A Review on Encryption Techniques to Secure a Cloud

Ramandeep Kaur[1], Ashish Verma[2]

[1]M.Tech Student, Department of Computer Science, Punjabi University Patiala[1]

[2]Assistant Professor, Department of Computer Science, SSIET, PTU, Dera Bassi[2]

Abstract: ***Cloud computing brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers which is not within the same trusted domain as data owners. Homomorphic encryption is a form of security technique which allows specific types of computations to be carried out on encrypted data (text) and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. To keep sensitive user data confidential against untrusted servers, cryptographic methods are used by disclosing data decryption keys only to authorized users. There are various cryptographic methods are used by disclosing data decryption keys only to authorized users To keep sensitive user data confidential against untrusted servers. In this paper, a review on different encryption techniques is done to protect cloud data. [10]***

Keywords: Homomorphic encryption, cloud computing, Unpadded RSA, security, AES

1. Introduction

A. Cloud Computing

Computing is calculating arithmetic processing by the use of computers. Cloud computing is the delivery of computing. It is used as a service which can be SaaS, PaaS, IaaS. The shared resources, software, and other information are provided to computers over a network. It also provides storage services that do not need end-user knowledge of the physical location and configuration of the system that delivers the services.

Cloud computing is similar to grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

Cloud computing shares different characteristics with following:

- Client–server model — Client–server computing uses software architecture of client server model to any distributed application that distinguishes between service providers (servers) and service requestors (clients).
- Grid computing — "A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."
- Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: census; industry and consumer statistics; police and secret intelligence services; enterprise resource planning; and financial transaction processing.
- Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."
- Peer-to-peer — A distributed architecture without the need for central coordination. Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).

B. Cloud Computing Security

Cloud security is sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

The encryption methods are

1. Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form.
2. A garbled circuit, a technique developed in the mid-1980s and widely used in cryptography. A garbled circuit lets a user decrypt the result of one cryptographically protected operation on one cryptographically protected data item—say, "Is this record a match?" The problem is that, if the garbled circuit is used on a second data item—"How about this record?"—the security breaks.
3. Functional-encryption scheme by fitting together several existing schemes, each of which has vital attributes of functional encryption

C. Homomorphic Encryption

There are several efficient, partially homomorphic cryptosystems, and a number of fully homomorphic, but less efficient cryptosystems. Although a cryptosystem which is unintentionally homomorphic can be subject to attacks on this basis, if treated carefully homomorphism can also be used to perform computations securely. In the following examples, the notation $\varepsilon(x)$ is used to denote the encryption of the message x.

1.1 Unpadded RSA

If the RSA public key is modulus m and exponent e, then the encryption of a message $\mathfrak{X}$is given by $\varepsilon(x) = x^e \bmod m$. The homomorphic property is then

$$\varepsilon(x_1).\varepsilon(x_2) = x_1^e x_2^e \bmod m = (x_1 x_2)^e \bmod m = \varepsilon(x_1.x_2)$$

1.2 ElGamal

It is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. This encryption consists of three components:

1. The key generator
2. The encryption algorithm
3. The decryption algorithm.

ElGamal encryption is unconditionally malleable, and therefore is not secure under chosen ciphertext attack. Since this encryption uses randomness in encryption which means that a single plaintext can be encrypted to many possible ciphertexts. So this scheme has probabilistic feature.

1.3 Goldwasser–Micali

GM has the distinction of being the first probabilistic public-key encryption scheme which is provably secure under standard cryptographic assumptions. However, it is not an efficient cryptosystem, as ciphertexts may be several hundred times larger than the initial plaintext.

GM consists of three algorithms:

1. A probabilistic key generation algorithm which produces a public and a private key
2. A probabilistic encryption algorithm
3. A deterministic decryption algorithm.

The scheme relies on deciding whether a given value *x* is a square mod *N*, given the factorization (*p*, *q*) of *N*. This can be accomplished using the following procedure:

1. Compute $x_p = x \bmod p$, $x_q = x \bmod q$.
2. If $x_p^{(p-1)/2} = 1(\bmod p)$ and $x_q^{(q--1)/2} = 1(\bmod q)$

1.4 Benaloh Cryptosystem

It is an extension of the GM created in 1994. The main improvement of this over GM is that in GM each bit is encrypted individually but in Benaloh, longer blocks of data can be encrypted at once. This scheme works in the group (Z/nZ)* where *n* is a product of two large primes. This scheme is homomorphic and hence malleable.

1.5 Paillier Cryptosystem

It is a also the probabilistic asymmetric algorithm for public key cryptography. The problem of computing n^{th} residue classes is believed to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based. The scheme is an additive homomorphic cryptosystem; this means that, given only the public-key and the encryption of $m_1$and m_2, one can compute the encryption of $m_1+ m_2$.

2. Literature Survey

S. Singla et al. [1] discussed that cloud computing is a technology where users can remotely store their data into the cloud to enjoy high quality application and services. Cloud is being the most vulnerable next generation architecture. It consists of two major design elements i.e. the Cloud Service Provider (CSP) and the Client. No doubt the cloud computing is promising and efficient, but still there are many challenges for data privacy remotely store their data into the cloud to enjoy high quality application and services and security. This paper explores the security of data at rest as well as security of data while moving.

S. Singla et al. [2] stated that cloud computing emerges as a new computing paradigm. It provides reliable, customized and quality of service guaranteed dynamic computing environments for clients. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. In a cloud computing environment, the data as well as the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. The one of the major issues in cloud computing is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with the methods of providing security by data encryption and to ensure that unauthorized intruder can't access your file or data in cloud.

