Secure Data in Cloud Computing using Cryptographic Technique

Rakesh Kumar ER
Asst. Prof. & Head
Computer Science and Engineering,
SAMS College of Engineering and Technology, Chennai, INDIA
rakeshkumarer@gmail.com

Abstract- The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspects refers to security. while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. Scope of modern cryptography also includes techniques and protocols to achieve authentication, non-repudiation, and integrity as objectives. In this paper, we present the opportunities for cryptography to address some of these security challenges in cloud computing.

Key words: Cloud Computing, Resources, Security issues, Cryptography, Non-Repudiation, Integrity

---

I. INTRODUCTION

There have been many techniques of storing data on server storage. Such data storages provided by cloud service providers have to ensure client about Confidentiality, Integrity and Availability of data. Confidentiality refers to keeping data private. Privacy is of importance as data leaves the borders of the owner .Confidentiality is supported by technical tools such as encryption and access control, as well as legal protection. Integrity is a degree of confidence that what data is supposed to be in cloud, what is actually there, and is protected against accidental or intentional alteration without authorization. Availability means being able to use the system as anticipated by cloud user. Cloud technologies can increase availability through widespread internet -enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement [1].

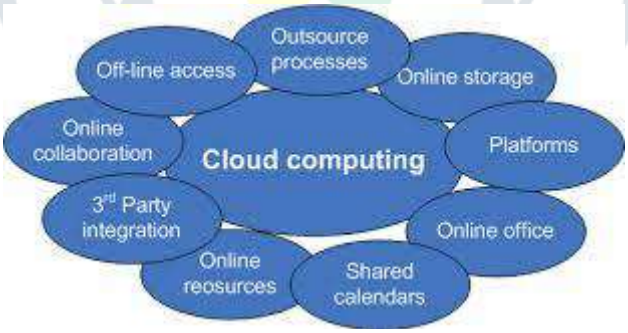

Fig.1: Cloud Computing Standards [3]

Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose taxonomy of security in cloud computing, giving an overview of the current status of security in this emerging technology [1]. Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user [2].

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting your data on to a third party who is providing cloud services is an issue. Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same

physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems.

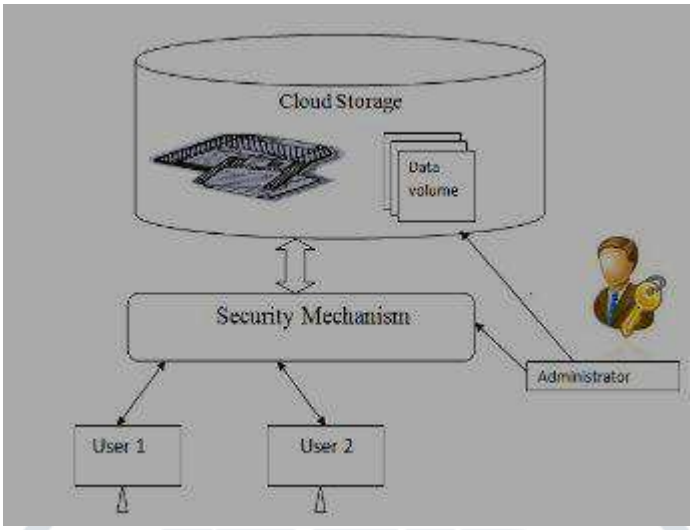

Fig. 2: Security Mechanism in Cloud Environment [4]

II. SECURITY ISSUES IN CLOUD COMPUTING

Cloud Computing or software as a service (SaaS) has brought a huge difference in the ways in which business is done today. As we know, Cloud Computing is a service through which you can avail shared resources, software and information on your computer or other devices via the Internet. This means that you can access the information you want any time, expense your claims on the go, save time on tedious reporting, claims settlement and much more [3]. **Why to concern about security issues in cloud computing?** While the cloud may be flexible and cost-efficient, a lack of data safeguards and compliance standards makes security the largest hurdle to leap. Together with the benefits, we can point on the cloud's weakness points such as system complexities build from shared multitenant layers and it is a fact that hackers know where that data stored exactly. With cloud computing, a task that can take several days to run on a single computer will take only minutes to accomplish on a cluster of hundreds virtual machines. Because cryptography is used widely in authentication, data confidentiality and integrity, and other security mechanisms, these mechanisms become, in effect, less effective with the availability of cryptographic key cracking cloud services.

Fig.3: Security concerns in cloud computing [5]

Data protection The data isolation is one of the major security issues that are raised by potential SaaS users and customers. Data isolation basically means that a specific subscriber (user) will not be able to browse to other tenants' data using the shared environments. Data protection includes also strict procedures when storage is moved or backups are kept. Data must be secured and encrypted while at rest, in transit or in use. Standards for communications protocols and public key certificates allow data transfers to be protected using cryptography.

Identity and Access Management Data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern. There are today many initiatives and startups that deliver tools for access management and user provisioning for SaaS systems.

III. SECURE DATA IN CLOUD

Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide confidentiality. Cryptographic systems can provide one or more of the following four services. It is important to distinguish between these, as some algorithms are more suited to particular tasks, but not to others. When analyzing your requirements and risks, you need to decide which of these four functions should be used to protect your data [6].

- Authentication: the origin of a message can be verified.
- Integrity: proof that the contents of a message have not been changed since it was sent.
- Non-repudiation: the sender of a message cannot deny sending the message.

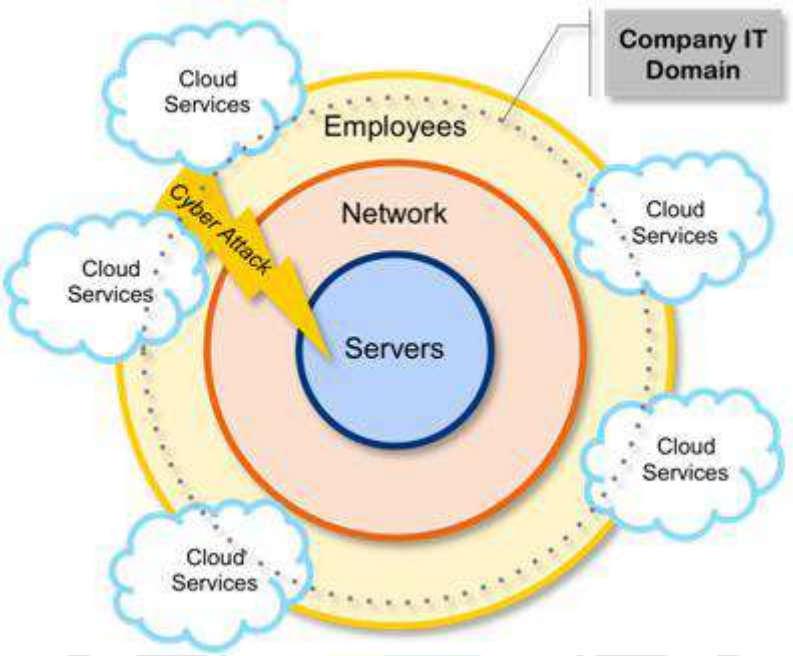

Fig.4: Providing data security to cloud using Cryptography algorithms [7]

IV. RSA PUBLIC - KEY ALGORITHM

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data [7]. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, hereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only. RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

V. CONCLUSION

Finally we conclude that Security and Privacy are the major issues that are needed to be countered, efforts are being made to develop many efficient System That can Provide Security and privacy at the user level and maintain the trust and intellectual property rights of the user. Cloud computing is one among the better way to store and access data with confidentiality, integrity and authentication properties. Privacy and security are the key issue for cloud storage. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private key encryption to hide the sensitive data of users, and

cipher text retrieval. Data is encrypted before uploading to server storage, so message confidentiality is preserved. Our method States Encryption is one such method that can provide peace of mind to user and if the user have control over encryption and decryptions of data that will boost consumer confidence and attract more people to cloud platform.

REFERENCES

[1] H S Venkatesh Prasad, Madhu B K, Lokesha V, *FMKMC College, Madikeri. Coorg, Karnataka*, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 7, September – 2012.

[2] Journal of Theoretical and Applied Information Technology, www.jatit.org

[3] www.bangalore.post2find.com

[4] Yogesh Sharma, DCSA, Kurukshetra University, India, Volume 3, Issue 5, May 2013, International Journal of Advanced Research in Computer Science and Software Engineering.

[5] http://iamondemand.com/blog/the-cloud-security

[6] http://searchsecurity.techtarget.com/definition/encryption

[7] http://www.cloudentr.com/latest-resources/blog/it-pros-speak-top-3-priorities-for-your-it-security-budget-in-2013

AUTHOR DETAILS

Rakesh Kumar ER was born in Kanyakumari District, Tamil Nadu, India in 1985. He obtained his B.Sc., M.Sc. M.E. M.Phil. Degrees in Computer Science in the years 2005, 2007, 2010 and 2012, M.B.A Degree in Human Resources in the year of 2013 respectively. He has more than 7 years of teaching experience. He has presented 5 research papers in various national and international conferences. He has also published more than 15 research papers in reputed national and international journals. He has guided several UG and PG students for their project work. His area of interest is Network Security and Wireless Sensor Networks. Currently, he is with SAMS College of Engg. & Tech, Chennai, India, as Asst. Prof and Head of the Department of Computer Science and Engineering.