Review on Cryptographic Measures for Information Security in Cloud

D. Santhadevi*
Anjali Chhabra**
Suruchi Sinha***

Abstract

Cloud is the next milestone of the information technology. It has many potential advantages and many enterprises are migrating to public, private or hybrid cloud. Cloud computing is the internet based computing, it provides services of resource sharing, software and information sharing on the basis of demand, while cloud computing promises to offload tasks like data storage and processing power; the model raises questions about data accessibility, privacy and security. From the users' perspective, cloud computing security more concern on privacy protection and data security issues. Good practice to ensure security and privacy in the cloud by cryptographic techniques; it provides efficient security in a cloud computing environment.

Keywords: Encryption/Decryption, Cloud, RSA, Cloud Security

Introduction

More companies and educational institutions are started to recognize and realize the benefits & advantages of cloud computing. The adoption of cloud controls the costs and provision of infrastructure as needed particularly appeals to new businesses with fewer resources and may lead to gains in efficiency & effectiveness in developing , deploying, and maintaining the infrastructure, from initial concept building to current actual deployment, cloud computing is growing more and more mature.

Security control measures in cloud are similar to ones in traditional IT environment. As multi-tenant characteristic, service delivery models and deploy models of cloud computing, compared with the traditional IT environment, however, cloud computing may face different risks and challenges. Traditional security issues are still present in cloud computing environments. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in cloud [3].

Due to the openness and multi-tenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field [3]:

- Cloud service Provider (CSP) does not provide any standard infrastructure and security boundaries in a dynamic scalability environment that may lead to compromise in data security.
- Deployment of unique security measure is difficult in accordance with service delivery models of cloud computing, resources cloud services based on may be owned by multiple providers. They may have a conflict of interest in security measures.
- Unauthorized users can access any user's data in the open cloud and virtualized resources are shared by multi-tenant.
- As the cloud platform has to deal with massive information storage and to deliver a fast access, cloud security measures have to meet the need of massive information processing.

D. Santhadevi*
IINTM, GGSIPU

Anjali Chhabra**
IINTM, GGSIPU

Suruchi Sinha***
IINTM, GGSIPU

This paper describes data security and protection for privacy issues in cloud. This paper is organized as follows: Section 2 gives a brief description of what exactly cloud computing is. Section 3 describes the potential threats in cloud. Section 4 shows cryptographic technique for information security and protection for privacy issues in cloud. Section 5 summarizes the contents of this paper.

Cloud Computing

Cloud computing allows the clients to access their applications and data from anywhere at any time with the help of internet. Data wouldn't be limited to a hard drive on one user's computer or even a corporation's internal network. It reduces the hardware costs and need of advanced hardware deployment in the client side. No need to buy the fastest computer with the most memory. Instead, client needs an inexpensive computer terminal. The terminal could include a monitor, input devices like a keyboard and mouse and just enough processing power to run the middleware necessary to connect to the cloud system. Cloud users don't need a large hard drive because their all information's are stored on a remote computer. Cloud computing systems facilitate right software, software license and company-wide access to computer applications. Instead, the company could pay a metered fee to a cloud computing company [8][3].

The three major services provided by the cloud that are; **IaaS**- provides Infrastructure as a Service such as raw computing power, storage and network bandwidth via Internet. **PaaS-** provides Platform-as-a-Service such as databases, development tools and other components required to support the delivery of customer application. **SaaS-** provides Software-as-a-Service such as general and specialized application. General applications are word process, spread sheet, email, etc., Specialized application such as customer relationship management (CRM) and enterprise resource management (ERM)[3].

Characteristics of Cloud

- Availability of data, software, resource at anytime and anywhere on demand.
- Application integration and support- Integrating multiple services and assets into a powerful composite application is more convenient with well-designed cloud platforms. This enables easy interaction with and support of legacy resources and other infrastructure services.
- Dynamic Scalability – it ensures elasticity that is adding or removing resources as on demand. This offers dynamic provision of resources in real time for peak loads placed on computing power, bandwidth, application and storage resources.
- Virtualisation- allows sharing of storage devices and servers are increased in utilisation. It allows applications can be easily migrated from one physical server to another.
- Multitenancy- it reduces the cost and significantly more value over time and simple revenue & cost economics of cloud services. But this type of configuration needs high level of security with firewall and access control requirements to the physical location.

Potential Threats in Cloud

Security and privacy are still referring by many organisations as the top substance of cloud services adoption, which has led to the need of encryption in the cloud. From the research six main security issues addressed are:

- Notification violation and data residency
- Data management in cloud
- Data protection in transmission
- Encryption key management
- Access controls
- Management of the encryption system

Notification Violation and Data Residency

Not all data requires equal protection, so businesses should categorise data intended for cloud storage and identify any compliance requirements in relation to data notification violation or if data may not be stored in other authority control. It is recommended that enterprises should put in place an enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities [9]. The plan should take stakeholders into account, such as legal, contract, business units, security and IT.

