Volume 4, Issue V, May 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Security in Cloud Computing

Archana Sood[1], Kanika Gulati[2]

[1]MCA, Panjab University, [2]MCA, M.Tech., KUK
[1]soodarchana2@gmail.com, [2]kanika.silki@gmail.com

Abstract*: The data produced by the enterprises that need to be stored and utilized such as emails, personal health records, photo albums, tax documents, financial transactions, etc. is rapidly increasing; data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. Cloud computing deliver the computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Cloud service providers must have a viable way to protect their client's data, especially from unauthorized users. But for data privacy protection and data retrieval control, service provider must provide authentication for valid user otherwise security reduce and cloud system may collapse. This paper mainly focus on core secured cloud storage services i.e. Cryptography to provide cryptographic techniques for securing data and computation in a cloud environment.*

Keywords: *Cloud Computing, Data security issues, Cloud security*

1. INTRODUCTION

Cloud computing is a buzzword that means different things to different people. Cloud computing is a computing model that is driven by economies of scale and is distributed on large scale. Cloud architectures are developed according to latest and urgent demands. That is, the resources are dynamically provided to a user as per his request and taken back after the job is done. Cloud computing is a service pool which includes the hardware and operating system infrastructure, the formation of systems management software, system and platform, and virtualization components.

Cloud computing introduces new security challenges as client can't fully trust cloud providers. Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. Cryptography in cloud computing depends on a secure cloud computing architecture. Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used.

2. DATA SECURITY ISSUES IN THE CLOUD

Security has always been the main issue for IT Executives when it comes to cloud computing and its adaptation. The security challenges for cloud computing approach are somewhat dynamic and vast. Some of the security issues are as follows:

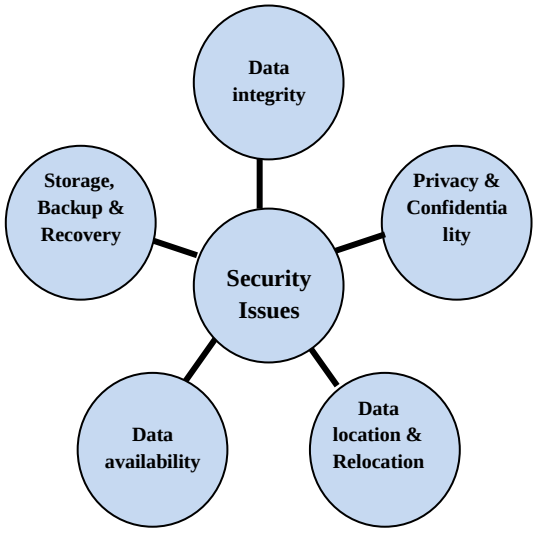

Figure 1: Security issues in cloud computing

***2.1 Privacy and Confidentiality*:**

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. The cloud seeker should be assured that data hosted on the cloud will be confidential.

2.2 Data integrity:

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point.

2.3 Data location and Relocation:

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information.

2.4 Data Availability:

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

2.5 Storage, Backup and Recovery:

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.

In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

3. SECURITY IN CLOUD COMPUTING

Cloud computing is aggregation of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. For example, browser based attacks, denial of service attacks and network intrusion became carry over risks into cloud computing world. The benefits of using cloud computing are very well known and several of the benefits are outlined above. In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption.

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in research work are as follows;

3.1 Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure.

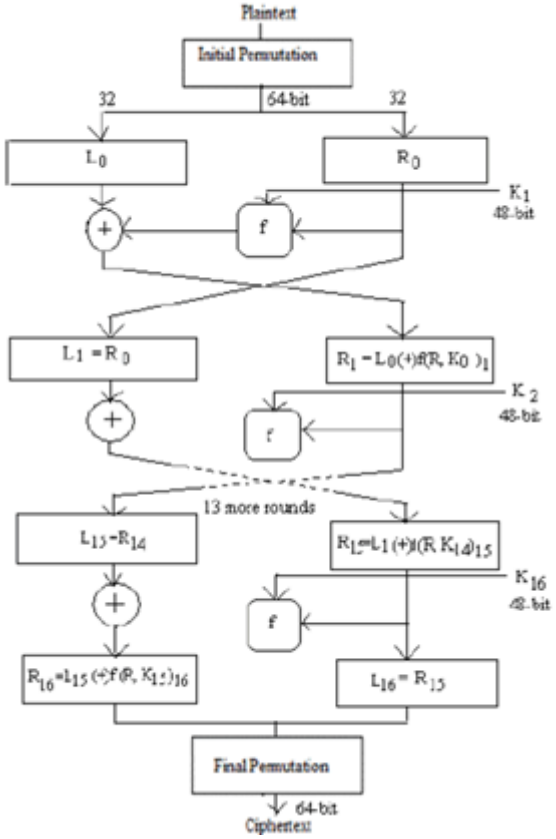

Figure 2: DES Algorithm

DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds. Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text.

3.2 RSA 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. 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

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

known to all, whereas 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: Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.
2. Encryption: Encryption is the process of converting original plain text (data) into cipher text (data).
3. Decryption: Decryption is the process of converting the cipher text (data) to the original plain text (data).

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 3: RSA Algorithm

4. CONCLUSION

In this paper, we review the gold plating technique and effect of gold plating on the system software and how the extra features which are added by the developer to get the extra credit effects the software performance. In this paper, we also propose a new approach in which we develop the new tool which checks the effect of gold plating on the neural network systems like face recognition, voice recognition etc. They had taken 15 inputs and 5 outputs on the basis of this assumption they had analysis that which factor greatly degrades the performance of the system which are added by developer and are not specified in the requirements analysis.

In our future work, we work on the implementation of the new tool which checks the effect of gold plating on the neural network systems.

References

[1] **AL. Jeeva, Dr. V. Palanisamy and K. Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.30333037, May-Jun 2012.**

[2] **Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.**

[3] **Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.**

[4] **Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847), Volume 3 Issue 3, pp.171-176, March 2014.**

[5] **Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3 Issue 5, pp.571-575, May 2013**

[6] **L. M. Kaufman, "Data security in the world of cloud computing, "IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.**

[7] **S C Rachana, Dr. H S Guruprasad, "Emerging Security Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3 Issue 2, pp.485-490, March 2014.**

[8] **Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication, NIST SP - 800144 ,80 pp., 2011.**

[9] **Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2, pp.831-835, October 2012.**

[10] **Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013**

[11] **Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010.**