SECURITY ARCHITECTURE BASED CLOUD NETWORKING

[1]Ashwini K.Lode, [2]Anusha A.Adur, [3]Vaishnavi R.Ghubde, [4]Tejaswini B.Waghmare, [5]Prof.Anand D.G.Donald

Department of Computer Technology
Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur

***Abstract*: The cloud computing offers service over internet with dynamically scalable resources. Cloud computing services benefits the users by cost and ease to store and use. The services need to address the security during the communication of sensitive data and critical applications to shared and public cloud environments. Cloud computing environments have many advantages and drawbacks related to data security. Hence, the project aims to emphasize main security issues existing in cloud computing environment. It will also provide security to users individual data loss attacks. It also focuses on the means of information assurance that provides the ability to automatically access or transfer information between two or more security domains. This privacy model also indicates that when protecting ones data, one should net only prevent it collection but also have control our its use. i.e computing services provide and service users needs to work together.**

***Keywords*: Infrastructure-as-a-Service (IaaS), platform-as-a-Service (PaaS), software-as-a-Service (SaaS),Virtual Machine(VM).**

1. INTRODUCTION

OVERVIEW

Cloud Computing is a common word for the delivery of hosted services over the internet. It has been divided into three broad services categories: Infrastructure as a Service (Iaas), Platform as a Service (Paas) And Software as a Service (Saas).cloud Computing is a word coined to the recent trend in computing service provision. this trend has been the technological and Cultural Shift Of Computing Service Provision From Being Provided Locally To Being Provided by Third-Party Service Providers Functionality such as storage, Processing and other functionality is now offered on Demand, As A Service And Both Freely And At Cost Data, That Was Once Housed Under A Consumers Own Administrative And Security Domain, Has Now Been Extracted And Placed Under The Domain Of The Cloud Service Provider.

OBJECTIVE

- Provide security to user individual the data.
- Protect from data breach and data loss attacks.
- Implementation of ABE algorithm.

2. LITERATURE REVIEW

There are many settings where a user would want to give access to documents based on certain credentials or the Position/Role of a Person. We would want different kind of users of the database to be able to see only those contents that are relevant to them. Similarly, In a distributed setting where all the data may be stored in a server, The server might allow access to files and documents based on some predefined access control policy, For example, Clients may have to provide proper certification to retrieve specific files. ABE Attributed based encryption (ABE), FIrst introduced by Sahai and Waters provides a mechanism by which we can ensure that even if the storage is reduced, the loss of information will very less. Attribute Based Encryption effectively binds the access-control policy to the data and the users (clients) instead of having a server mediating access to files Types of ABE. ABE can be divided in two categorized depending on whether the attributes are embedded in the ciphertext or whether the access-structure is embedded in the ciphertext.

2.1 Security Problems of Cloud Computing Network

Traditional network attacks: Cloud computing is based on the network structure, so there exist great menace for the traditional network attacks. Basically they are the following kinds: distributed denial of service (DDOS) attack, utilization type attack, information collection type attack and the false news attack [10]. Cloud computing has the characteristics of its own: huge user information resources, highly centralize, complicated management, so are also more likely to become the target of hackers, hackers probably attack the whole cloud computing services via a user, and the damage and loss will be obvious more than the traditional enterprise nets application environment. Priority access control: Generally speaking, the cloud services has the priority right to access data but not the users, so the user's data may be leaked out by the administrative staff and other employees, unable to guarantee the user's important and confidential data security. SSL attack: Secure Sockets Layer (SSL) is the encryption method to provide security for network communication; a lot of cloud providers employ SSL to guarantee cloud security. Now many hackers and communities are studying the SSL, different from the general way of network attack, at present the SSL attacks are rare, but SSL has become a worry to cloud computing security.

