Journal of Engineering Design and Analysis
Volume 3, Issue 2 - 2020, Pg. No. 98-100
Peer Reviewed Journal

ADVANCED RESEARCH PUBLICATIONS

Article

Cloud Security and Privacy – A Cryptographic Approach

Prasanta Kumar Bal

Department of Computer Science and Engineering, Gandhi Institute for Technological Advancement, Bhubaneswar, India.

INFO

E-mail Id:
prasantakbal9@gmail.com
Orcid Id:
https://orcid.org/0000-0003-3779-277X

How to cite this article:
Bal PK. Cloud Security and Privacy – A Cryptographic Approach. *J Engr Desg Anal* 2020; 3(2): 98-100.

Date of Submission: 2020-11-27
Date of Acceptance: 2020-12-20

ABSTRACT

Recently, cloud computing emerged as the leading technology for delivering reliable, secure, fault-tolerant, sustainable, and scalable computational services, which are presented as Software, Infrastructure, or Platform as services (SaaS, IaaS, PaaS). Moreover, these services may be offered in private data centers (private clouds), may be commercially offered for clients (public clouds) or yet it is possible that both public and private clouds are combined in hybrid clouds. As the user data is stored in some undisclosed location upon which the user does not have any control, it creates the atmosphere of vulnerability of security and privacy of user data. In this paper we have highlighted some of the security and privacy issues in cloud and the role of cryptography in mitigating those issues.

Keywords: Cloud Computing, Security, Privacy, Cryptography

Introduction

Cloud computing has been a paradigm shift in the information technology domain,[1] that delivers highly scalable distributed computing platforms in which computational resources are offered as a service.[2] Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing provides a facility that enable large scale controlled sharing and interoperation among resources that are dispersedly owned and managed.[3] The cloud model is depicted in Figure 1, as follows.

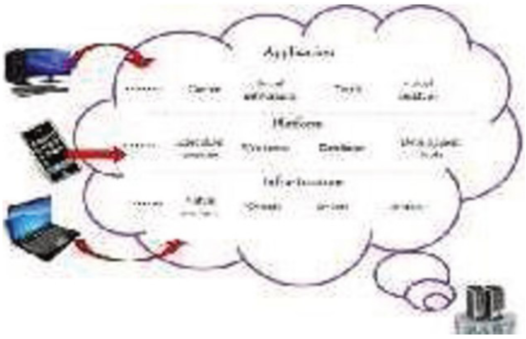

Figure 1.Cloud Model

Since user data is stored at distributed locations and user does not have any control over cloud storage, the cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange. Cryptography in the cloud allows for securing critical data beyond your corporate IT environment, where that data is no longer under your control. In the cloud, we don't have the luxury of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key. Moving away from that, when we want to talk of security of data in the cloud, it is of dire importance for us to approach it in a proactive manner. Data moving or to the cloud exists in two forms. We have data in motion and data at rest. Data in motion must be protected always through encryption, notwithstanding that we cannot assume that data at rest wi 11 be safe always.

Literature Review

Brian Hay et al.[4] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that. the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storaae and do the computation on encrypted data which is called as homomorphic encryption.[5] New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data.

Kevin Curran et al.[6] mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems by storing their data in Cloud Storage they will befacedwtth the task of seriously reassessing their current security strategy.

Randeep Kaur et al.[7] mentions some of the notable challenges associated wilh cloud Storage. The challenges are Security, Privacy and Lack of Standards which slow down services in the cloud.

Weikai Wang et al.[10] have focused on two sources of data, one was intrusion detection of external non-self-samples and another was security calculation of self-samples.

Rashmi Nigoti et al.[8] defines some privacy and security-related issues that are believed to have long-term significance for cloud storage. They proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form morejustifiable and financially beneficial security policy decisions.

Summary on Literature Review

A number of researchers have discussed the security challenges that are raised by cloud computing. It is clear that the security issue has played the most important role in hindering the acceptance of Cloud Computing. For security purpose of cloud storage various encryption techniques are being analyzed by researchers. As discussed in survey there are many security techniques which are currently applied to cloud storage. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level inthe cloud storage.

