Abstract- Cloud Computing is one of the fastest growing technology of the IT trade for different occupations. Since cloud computing is a widely used phenomenon in the IT world and used by so many peoples, the major priority of the service providers is to maintain the data security and privacy which can be breached by cybercriminals. To prevent this scenario, a majorly used technology is cloud cryptography which prevents the user data from unauthorized privacy breaches by untrusted service providers or hackers. This paper will explore the Data Security Issues, and components and protocols of Cloud Cryptography.

Index Terms- cloud computing, cloud cryptography, cloud security, data security, encryption protocols, encryption, components.

INTRODUCTION

Cloud computing is one of the hottest topics in the research area in the technological world due to its ability of cost reduction and big flexibility and scalability of computing services. Cloud is a virtualized pool of computing resources which can be divided and allocated to different user with different kind of needs. It only takes few minutes to automate the resources which is very time preventing. It is a set of hardware, interfaces, software, services, networks and storages which can be shared any time according to the need. It provides on demand, self service, and pay per use models which are much more convenient than the deployment.

With the various benefits and uses of the cloud, comes the underlying security and privacy risks such as, resource pooling, multi tenancy, and shareability features which are exploited by cybercriminals and hackers with wrong purposes. It has always been a very important topic for the researchers and the security and privacy of the customer data is the first priority. It is known that when users upload the data on the cloud, they never know the path of the transferred data and if it is being used by some third party. There is no transparency in the cloud system, so it is important to maintain the privacy and security of the user data to get the trust of customer. It is very important maintain the balance between privacy, data access and surveillance to ensure the privacy of users.

Cryptography is the technique which is most talked about when it comes to security and privacy in the world of cloud computing. Before uploading or storing the data to an untrusted cloud service provider, the user can encrypt the data to ensure the security. If the data got accessed by any of the third person, they won't be able to read the encrypted data.

CLOUD DEPLOYMENT MODELS

1. Public Cloud: This is the infrastructure made available for the general public and some large industry groups which is provided by single cloud service provider.

2. Private Cloud: This type of infrastructure is only limited or specifically used by any organization. It has many advantages like security, compliance and quality better than others.

3. Community Cloud: This one kind of infrastructure is used by multiple organizations which serve for the same motive and has shared concerns like security, policy, compliance.

4. Hybrid Cloud: This infrastructure is the combination of two or more than two cloud infrastructures which enables data application portability through load balancing.

CLOUD CHARACTERSTICS

1. On demand service: Every cloud is a huge pool of resources and services which you can access by paying some amount of money accordingly.

2. Network Access: Cloud provides service everywhere through standard devices like mobile, laptops etc. with a good internet connection.

3. Easy Use: Majority of the cloud providers gives internet-based services and interface which are much simpler than the applications and softwares.

4. Business Model: Cloud is a business model where the user has to pay for the services they need according to pay per use.

5. Location Independent resource poling: The computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

CLOUD SOLUTIONS

1. Infrastructure as a service (IaaS): This provides a platform virtualization environment as service instead of purchasing the servers, software, and data centers.

2. Software as a Service (SaaS): In this a software is deployed over internet through a compatible web browser to run behind the firewall on the PCs.

3. Platform as a Service (PaaS): This computing provides development environment as a service. One can use third party equipment to develop their own program and deliver it to the users through internet.

4. Storage as a Service (SaaS): This is a database like service build on utility computing for example, gigabytes per month.

5. Desktop as a Service (DaaS): This is the provisioning of the desktop environment either within a browser or as a terminal server.

CLOUD SECURITY ISSUES

Cloud Security has always been a big challenge for the users and the cloud service providers and the organizations. Most of the industries are migrating to cloud services now, especially public cloud services, where infrastructure service is provided by a cloud service provider.

To cope up these issues, it is really important to take management initiatives within. The ownership and responsibility roles should clearly be distributed to both cloud service provider and the organization or user.

There are a lot of factors on which these management initiatives should be taken. There are security managers who determine the detective and preventive controls exist to define security posture of an organization. Asset, threat, and vulnerability risk assessment matrices are the factors on which the proper security control must be implemented. The security risk assessment report is always from vendor’s point of view because they are the one who manages the cloud service. Here are some security risks list.

- Regulatory Compliance: Cloud Computing providers who refuse to external audits and security certifications.

- Privileged user access: sensitive data processed outside the organization brings with in an inherent level of risk.
- Data Location: When you use cloud, you probably won’t know exactly where your data hosted.
- Data Segregation: Data in the cloud is shared environment alongside data from other customers.
- Recovery: Even if you don’t know where your data is, a cloud provider should tell you what will happen to your data in case of a disaster.
- Investigative Support: Investigating inappropriate or illegal activity may be impossible in cloud computing.
- Long Term availability: You have to make sure your data will remain available even after such event.

PROPOSED SOLUTIONS

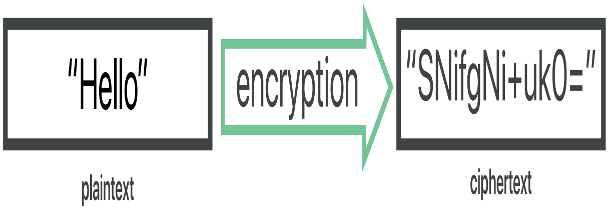
Data storage concerns always arise in cloud computing as it requires to transfer large amount of data throughout the cloud. Users know nothing about what happens to their data after the upload it on a cloud service. Nor the exact location, neither the sources of data collectivity.

To preserve the security of a cloud based virtual infrastructure, it is necessary to maintain confidentiality, authenticity, integrity and availability. These steps should be taken for better security.

