International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 02 – Issue 06 || June 2017 || PP. 25-29

SURVEY ON SECURITY OF CLOUD DATA SHARING

D.Vijaya lakshmi[1], Dr.G.S.Anandha mala[2], P.Hari kumar[3]

[1] *Department of Computer Science and Engineering*
Easwari Engineering College
Chennai,India
[2] *Department of Computer Science and Engineering*
Easwari Engineering College
Chennai,India
[3] *Department of Computer Science and Engineering*
Easwari Engineering College
Chennai,India

Abstract: Cloud computing is an emerging scenario of information technology .The cloud architecture comes with various benefits and services like location independent, on demand self-service, universal data access,remote data storage in cloud etc. All these service facilitate users to be relieved from the burden of storage and maintenance of data.But data in Cloud server is associated with high security risk especially when data is stored and shared at the server . Data security has become the major issue nowadays. Thus cloud computing needs a secure technique. Hence we propose a architecture based on a Cryptosystem using RSA (Rivest Shamir Adleman) and ECDSA(Elliptic Curve Digital Signature Algorithm) which aims to protect the data stored in the cloud from the unauthorized access using Open stack environment.

Keywords: RSA(Rivest Shamir Adleman), ECDSA(Elliptic Curve Digital Signature Algorithm).

1. Introduction

Cloud computing has quickly gained its popularity over traditional software and hardware models over the last decade. While companies and customers are moving their data and businesses to the cloud, people raise more and more concerns about the security and privacy of cloud systems. Protecting customers data and businesses in the cloud is vital to all cloud system designers and service providers. Cryptography for Data security is a very powerful method for protection of data from being stolen. Cryptography is a method to encode the information to keep the information from being hacked by the other party.

Figure1: cloud computing architecture

This model of cloud has 5 characteristics, 3 service models and 4 deployment models.
This model of cloud has 5 characteristics, 3 service models and 4 deployment models.

1.1 CHARACTERSTICS

- On-demand self-services: The cloud computing provides the resource on demand when the consumer wants it i.e users can use the on demand services from the cloud at any time through the internet.
- Broad network access:Capabilities are available over the network and accessed across the internet from broad rangeof devices such as PCs ,laptop and mobile devices using standard APIs.
- Resource pooling:The computing resources of the provider's were pooled to serve multiple consumers using a multi-tenant model,these services can be adjusted to suit each client's need.
- Rapid elasticity: Capabilities are elastically provisioned and released automatically to provide scalable services .consumer can purchase as much or as little computing power as they need.

- Measured service: Cloud systems automatically controls and optimize resource by monitoring,measuring based on utilization.in short pay for use.use

1.2. SERVICE MODELS

The Service Models in cloud computing are

- Software as a Service (SaaS) :
  The ability provided to the consumer is to use the provider's applications that is hosted in the cloud. The applications are accessed through various client devices by either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The cloud infrastructure is not managed and controlled by consumers including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- Platform as a Service (PaaS):
  The ability provided to the consumer is to deploy their own software on to the cloud infrastructure consumer-created or acquired applications are supported by the provider. The consumer does not control the cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications.

- Infrastructure as a Service (IaaS):
  The ability provided to the consumer is to provision processing and other fundamental computing resources where the consumer control and manage the system in terms of operating system. The consumer does not manage or control the cloud infrastructure but has control over operating systems.

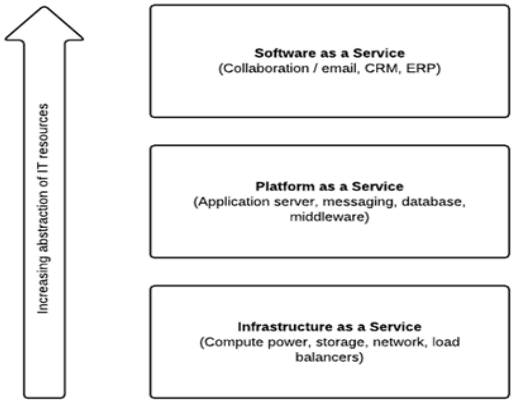

Figure 2 Service models

1.3.DEPLOYMENT MODELS

The Deployment Models in cloud computing are

- Private cloud:A cloud is called a "private cloud" when the services are rendered over a network that is open for own use The infrastructure has been deployed and is maintained and operated for the use of a single organization consisting of multiple consumers. It may be in-house or with third party.

- Community cloud: The infrastructure is shared among number of organization with similar interests and requirements. It may be operated , owned and managed by one or more organizations in the community.