Data Management in Cloud

The cloud service provider's (CSP's) must provide the data storage life cycle and security policy to the tenants. Tenant should find out if:

- What type of separation mechanism used in the multi-tenant storage?
- Should mechanisms are used to prevent data being replicated to specific countries or regions?
- Is storage used for backup and archive is encrypted? What type of the key management strategy includes for a strong identity and access management policy to restrict access within certain jurisdictions?
- Is data is encrypted at transmission. What type of key management techniques used to protect encryption key?

Data Protection in Transmission

As a minimum requirement, that businesses ensure that the CSP will support secure communication protocols such as SSL/TLS for browser access or VPN-based connections for system access for protected access to their services[6]. The good business policy says that encrypt sensitive data in movement to the cloud, if data is unencrypted while in storage or use, it will be serving on the enterprise to hack against data breaches [9].

Encryption Key Management

- General security issues are Keys being stolen and Keys being vulnerable to attack or compromise.
- Management of all keys include single point of failure and needs to scale linearly to handle lots of keys.
- Availability allows authorized users to access their data.
- Governance- policy that defines proper protection, access and usage; to get the rights is probably hard.

Access Controls

Access control manages users, controls the user's privileges, files and other resources. It manages users by identification and authentication with the help of username and password. For accessing the file, authorization is provided on the basis of requirements or on the basis of their roles. There are many traditional access control models, Discriminatory Access Control (DAC), Role Based Access Control (RBAC), Identification Based Access control (IBAC), that works well in the non-cloud environment [1][5]. But in open environment of cloud, it is difficult to manage multitenant access. Attribute Based access Control and Biometric Access control provide best solution for the cloud.

Management of Encryption Key

"Key management is really where the brains need to be applied and where the pitfalls can occur. At the end of the day, keys have to be kept secret, otherwise the encryption was a waste of time in the first place."

- Richard Moulds

Cloud computing introduces other risks for key management. Vulnerabilities have been found in all virtualisation software that can be exploited to bypass certain security restrictions or gain increased privileges. New technologies can't assume existing processes are still secure. Poor key management, week key generation and storage practices could easily leak the key. Add an additional risk of having a third party control for securing the keys becomes much harder. A corrupt employee could add a backdoor to your machine to access the keys and your machine while it is running or live transfer it over an unencrypted link. At any time a key has stolen or your data at risk, for this situation, revoke the key and re-encrypt data with a new key.

Segregation of encryption key management from the cloud provider helps protect both the user and cloud provider from compliance issues. Crypto-shredding is also an effective technique for migrating cloud computing risks. In this where the provider destroys all copies of the key ensures that any data that's from the outside your physical control is extracted inaccessible. In crypto-shredding user manage their keys[5].

Encryption for Privacy and Protection

Encryption in the Cloud

Encryption is the first options for protecting data in the cloud, and a variety of new solutions and tools can help organizations adequately control encryption keys, policies, and authentication and authorization associated with data protection in cloud environments where data and systems are dynamically migrated across platforms and even distinct data centers.

In private cloud and Infrastructure as a Service (IaaS) provider environments, there are several options for encrypting data that minimize the need to redesign applications and re-architect system and network design. These include the following [4]:

- **Volume-based encryption**: In cloud data volumes are online; any authenticated user can access data on the volume. This may be highly impractical in a multi-tenant environment unless providers manage access to volumes per cloud instance. In most provider environments, managing storage volume security options will be a significant amount of work, because each customer would need specific encryption options, availability scenarios and access types.
- **Application-specific encryption**: Custom applications may include encryption with keys and certificates, and this is often incumbent on the developers to ensure key portability and encryption continuity is maintained when applications are moved to a cloud provider environment. In Platform as a Service (PaaS) environments, encryption APIs may be made available.
- **File encryption:** File encryption is likely the most flexible type of encryption for us within virtualized and cloud environments. Encryption is applied at the source, and managed by customers or third-party providers that act as "proxies" for key management and encryption policy application.
- Cloud provides built-in Security of policy-based encryption for entire virtual machines, and the VMs stay encrypted when moved throughout a cloud provider's environment. All key management and role-based access is defined locally before moving to the cloud, greatly simplifying the ability to migrate VMs without checking compatibility requirements in the CSP infrastructure.