- Encryption can be used at the host OS software through which the data transfer from virtual machine would be in encrypted form.
- Physical Security is where the cloud management hosts and virtual systems are safe in the environment with carded doors.
- Authentication capability of a virtual system should be same as of the physical machine authentication system. Digital signatures, biometrics and one-time passwords are some good examples of authentication.
- Separation of duties is important because as the system gets more complex, there is a very high chance of misconfiguration due to less experience with poor communication. Enforcing least privileges with access controls and accountability should also be done.
- Configuration, change control, and patch management are overlooked in small organizations sometimes but they are really important for data security and should be managed in virtual as well as physical world.
- Intrusion detection and prevention is used to know that what data is transferring through the network. This can keep a check on virtual network traffic with a hypervisor-based solution.

ENCRYPTION IN CLOUD

Encryption s away of scrambling data so that only authorized parties can understand the information. In technical terms, it is a process of converting plaintext into cyphertext. In simple terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of encryption key which is a set of mathematical values that both the sender and the recipient of an encrypted message know.



SECURITY COMPONENTS

Confidentiality, Integrity, and Availability, also known as the CIA triad, is a model designed to guide the policies for information security in some organization and are the three most important components of data security. It is also referred as AIC to avoid the clash with Central Intelligence Agency.

Confidentiality limits the access to the information, Integrity is the assurance for the information to be trustworthy and accurate, and Availability guarantees the access of information to the authorized entities in the cloud network.

1. CONFIDENTIALITY

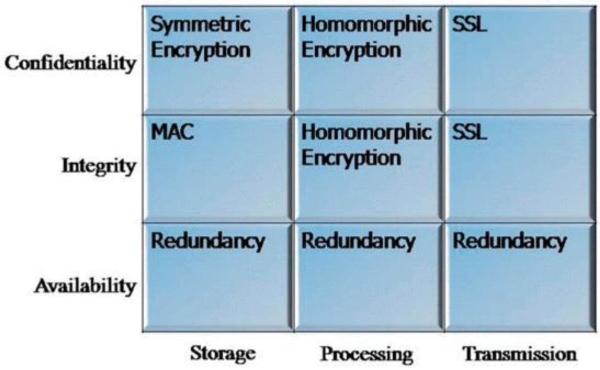
Confidentiality is very close to privacy. The steps are taken to stop the sensitive information from reaching in the wrong hands, and making sure that the right people could access it like biometric verification, data encryption and security tokens etc. The data is categorized according to the amount it can do to a particular user or organization if it falls in the wrong hands. According to that, the measures are taken and implemented because of their priorities and severeness.

2. INTEGRITY

Integrity maintains the trustworthiness, accuracy and consistency of data through its life. If a data has to be transferred from one user to another or if someone wants to upload it on the cloud, data could not be changed or should maintain its consistency and accuracy throughout. The measures taken include file permissions and user access control. Checksums are often used for the verification of integrity.

3. AVAILABILITY

Availability keeps an eye on the resources requirement for the user such as maintaining all the hardware, performing hardware repairs when needed and maintaining a correctly functioning operating system, and also all the necessary system updates which are required. These measures make the system fast and adaptive for the worst-case scenarios.



	Storage	Processing	Transmission
Confidentiality	Symmetric Encryption	Homomorphic Encryption	SSL
Integrity	MAC	Homomorphic Encryption	SSL
Availability	Redundancy	Redundancy	Redundancy

ENCRYPTION PROTOCOLS

1. Homomorphic Encryption:

Homomorphic encryption is a method of encryption that allows any data to remain encrypted while it's being processed and manipulated. It enables you or a third party (such as a cloud provider) to apply functions on encrypted data without needing to reveal the values of the data.

In practice, most homomorphic encryption schemes work best with data represented as integers and while using addition and multiplication as the operational functions. This means that the encrypted data can be manipulated and analysed as though it's in plaintext format without actually being decrypted.

2. Symmetric Key Encryption: Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form.

3. SSL (Secure Socket Layer) Encryption: Secure Socket Layer is a standard security technology for establishing an encrypted link between a server and a client, typically a web server (website) and a browser, or a mail server and a mail client (e.g. Outlook).

More specifically, SSL is a security protocol. Protocols describe how algorithms should be used. In this case, SSL protocol determines variables of the encryption for both the link and the data being transmitted.

4. MAC (Message authentication Code): A message authentication code (MAC) is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.

A MAC requires two inputs: a message and a secret key known only to the originator of the message and its intended recipient(s). This allows the recipient of the message to verify the integrity of the message and authenticate that the message's sender has the shared secret key. If a sender doesn't know the secret key, the hash value would then be different, which would tell the recipient that the message was not from the original sender.

In the past, the most common approach to creating a MAC was to use block ciphers like Data Encryption Standard (DES), but hash-based MACs (HMACs) which use a secret key in conjunction with a cryptographic hash function to produce a hash, have become more widely used.

REFERENCES

1. Veerraju Gampala, Srilakshmi Inuganti, and Satish Muppidi, *Data Security in Cloud Computing with Elliptic cloud cryptography*, International Journal of Soft Computing and Engineering (IJSCE), ISSN:2231-2307, Vilume-2, Issue-3, July 2012

2. Kim-Kwang Raymond Choo, Joseph Domingo-Ferrer, and Lei Zhang, *Cloud Cryptography: Theory, Practice and Future Research Directions*, Conference on Computer and Communication Security (ACM CCS 2006)

3. D. L. Ponemon, *Security of Cloud Computing Users*, 2010

4.https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA