Enhancing Security in Cloud Computing

Joshi Ashay Mukundrao (Corresponding author)
D.Y. Patil College Of Engineering, Akurdi, Pune University of Pune, Maharashtra, India
Tel: +918446356591 E-mail: ashay016@gmail.com

Galande Prakash Vikram
D.Y. Patil College Of Engineering, Akurdi, Pune, University of Pune, Maharashtra, India
Tel: +919422962961 E-mail: prakashgalande21@gmail.com

Abstract

Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing.

This paper has been written to focus on the problem of data security. Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. To ensure the security of users' data in the cloud, we propose an effective and flexible scheme with two salient features, opposing to its predecessors. Avoiding unauthorized access to user's data by signaling user by sending message to his/her mobile number at the start of transaction. Displaying fake information in case of unsuccessful login for avoiding further login trials by intrusion (Honeypot).

Keywords*:* Cloud Computing, Authentication, Honeypot

1. Introduction to system

Refer Figure 1

A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.

In which if a user (either employee or anonymous) want to access the data if it belongs to protection then user have to register itself (if he is already registered need not require further registration Now suppose the user registered itself for accessing data, Organization will provide username and password for authentication. At the same time organization sends the username to cloud provider. Request for access data

1. Request for access data
2. Send the signal to redirect person
3. Redirects

Now when user sends request along with username to access the data to cloud provider, the cloud provider first check in which ring requested data belong. If authentication is required, it first checks the username in its own directory for existence, if the username does not exist it ask the user to register itself. If the username matches it redirect the request to company for authentication.

(1) Send password for authentication

(2) Redirect to access resource

(3) Request redirected

Now the user sends password for authentication, and after authentication it redirect the request to cloud provider to access resource .If user-name and password doesn't match then user is not allow to access their account. And also in some case if hacker wants to hack the account of a perticular user then in that case hacker gets only the fake database of the account i.e concept of Honeypot in which certain limit is there to access the account by hitting the user-name and password, if limit become cross then hacker get's the fake database.

2. Literature Survey

The Internet began to grow rapidly in the 1990s and the increasingly sophisticated network infrastructure and increased bandwidth developed in recent years has dramatically enhanced the stability of various application services available to users through the Internet, thus marking the beginning of cloud computing network services.

Previously many organizations tried to enhance their security for their security constraints, for their secure database, for their secure web applications but they had not got success to achieve a high-level security for their organizations.

Example- A commonwealth games website- It did not got the success to achieve the high security level as per the user's requests. it was totally failed down to handle the many requests at a once. it was failed down to provide the online ticket booking facility to the user's because of the hitting of many requests at a one time. So that's why there is need to provide the high level of security over the computing network, we have to use the cloud computing .and provide better security over it.

Cloud computing services use the Internet as a transmission medium and transform information technology resources into services for end-users, including software services, computing platform services, development platform services, and basic infrastructure leasing. As a concept, cloud computing primary significance lies in allowing the end user to access computation resources through the Internet. Vaquero, Rodero-Merino, Caceres, and Lindner suggested that cloud computing could be defined as the integration of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services. The special features of cloud computing include the storage of user data in the cloud and the lack of any need for software installation on the client side. As long as the user is able to connect to the Internet, all of the hardware resources in the cloud can be used as client-side infrastructure. Generally speaking, cloud computing applications are demand-driven, providing various services according to user requirements, and service providers charge by metered time, instances of use, or defined period.

Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission. These protection methods normally require cryptography algorithms and digital signature techniques, as explained below. Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric cryptography is used in the U.S. Federal Information Processing Standard's (FIPS) Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES) or 197 Advanced Encryption Standard (AES) and others. This type of encryption and decryption process uses a secret key. Asymmetric cryptography, on the other hand, uses two different keys, a "public key" for encryption, and a "private key" for decryption. Examples include RSA cryptography and Elliptic Curve Cryptography (ECC). Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography. The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed access. In the process of challenge and response the client's encrypted key uses the client's password to convert a derived value and. In this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most peoples' conception of a password[13]. Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP, however is the single-use nature of the password. After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels[14], primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them.

3. Cloud Computing

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service.

Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers.

Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. In some cases, legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location. Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies.

4. Essential Characteristics of system

4.1 On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

4.2 Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants (PDAs)).

4.3 Resource pooling

The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the subscriber generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

4.4 Rapid elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

4.5 Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

5. Software Quality Attributes of system

5.1 Information security

Information security pertains to protecting the confidentiality and integrity of data and ensuring data availability. An organization that owns and runs its IT operations will normally take the following types of measures for its data security:

- Organizational/Administrative controls specifying who can perform data related operations such as creation, access, disclosure, transport, and destruction.
- Physical Controls relating to protecting storage media and the facilities housing storage devices.
- Technical Controls for Identity and Access Management (IAM), Encryption of data at rest and in transit, and other data audit-handling compliance requirements.