Cases for Cloud Encryption

There are three major components to any encryption system: the data, the encryption engine and the key management. Here we discussed how these three pieces are distributed in some common cloud security architectures.

- **When using the cloud for data storage**, implement virtual private storage architecture. Encrypt the data before it's sent to the cloud, and decrypt it when it comes back. Since you are managing the encryption and keys, it's critical you keep copies of the keys in a secure backup (which should be a function of the key management built into your backup solution).
- **For basic encryption of data stored in an IaaS application**, you can build volume encryption into your instance, and store the data in a second encrypted volume. This isn't the most secure option, since you are storing the key with the encryption engine in your instance,

but this does protect you from anyone without the right access to the running instance from seeing your data.

- **For more advanced encryption**, you can separate the key from the encryption engine in the instance. In this three-tier architecture, you have a volume with the encrypted data, an instance with the encryption engine, and key-management server that provides the encryption key on-demand. This is useful if you don't want the key embedded with the instance, since then an attacker who obtains a copy of the instance has a copy of the key. An attack might also spin up a new instance off the same image with the embedded key. The external key management server should only return the key when a set of policy-based criteria are met, such as manual approval of a new running instance, or based on integrity checks in the encryption client running in the instance. The key is then used by the instance in memory until it's shut down.

Cloud Encryption with RSA Data Protection Manager

RSA (cryptosystem for public key encryption) Data Protection Manager provides encryption of data at rest and in motion in virtualized and multi-tenant environments with enterprise-controlled key management. It provides tenant-specific data encryption and enables flexible security administration control, performance monitoring, and integrated key management with RSA Data Protection Manager.

Cloud Encryption with RSA Data Protection Manager Features includes [7]:

- **Enterprise-Controlled Key Management: An enterprise or a cloud service t**enant has the control of the keys using RSA Data Protection Manager Server. It separates data encryption in the cloud from the encryption key management.
- **Regulatory Compliance:** Enables enterprises to meet regulatory-compliance requirements such as PCI, HIPAA, and SOX in a multi-tenant cloud and virtualized environment.
- **Virtual Storage Encryption:** Carves out a virtual storage volume from a shared multi-tenant cloud storage infrastructure and encrypts the virtual storage volume at block level with AES-256 encryption algorithm to ensure data security.
- **Secure Communications:** Extends enterprise key management into the cloud by creating a secure VPN tunnel between the enterprise and external cloud environments, enabling the enterprise to manage encryption keys and extend other security-management capabilities to the cloud.
- **Private or Public Cloud Support:** Supports VMware vSphere, VMware vCloud Director, and Amazon EC2/VPC.
- **Pre-Integrated Key Management:** Helps to ensure easy deployment and management of these two products in the enterprise data center environment.

Conclusion

Cloud computing which involves information storage, retrieval and processing on the computing machine that are connected through internet. But security is the most important issue which is refraining industry to adopt cloud as a long term solution to store their sensitive data. In this environment unauthorized persons either deliberately or accidently try to steal the data that leads to violation of privacy and data security. So we need a security mechanism to enforce information security and integrity. This paper discusses merits of RSA based encrypted data key management and distribution of data in cloud and in transit. This paper analysis various dimension of security issues existing in the cloud computing environment.

References

1. Abdul Raouf Khan, "Access Control in Cloud Computing Environment" May 2012. *ARPN Journal of Engineering and Applied Sciences* by Asian Research Publishing Network. Vol- 7, NO. 5, ISSN 1819-6608.

2. Deyan Chen and Hong Zhao ,"Data Security and Privacy Protection Issues in Cloud Computing",2012. *International conference on Computer Science and Electronics Engineering* by IEEE computer Society.

3. Ferraiolo DF and Kuhun DR," Role Based Access Control" 1992. Proceeding of 15th *National Computer Security Conference*, Baltimore MD. pp. 554-563.

4. http://cloudsecurity.techtarget.com

5. http://www.opengroup.org/soa/source-book

6. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, " An analysis of security issues for cloud computing" 2013.*Journal of Internet Services and Applications* 4:5. Published by Springer Open Journal.

7. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing", Proc. of *IEEE International Conference on Cloud Computing* (CLOUD-II, 2009), pp. 109-116, India, 2009.

8. Peter Mell & Timothy Grance, "The NIST Definition of Cloud Computing", Jan, 2011.

9. Rohit Bhadauria & Sugata Sanyal. " Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", June 2012. *International Journal of Computer Applications* 47(18):47-66. Published by Foundation of Computer Science, New York, USA.

10. W.Jansen and T.Grance," Guidelines on Security and Privacy in Public Cloud Computing" 2011. *National Institute of standards and Technology(NSIT SP 800-144). U.S, Department of commerce.*