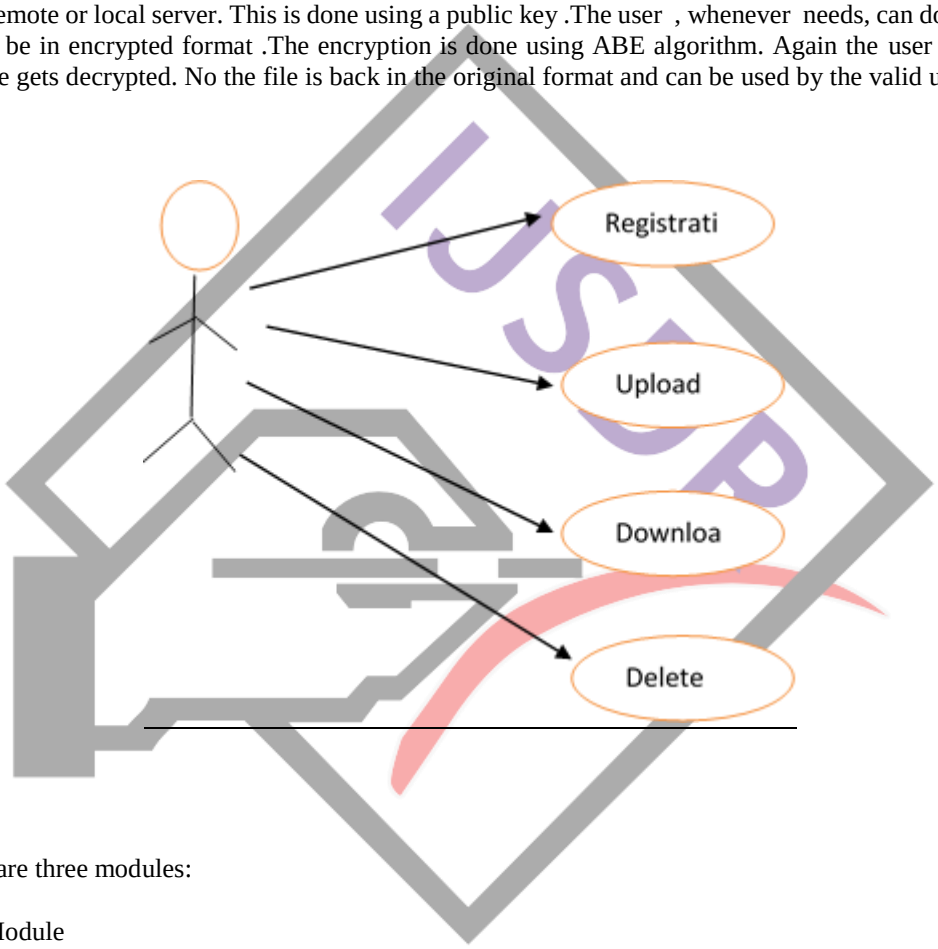
2.2 Data Security of Computing Clouds

Data Location: When use cloud computing services, customers don't know where the data are placed on the servers, even don't know which country these servers are placed . When these countries need to investigate these data, due to the different law, providers may be forced to submit data and be unable to guarantee the security of user data. Data separation: In the cloud computing services, a large amount of user data are in a shared environment. In order to reduce spending, providers usually reuse the IP address, the IP address of one user may be reused to another, so often leads to the abuse of the data, there is no guarantee to data privacy. The data encryption is the way to ensure the data security in one way, but encryption does not always guarantee the security of the data, the fail of decryption may cause damage to the data . To users and cloud services the data can't use, this reduces efficiency of data, causes waste of resources. Data backup: To the important and confidential data, if cloud services dose not backup the data, when data lost by the server problems, or users accidentally delete data, important data can't be restored.

3. PLANNING

In this project, the user can store and process the files. For this the user has to first sign up, or if he or she is an existing user , then they have to log in. After log in, the user has to select the file for uploading. This file then gets encrypted and in this encrypted format, is stored on remote or local server. This is done using a public key .The user , whenever needs, can download this file. The downloaded file will be in encrypted format .The encryption is done using ABE algorithm. Again the user needs to enter a key, through which the file gets decrypted. No the file is back in the original format and can be used by the valid user.

Use Case Diagram



In this project, there are three modules:

1. New User Grant Module

2. File Upload Module

3. File Access Module

1. New User Grant Module: In this module, there is normal registration for many users. There may be many owners, and many users.

