A Security Mechanism for Cloud Computing Threats

Arun Kumar Dewangan
Asst. Prof., Dept of CSE
GD RCET, Kohka, Bhilai

Gurudatta Verma
Asst. Prof., Dept of CSE
GD RCET, Kohka, Bhilai

ABSTRACT

Cloud computing could be a platform for enhancing capabilities and developing potentialities at run time while not adopting new infrastructure, human resources, or software package systems. Also cloud computing originated from an enterprise idea, and developed into a successful IT invention. Despite the plug surrounding cloud computing, customers stay reluctant to deploy their industrial enterprise into the cloud. All the same, lack of security is that the only major concern that hinders increased use of cloud computing. Moreover, the complexness with that cloud computing manages information privacy, and information security makes the market hesitant concerning cloud computing. The design of cloud models threatens the security of existing technologies once deployed in an exceedingly cloud environment. Thus, users of cloud services must understand the dangers of uploading information into the new atmosphere. Therefore, in this paper we are proposing a different type of security technique for cloud computing threats so that all same problematic situations can be overcooked.

KEYWORDS

CC, Cloud Security, SHA, RSA, Crypto-Chest

1. INTRODUCTION

Cloud computing is a computing mechanism which is based on resource sharing. Here the word "Cloud" is symbol for internet. Cloud computing is the technique through which we deliver computing resources or services over the internet. These services allow individuals or business groups to use resources (software and hardware) which are managed by third party group at different locations [1]. Cloud computing consists of activities such as the use of social networking sites and other forms of interpersonal computing; most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. It is a way to enhance the capacity and/or add capabilities at run time without having new infrastructure, training new employees, or licensing new software. It extends Information Technology's existing capabilities [2]. Developers with great innovative ideas for Internet services require no longer large capital outlays in hardware to deploy the services; this paradigm shift is transforming the Information Technology industry. The operation of large scale, commodity computer datacenters was the key enabler of cloud computing, as these datacenters take benefit of economies of scale, permitting for reduce in the cost of electricity, bandwidth, operations, and hardware [3]. Based on purpose and characteristics cloud computing uses various delivery models [6]:

1. Public Cloud

Cloud computing services from vendors that can be accessed across the internet or a private network using one or more data centers, shared among multiple customers with varying degrees of data privacy control.

2. Private Cloud

Private clouds are built for the exclusive use of one client, providing the utmost control over data, security, and quality of service. The company owns the infrastructure and has control over how applications are deployed on it.

3. Hybrid Cloud

Hybrid clouds merge both private and public cloud models. They can help to supply on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations.

2. CRYPTOGRAPHY & CLOUD COMPUTING

Cryptography involves the conversion of simple text into an unreadable form. Cryptography is a technique which is frequently used to transfer data safely by ensuring that only the intended recipient can read them. This domain provides an overview of the history of cryptography and the lots of complex, creative approaches used in current enterprise encryption.
Bleikertz et al. [8] proposed the secret key principles, which are applied to virtual machines on the basis of unique client-controlled CaaS architecture for cloud computing. However, these researchers focused the use of physical hardware security modules, and found that architecture separates the management and storage of the keys of cloud clients as well as all cryptographic operations into a secure crypto-domain called DomC, which is tightly coupled to the workloads of clients. Whereas, Sanyal and Iyer [9] explored cloud security based on public key values. They discussed a secure, and efficient algorithm based on the multi-key encryption AES technique, a 128/192/256 bit cipher key used to encrypt and decrypt data. Results confirmed, that AES increases security for the cloud computing compared with RSA. But, AES can be used in virtual machines and in public or private clouds. Mao [10] noted an important problem for secure network virtualization: the negligent usage of intelligence and distributed power by hypervisors. The research discussed how hypervisors use information boxes to gain control. Therefore, he proposed network virtualization using modern technology with several useful applications, including secure multi-tenancy for cloud computing. Cryptography significantly affects the management of the intelligence and distributed power of hypervisors.

3. PROBLEM IDENTIFICATION

Cloud computing has presented problems concerning data control, the effect of software systems on organic resources, and the transfer of data access manage to another. Based on the above literature review, we can conclude that cryptography can be used for the following concern:
Proofs of irretrievability

- Petite signatures.
- Televise encryption.
- Private information rescue.

Cloud computing as well as web services run on a network structure so they are always open to network type attacks. One of these attacks is the distributed denial of service attacks. If a user (hacker) could capture a server then the hacker could stop the services from operation and demand a ransom to put the services back online for proper operation. The security issue has played the most important aspect in hindering Cloud computing. No doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears scary to many.
Well-known security concern like data loss, botnet (running remotely on a collection of machines) and phishing pose severe threats to organization's data and software. In Cloud computing environment data protection against vulnerable threat is the most important security issue. In this issue, it concerns the method in which data is stored and accessed, compliance, audit requirements.

- If the password is too short or poor, key guessing attacks are possible.
- The key management techniques are always complex to handle.
- Integrity of data is also an important issue.
- No protocols are fully safe from attack, more than one combination of techniques are required.

4. METHODOLOGY

The design of cloud models threatens the security of existing technologies once installed in an especially cloud environment. Thus, users of cloud services must understand the risk of uploading data into this new atmosphere. Therefore, we are proposing a different type of security mechanism for cloud computing threats so that all same problematic circumstances can be overcooked. By use of Crypto-Chest we can enhance the security of data over cloud.
As we have already discussed in problem identification section that data integrity and security of client data is our most important security concern. Hence, to overcome these issues we have proposed the combination of SHA based hashing (for data Integrity) and RSA encryption technique (for data security) referred as Crypto-Chest which will responsible for data integrity and security.