When an organization subscribes to a cloud, all the data generated and processed will physically reside in premises owned and operated by a provider. In this context, the fundamental issue is whether a subscriber can obtain an assurance that a provider is implementing the same or equivalent controls as to what the subscriber would have implemented. The following issues arise when a subscriber is trying to ensure coverage for these controls:

- Compliance requirements, with regard to data that a subscriber is intending to move to a cloud, may call for specific levels and granularities of audit logging, generation of alerts, activity reporting, and data retention.
- For encryption of data at rest, the strength of the encryption algorithm suite, the key management schemes a provider supports, and the number of keys for each data owner (individual or shared keys) should be known by the data owners. Data processed in a public cloud and applications running in a public cloud may experience different security exposures than would be the case in an onsite hosted environment.

5.2 Data Privacy

Privacy addresses the confidentiality of data for specific entities, such as subscribers or others whose information is processed in a system. Privacy carries legal and liability concerns, and should be viewed not only as a technical challenge but also as a legal and ethical concern. Protecting privacy in any computing system is a technical challenge; in a cloud setting this challenge is complicated by the distributed nature of clouds and the possible lack of subscriber awareness over where data is stored and who has or can have access.

5.3 System Integrity

Clouds require protection against intentional subversion or sabotage of the functionality of a cloud. Within a cloud there are stakeholders: subscribers, providers, and a variety of administrators. The ability to partition access rights to each of these groups, while keeping malicious attacks at bay, is a key attribute of maintaining cloud integrity. In a cloud setting, any lack of visibility into a cloud's mechanisms makes it more difficult for subscribers to check the integrity of cloud-hosted applications.

6. System Features

6.1 Web Service

Creating web service that facilitates Encryption & Decryption of data using specified algorithm.

6.2 Client side console

The user can access functionality of Cryptography services through client console.

6.3 Server Console

Software’s installation & s/w functionalities are executed on server side.

7. Advantages of system

- Scalability
- Remote Accessibility

- Quality of Service
- Security & Backup
- Cost & Efficiency

8. Conclusion

This paper proposes a more effective and flexible distributed verification scheme to address the data storage security issue in cloud computing. As it rely on the cryptography algorithms [RSA] and digital signature techniques, for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission.

This method achieves the availability, reliability and integrity of erasure coded data and simultaneously identifies misbehaving servers i.e. whenever data corruptions will occur during the storage correctness verification, this method should

Identifies the misbehaving servers, Through detailed performance analysis, it show that the scheme should provide more security to user's data in cloud computing against failure, unauthorized data modification attacks and even server colluding attacks

9. References

"AWS Security Whitepaper," http://s3.amazonaws.com/ aws_blog/AWS_Security_Whitepaper_2008_09.pdf

"Cloud Computing Security: Raining On The Trendy New Parade," Black Hat USA 2009, www.isecpartners.com/files/Cloud.BlackHat2009-iSEC.pdf

"ENISACloudComputingRiskAssessment,"November20th,2009, www.enisa.europa.eu/act/rm/files/deliverables/ cloud-computing-risk-assessment/at_download/fullReport

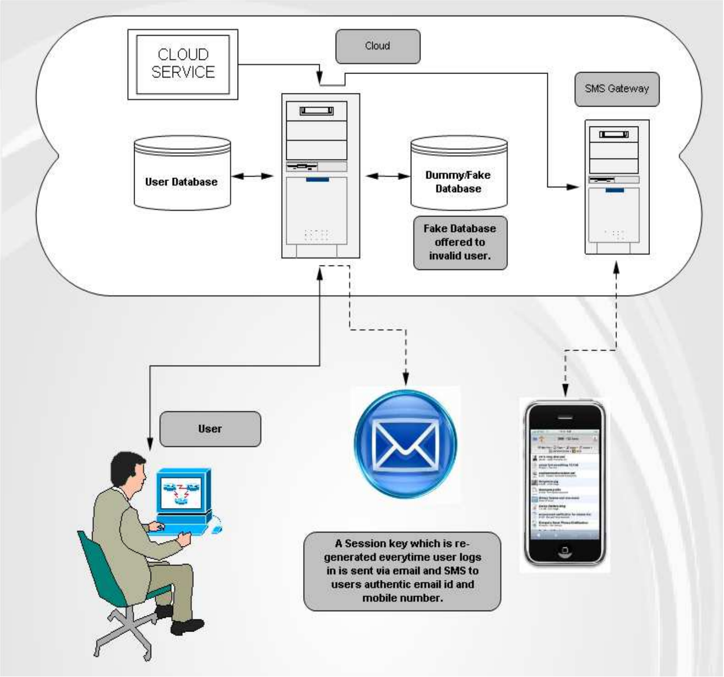
"Encrypted Storage and Key Management for the cloud". Cryptoclarity.com. 2009-07-30. Retrieved 2010-08-22. http://www.csrc.nist.gov/groups/SNS/cloud-computing/ Cloud-computing-v26.ppt

http://www.amazon.com/Enterprise-Cloud-Computing-Architecture Applications/

On technical security issues in cloud computing, Meiko Jensen etal, 2009

Van Brussel, H., Wyns, J., Valckenaers, P., Bongaerts, L. & Peters, P. (1998), "Reference Architecture for Holonic Manufacturing Systems: PROSA", *Computers in Industry* **37**(3), 255-274.

Figure no.1



Fake Database offered to invalid user.

A Session key which is re-generated everytime user logs in is sent via email and SMS to users authentic email id and mobile number.