- Public cloud: A cloud is called a "public cloud" when the services are available to the public on a commercial basis. There may be very little financial outlay compared to the capital expenditure requirement normally associated with other deployment models

- Hybrid cloud: Hybrid cloud consist of number of clouds of any type but the clouds have ability through their interface to allow data and applications to be moved from one cloud to another.composition of two or more clouds that remain different entities but are bound together, offering the benefits of multiple deployment models such as data and application portability. Hybrid

cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

2. SECURITY

Security in cloud computing involves concepts such as network security, equipment and control procedures deployed to protect data, applications and infrastructure associated with cloud computing.

2.1. SECURITY CHALLENGES AND THREATS IN CLOUD COMPUTING

- Cloud computing is an emerging technology with shared resources and lower cost that relies on pay per use. Due to cloud characteristics, it may face lots of threats and problems in the security. In this section, these issues are explained and discussed

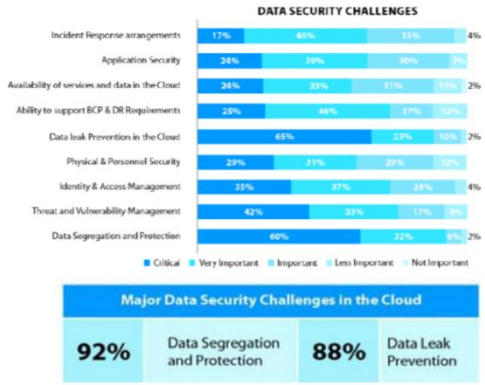

Figure 3Data Security and Privacy

3. ASYMMETRIC ENCRYPTION

Asymmetric cryptography is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. The keys are simply large numbers that have been paired together but are not identical . The public key is used to encrypts the plaintext or verifies a digital signature, whereas the private key is used to decrypt cipher text or to create a digital signature.

Figure 4Asymmetric key

3.1. RSA ALGORITHM

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adelman. RSA is an asymmetric encryption/decryption algorithm. Public key is distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone**.**

3.2. ELLIPTIC CURVE CRYPTOSYSTEM

Elliptic curve cryptography(ECC) depends on elliptic curve theory over finite fields which is one of the public key encryption algorithms which is used to make cryptographic keys smaller and more efficient. The functions and characteristics of an elliptic curves are mainly used for encryption,digital signature and pseudorandom generators .

4. FUNDAMENTAL SECURITY DEFINITIONS

In order to build a secure cloud system, similar as other information systems, it requires many important security properties including but not limited to:

- Confidentiality implies that only intended parties can read the protected information. Information leakage is an example of violating confidentiality. Data stored in and transmitted to cloud systems may be encrypted to protect confidentiality.

- Authenticity refers to that messages, transactions, and documents are assured to be genuine, i.e., created by claimed parties and unaltered by someone else. Please note that authenticity automatically implies integrity, where integrity means that data has not been modified in an unauthorized manner.

- Availability means that data should be available when it is needed. Availability is vital in cloud systems since customers' businesses may depend on data stored on external cloud servers. For example, Denial-of-service (DoS) attacks specifically attempt to affect availability.

5. RELATED WORKS ON SECURITY

Nadeem et al[5] analyzed the popular secret key algorithms including DES, 3DES, AES (advanced encryption system), Blowfish. Their implementation and performance was compared by encrypting varying contents and sizes. The algorithms were implemented mainly on two distinguishable hardware platforms to compare their performance. In the end, the results were presented which concluded that the Blowfish was the faster.

Eguro, K et al[3] "FPGAs for trusted cloud computing,in this paper it describes that protected bitstreams can also be used to create a root of trust for the clients of cloud computing services. This hardware-based approach solved a fundamental problem that currently impedes the greater adoption of cloud computing. This approach can be applied to the specific application of handling sensitive and healthy data. This system also maintained the advantages of the cloud computing with minimal additional hardware. It also described, this system can be extended to provide more generic secure cloud architecture using various cryptography techniques providing security with FPGA hardware.

Khan, Kiah et al[10] have described and improve the resource limitation of mobile devices, mobile users may utilize cloud-computational and storage services. mobile user in cloud environment to protect the mobile user's identity with dynamic credentials by a light-weight security scheme. frequently occurring dynamic credential generation operations towards a trusted entity to keep minimum processing burden on the mobile device is offloaded by this scheme. to enhance the security and reliability of the scheme, the certified information is updated frequently on the basis of mobile-cloud packets exchange. the credentials with the mobile user public key are encrypted to ensures the confidentiality. And also described an incremental version of proxy re-encryption scheme to improve the file modification operation and compared with the original version of the proxy re-encryption procedure on the basis of turnaround time, energy consumption, CPU utilization, and memory consumption during executing the security operations on mobile device. the incremental version of proxy re-encryption scheme shows expressive improvement while performing the file modification operations using limited processing capability of mobile devices

NesrineKaaniche et al[2] has proposed ID based cryptography in which the data is firstly encrypted and stored on the public cloud server. This concept also offers access control so that only authorized users can use the data. With the help of this approach unauthorized user even not get the data without client permission.