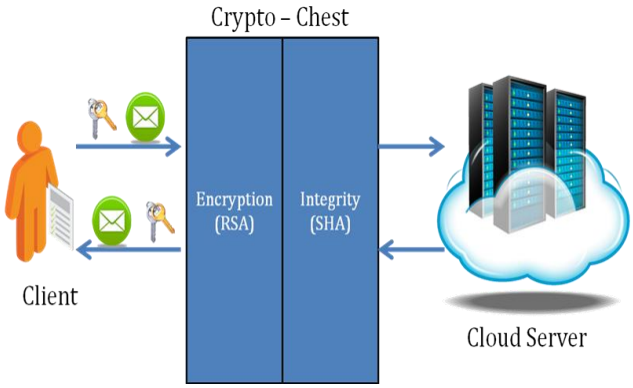

Fig. Proposed Architecture in Cloud Computing

Encryption using customized RSA

The frequently used public-key algorithm is the RSA (Rivest, Shamir, and Adleman) cryptosystem, named for its inventors. Following are the main aspects of the algorithm:

- Authentication: this feature is very essential because RSA assures the origin of the sent information, only the sender with his/ her private key is permitted to encrypt the message hence transform the message into unreadable form as a result the receiver will have confirmation of the source or origin because he/ she will only be able to decrypt the message only through the corresponding public key.
- Privacy & Secrecy: The content of the information and communication must be only accessible to the sender and the recipient of the information.
- Non repudiation: The sender cannot say that the message has not been encrypted with his/ her private key since the private key used for the encryption is unique and it's the owner's/ sender's responsibility to make sure that it is not used by non-authorized third person/ parties.

NaQi, Wei Wei, Jing Zhang [12] concluded that disadvantage of RSA is fake public-key algorithms. The user should not worry if public key leak, but require considering someone takes another's place by counterfeiting published false public key, so it should be possible to broadly publish the right key to public to avoid counterfeiting, also complexity of the key creation. Because of the RSA algorithm is limited by the prime number and efficiency of generating prime number is comparatively low, so it is hard to get a secret once. Above issues can be overcome by modified RSA in which we are achieving integrity of public key by using SHA algorithm.

//Modified RSA Key Generation
Generate two different primes p and q

$$Calculate\ the\ modulus\ n = p \times q$$

$$Calculate\ the\ totient\ \phi(n) = (p - 1) \times (q - 1)$$

$$Select\ for\ public\ exponent\ an\ integer\ e\ such\ that\ 1 < e < \phi(n)$$

$$and\ gcd(\phi(n), e) = 1$$

$$Calculate\ for\ the\ private\ exponent\ a\ value\ for\ d\ such\ that$$

$$d = e{-}1 \bmod \phi(n)$$

$$Public\ Key = [e, n]$$

$$Private\ Key = [d, n]$$

$$S\_Public\ Key = SHA(Public\ Key)$$

5. CONCLUSION & FUTURE SCOPE

The design of cloud models threatens the security of existing technologies once installed in an especially cloud environment. Thus, users of cloud services must understand the risk of uploading information or data into this new atmosphere. By use of third party Crypto-Chest we can improve the security of data over cloud. Following are the benefits of using Third party Crypto-Chest:

Non-repudiation: The user cannot deny legitimate signature claims. **Practical and efficient**: The algorithms have costs comparable with those of standard signature schemes.

Semantic security: The hash value does not disclose data about the message signed.

Message hiding: No one have to reveal the original message to deny the validity of a forgery.

Lightweight key distribution/refreshment: Public keys do not need to be distributed after refreshment. Secret key retrieval is voluntary for recipients.

The RSA and SHA algorithm can be used further in VANET (Vehicular Ad Hoc Network) environment.

6. REFERENCES

[1] Heena I. Syed and Naghma A. Baig, "Survey On Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, pages 308-312, April 2013.

[2] Kuyoro S. O., Ibikunle F. and Awodele O., "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks, Volume 3, Issue 5, pages 247-255, 2011.

[3] AMIT GOYAL and SARA DADIZADEH, "A Survey on Cloud Computing", University of British Columbia, Technical Report for CS 508, pages 1-14, December 2009.

[4] Shilpashree Srinivasamurthy and David Q. Liu, "Survey on Cloud Computing Security".

[5] S.Sathyavani and T.P.Senthilkumar, "Survey on Cloud Computing", International Journal of Computer Trends and Technology, volume 4, Issue 9, pages 3116-3120, Sep 2013.

[6] Jason Carolan and Steve Gaede, "Introduction to Cloud Computing architecture", Sun Microsystems, Inc, 1st Edition, June 2009.

[7] Wayne Jansen and Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology Draft Special Publication 800-144, January 2011.

[8] S. Bleikertz, S. Bugiel, H. Ideler, S. Nürnberger, and A.-R. Sadeghi, "Client-controlled Cryptography-as-a-Service in the Cloud."

[9] S. Sanyal, and P. P. Iyer, "Cloud Computing--An Approach with Modern Cryptography," arXiv preprint arXiv:1303.1048, 2013.

[10] W. Mao, "The role and effectiveness of cryptography in network virtualization: a position paper." pp. 179-182.

[11] K. Rauber, "CLOUD CRYPTOGRAPHY," International Journal of Pure and Applied Mathematics, vol. 85, no. 1, pp. 1-11, 2013.

[12] NaQi , Wei Wei, Jing Zhang, Wei Wang, Jinwei Zhao, Junhuai Li, Peiyi Shen, Xiaoyan Yin, Xiangrong Xiao and Jie Hu Analysis and Research of the RSA Algorithm SCIENCE ALERT 2013.