2. File Upload Module: In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server.

3. File Access module: In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs).

4. SERVICE PROVIDER SECURITY ISSUES

The public cloud computing surroundings offered by the cloud supplier and make sure that a cloud computing resolution satisfies organizational security and privacy needs. The cloud supplier to provision the safety controls necessary to safeguard the organization's information and applications, and additionally the proof provided regarding the effectiveness of these controls migrating organizational information and functions into the cloud.

4.1 Identity and Access Management

Identity and Access Management (IAM) features are Authorization, Authentication, and Auditing (AAA) of users accessing cloud services. In any organization "trust boundary" is mostly static and is monitored and controlled for applications which are deployed within the organization's perimeter. In a private data center, it managed the trust boundary encompasses the network, systems, and applications. And it is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication. With cloud computing, the organization's trust boundary will become dynamic and the application, system, and network boundary of an organization will extend into the service provider domain. Application security and user access controls will compensate for the loss of network control and to strengthen risk assurance. Strong authorization, authentication based on claims or role, trusted sources with user activity monitoring, identity federation , accurate attributes, single sign-on (SSO), and auditing.

4.2 Privacy

Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify. In Private and confidential customer data fast rising for the consequences and potential costs of mistakes for companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure
Operations, and other related security and legal issues.

4.3 Securing Data in Transmission

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here.
In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

4.4 User Identity

In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privileged-user monitoring, including logging activities. This monitoring should include background checking and physical monitoring. To coordinate authentication and authorization with the enterprise back-end or third-party systems are identity federation and rapid on boarding capabilities. For allowing users to easily and quickly leverage cloud services use single sign-on capability is required to simplify user logons for both the cloud and internally hosted applications.

5. SECURITY ISSUES IN VIRTUALIZATION

A virtual machine (VM) could be a software implementation of a machine that executes programs like a physical machine. Extending virtual machines to public clouds causes the enterprise network perimeter to evaporate and therefore the lowest-common denominator to impact the safety of all.

Virtual Machines (VM) have some relation with host machines and if VM is improperly configured could allow functionality to fully avoid the virtual environment. It find full kernel or root access to customer node. This result gives full system failure in the security mechanisms and is called VM escape. Some more risks in VM is the hypervisor is the part of a virtual machine that allows enables VM/host isolation and resource sharing. It provides the necessary separation during planned attack greatly determines how the virtual machine can continue to exist risk. Rogue Hypervisors is the guest operating system is booted inside of a virtual environment working like as a traditional OS managing I/O to hardware and network traffic, even though it's controlled by the hypervisor. The hypervisor has a full control over the system, not only in the VM and also on the host machine. Increased Denial

of Service Risk: The threat of denial-of-service (DoS) attacks against a virtualized system is as prevalent as it is against no virtualized systems; but because the virtual machines share the host's resources, such as memory, processor, disk, I/O devices, and so on, a denial-of-service attack risk against another VM, the host, or an external service is actually greatly increased.

6. CONCLUSION

Cloud Computing embodies the as-a-Service paradigm and allows for services to be provided enmasse to consumers. The problems associated with the use of cloud based services can be summarised by the unknown risk profile and unknown expectation of privacy Section. When service users push data to the cloud they need to rely upon Cloud Service Providers (CSPs) adhering to their remit, and doing so dutifully. However, when looking to build solutions to protect data in the cloud it is important to remember that for the service user the CSP can be trusted, albeit at arms length.

REFERENCES

[1] Alex X. Liu and Fei Chen, "Privacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No 5, pp.887-895, 2011.

[2]Arockiam, Parthasarathy and Monikandan S, "Privacy in Cloud Computing: A Survey", Proceeding of International Conference of Adv Comp Sci. & Information Technology (ACSIT 2012), pp.231-230, 2012.

[3] Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13 (2009).

[4] Shen, Z., Tong, Q.: The security of cloud computing system enabled by trusted computing technology. In: 2nd International Conference on Signal Processing Systems (ICSPS 2010), vol. 2, pp. 2–11 (2010).

[5] Zhang, S., Zhang, S., Chen, X.: Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks, ICFN 2010, p. 93 (2010)