NehaTirthani et al[3]explain about cloud security issues and then proposed a security model for cloud in which Diffie Hellman Key Exchange and Elliptical Curve Cryptography algorithms are used. The whole model is described in four steps in which first step establish connection, the second is

Deyan Chen et al.[5] explain some serious security issues with cloud computing and then provide details of current security solution for data security and privacy protection in the cloud.

Ramesh et al.[2],the selected encryption algorithms namely DES, AES and BLOWFISH were used for performance evaluation in this paper. According to input size of text files and experimental result, it was conc1uded that Blowfish algorithm consumes less execution time and memory usage. Blowfish performs approximately 4 times faster than AES and 2 times faster than DES. Blowfish consumes less memory compared with AES and DES. However, AES showed poor performance results compared to other algorithms, since it requires more processing power. Blowfish was not only fastest but also provides the greater security through strong key size which enables it to be used in many applications like Bulk Encryption; Internet based Security and Packet Encryption.account creation, third is authentication and last step contain data exchange.

Yellamma et al[10] paper presented the data computing method relating to the cloud data storage methods and security in virtual environment. Authors presented a method for providing data storage and security in cloud computing using public key cryptosystem RSA

6. CONCLUSION

In this paper ,we discuss the overview of cloud computing, characterstic, service models, deployment models, security and its challenges and also done a literature survey on various cryptographic techniques. The literature survey has brought in on how the data security and data integrity is maintained on cloud servers Cloud computing has a probable for cost savings to the enterprises but the security risk are also gigantic. Enterprise considering into cloud computing technology as a tactic to cut down on cost and increase profitability should seriously analyser the security risk of cloud computing

7. REFERENCES

[1] Abdul Nasir Khan , M.L. Mat Kiah , Sajjad A, Madani , Atta ur Rehman Khan ,Mazhar Ali,(2013)"Enhanced dynamic credential generation scheme for protection of user identity in cloud computing" Springer Science and Business Media New York .

[2] Bruce Schneier(2005) ," Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)" , Lecture Notes in Computer Science, vol. no. 809, pp 191-204, 08.

[3] DeyanChen,Hong Zhao(2012)," Data Security and Privacy Protection Issues in Cloud Computing, " IEEE International Conference on Computer and Electronics engineering.

[4] Eguro, K.; Venkatesan, R.,(2012), "FPGAs for trusted cloud computing," International Conference on Field Programmable Logic and Applications (FPL), vol., no. 22, pp.63-70, 29-31.

[5] FarzadSabahi,(2009)"Cloud computing Security threats and responses Communication Software and Networks(ICCSN)".In IEEE 3rd International Conference.

[6] Nadeem, A.; Javed, M.Y.(2005), "A performance comparison of data encryption algorithms" International Conference on Information and Communication Technologies , vol. no. 1, pp.84-89, 27-28.

[7] NehaTirthani, GanesanR,(2013),"Data Security in Cloud Architecture Based on diffie Hellman and Elliptical Curve Cryptography" International Association for Cryptologic Research.

[8] NesrineKaaniche,AymenBoudguiga, Maryline Laurent(2013).,"ID Based Cryptography for Secure Cloud Data Storage"Cloud Computing (CLOUD), IEEE Sixth International Conference .

[9] N.Jayapandian, Dr.A.M.J.Md.Zubair Rahman, S.Radhikadevi, M.Koushikaa(2016)." IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16).

[10] P.Mell and T.Grance(2009)., "The NIST Definition of Cloud Computing.,"National institute of standards and Technology,Vol.53,no.6,p.50,[Online].Available:http://csrc.nist.gov/groups/SNS/cloud computing/clouddefv15.doc.

[11] Priyanka Ora, Dr.P.R.Pal.,(2015).," Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography" IEEE International Conference on Computer, Communication and Control .

[12] Ramesh, A.; Suruliandi, A(2013)., "Performance analysis of encryption algorithms for Information Security," International Conference on Circuits, Power and Computing Technologies, vol., no. 2, pp.840-844, 20-21.

[13] R. Velumadhava Raoa,, K. Selvamani,(2015).,"Data Security Challenges and Its Solutions in Cloud Computing "International Conference on Intelligent Computing, Communication & Convergence

[14] Viney Pal Bansal,sandeep singh(2015).," A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs" RAECS UIET Panjab University Chandigarh 21-22nd

[15] Yellamma, P.; Narasimham, C.; Sreenivas, V(2013)., "Data security in cloud using RSA," International Conference on Computing, Communications and Networking Technologies, vol. no. 4, pp.1-6, 4-6.