Various Cryptographic Algorithms

Data Encryption Standard (DES)

The DES algorithm is the most popular security algorithm. It's a symmetric algorithm, which means that the same keys are used to encrypt/ decrypt sensitive data. Key length is 8 byte(64 bit). So,to encrypt/ decrypt data, the DES algorithm uses an 8- byte key, but 1 byte (8 bit) for parity checking. It's a block cipher algorithm-that's why the data block size of DES algorithm is 64 bit. To encrypt/ decrypt data, the DES algorithm uses the Feistel structure. So, it uses some round to encrypt/ decrypt data. Though data block size is 64 bit, the number of rounds will be 16 rounds. So, tt will use different sub keys for each round. So the number of subkeys will be 16 subkeys. For more info on the process of finding sub keys.

Advanced Encryption Standard (AES)

AES is an iterative rather than Feistelcipher. It is based on 'substitution-permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged infour columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The features of AES are as follows -

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

RSA

RSA was first publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology, though the 1973 creation of a public key algorithm by British mathematician Clifford Cocks was kept classified by the U.K.'s GCHQ until 1997. Public key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys - one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method to assure the confidentiality, integrity, authentictty and non repudiation of electronic communications and data storage.

Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows specific types of computations to be executed on cipher texts and obtain an encrypted result that is the cipher text of the result of operations performed on the plain text. Applying the standard encryption methods presents a dilemma : If the data is stored unencrypted, it can reveal sensitive information to the storage/ database service provider. On the other hand, if it is encrypted, it is impossible for the provider to operate on it. If data are encrypted, then answering even a simple counting query (for example, the number of records or files that contain a certain keyword) would typically require downloading and decrypting the entire database content. A homomorphic encryption allows a user to manipulate without needing to decrypt it first. An example of homomorphic encryption is the RSA algorithm. Other examples of homomorphic encryption schemes are the ECC encryption, the El Gamal cryptosystem. Ryan Hayward and Chia Chu Chiang[9] have presented an implementation of a processing dispatcher which takes an iterative set of operations on Fully Homomorphism Encryption (FHE) on the encrypted data and splits them between a numbers of processing engines.

Conclusion

In this paper, the importance of cloud security and data privacy is very briefly presented. Some of the existing methodologies to provide cloud security is also presented in section 2. To enhance cloud security and privciy we can use some existing cryptographic algorithms like AES, DES, RSA etc. To further enhance security more than one algorithm can be applied in a cascading manner.

References

1. Kantarcioglu M, Bensoussan A, Sing R. Impact of Security Risks on Cloud Computing Adoption. In proceeding of IEEE International Conference on Communication. *Control and Computing* 2011; 670-674.
2. Mohemed Almorsy, John Grundy and Amani S. Ibrahim. Collaboration-Based Cloud Computing Security Management Framework. In proceeding of IEEE International Conference on Cloud Computing. 2011; 364-371.
3. Shaikh FB, Haider S. Security Threats in Cloud Computing. In proceeding of IEEE International Conference on Internet Technology and Secured Transactions. 2011; 214-219.
4. Hay B, Nance K, Bishop M. Storm Clouds Rising: Security Challenges for laaS Cloud Computing. Proceedings of the 44th Hawaii International Conference on System ciences. 2011; 1-7.
5. Maha TEBAA, Satd EL HAJJI, Abdellatif EL GHAZI. Homomorphic Encryption Applied to the Cloud Computing Security. *World Congress on Engineering* 2012; 1.
6. Curran K, Carlin S, Adams M. Security issues in cloud computing. *Elixir Network Engg* 2011; 38: 4069-4072.
7. Kaur R, Kinger S. Analysis of Security Algorithms in Cloud Computing. *International Journal of Application or Innovation in Engineering & Management* 2014; 3: 171-117.
8. Nigoti R, Jhuria M, Singh S. A Survey of Cryptographic algorithms for Cloud Computing. *International Journal of Emerging Technologies in Computational and Applied Sciences* 2013; 4: 141-146.
9. Hayward R, Chiang CC. Parallelizing fully homomorphic encryption for a cloud environment. *Journal of applied research and technology* 2015; 13(2): 245-252.
10. Wang WJ, Ren L, Chen L et al. Intrusion Detection and Security Calculation in Industrial Cloud Storage based on an Improved Dynamic Immune Algorithm. Information Sciences. 2018.