S. Marium et al. [3] discussed about cloud computing. It is emerging approach because of high availability, efficient cost and performance. In Cloud Computing, service providers will provide the storage for data along with services. But due to the lack of proper security policies, many business companies are reluctant to adopt the Cloud Computing technology. This paper has been written to highlight cloud security and privacy issues. The research is mainly focus on service provider’s side security. They must protect their client data by unauthorized access, modification or miss use, denial of services and repudiation. To ensure the security of the client data in the cloud, they purposed the implementation of the Extensible Authentication Protocol through three way hand shake with RSA. According to their study, EAP-CHAP and RSA are best solution to provide to any type of Cloud customer.

S. Ravindran et al. [4] had described what cloud computing is and how can be benefitted from it. As every technology has a flaw so does cloud computing. Since security is a major concern in cloud computing as data is stored in a cloud and it becomes very difficult to perform operations on the encrypted data, hence homomorphic encryption can be used to secure data and also perform operations on it. The RSA cryptosystem and the ElGamal cryptosystem is discussed and also described how they can be used to perform calculations. Currently the homomorphic cryptosystems can be used to perform only certain operations like addition, subtraction, multiplication, XOR and exponentiation. These algorithms can be used to enhance and to perform various other operations. With homomorphic encryption, a company could encrypt its entire database of e-mails and upload it to a cloud. Then it could use the cloud-stored data as desired—for example, to search the database to understand how its workers collaborate. The results would be downloaded and decrypted without ever exposing the details of a single e-mail.

M. Gomathisankaran et al. [5] proposed a novel homomorphic encryption scheme using RNS for cloud computing. Many research issues which are involved in HORNS (homomorphic encryption function using RNS) have been identified and proposed solutions for some of these issues. Also a homomorphic encryption scheme using Residue Number System (RNS) is proposed. In this scheme, a secret is split into multiple shares on which computations can be performed independently. Security is enhanced by not allowing the independent clouds to collude. Efficiency is achieved through the use of smaller shares.

J. Sen [6] discussed that cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand (Leighton, 2009). According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012). However, as the shape of the cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenges. Here description of various services and deployment models of cloud computing and identify major challenges. In particular, three critical challenges: regulatory, security and privacy issues in cloud computing are also discussed. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment.

G. Thomas et. al. [7] summarized that cloud computing has been envisioned as the next generation architecture of IT Enterprise. This concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In order for this to become reality, however, there are still some challenges to be solved. One of the most important among these are security and trust issues, since the user’s data has to be released to the Cloud and thus leaves the protection sphere of the data owner. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, 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. Security is to save data from danger and vulnerability. Various security issues and some of their solution are explained and are concentrating mainly on public cloud security issues and their solutions. Data should always be encrypted when stored (using separate symmetric encryption keys) and transmitted. If this is implemented appropriately, even if another tenant can access the data, all that will appear is gibberish. So a method is proposed such that we are encrypting the whole data along with the cryptographic key.

D. Meng et. al. [8] discussed the cloud computing services, and the issue of data security is one of the most important problems to be solved. Today's network construction, safety products, and encryption protocol have been protected the safety of data transmission. Data storage security can be solved through technical means in the design stage of cloud services, such as redundancy, parity, user authentication and access control; Data management security involves many aspects, the first is to improve the relevant laws and regulations as soon as possible, and the second is compatible with data between cloud computing service providers to ensure that users can seamlessly pan data, and service providers should establish a rapid and effective disaster recovery mechanisms to guarantee the availability of the data. At present, in a short period of time, the cloud computing cannot completely replace traditional computing. It is still not being fully accepted that to manage data by a third party, especially for large enterprises and government departments. In order to take full advantages of cloud computing characteristics, some large enterprises with strong economic and technological strength have begun to try to establish their own cloud computing platforms, such as China Mobile BigCloud, but the Chinese government is still in a wait-and see. It is foreseeable that in the near future, the average user will not shift entirely to the cloud computing model, firstly, because of the aforementioned security reasons, and secondly, they also hoard some computing devices, turning to cloud computing means to abandon existing investments. But some businesses with low level data confidentiality or even completely open can use commercial cloud computing model, such as some entertainment sites, SNS sites as well as public service platform, such as network library and public information release platform and so on. In addition, enterprises can also try to separate from the business, one part of the businesses involves confidential information are still running in the local network in accordance with the original mode and the other part complete by the cloud computing platform.

Y. Lee et. al. [9] discussed that internet traffic measurement and analysis have been usually performed on a high performance server that collects and examines packet or flow traces. However, when monitor a large volume of traffic data for detailed statistics, a long period or a large-scale network, it is not easy to handle large volume of traffic data with a single server. One of the common ways to reduce a large volume of continuously monitored traffic data are packet sampling or flow aggregation that results in coarse traffic statistics. As distributed parallel processing schemes have been recently developed due to the cloud computing platform and the cluster file system, they could be usefully applied to analyzing big traffic data. Thus, in this paper, an Internet flow analysis method based on the MapReduce software framework of the cloud computing platform for a large-scale network is proposed. From the experiments with an open-source MapReduce system, Hadoop, it was verified that the MapReduce-based flow analysis method improve the flow statistics computation time by 72%, when compared with the popular flow data processing tool, flow-tools, on a single host. In addition, MapReduce-based programs complete the flow analysis job against a single node failure.

3. Conclusion

In this paper, we have discussed the paradigm of encryption in cloud computing. Various types of homomorphic encryption and research studies are discussed. The history of partially homomorphic encryption is discussed. Research findings of different authors have been discussed and the future research scope is discussed.

References

[1] S. Singla & J. Singh, “Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm,” Global Journal of Computer Science and Technology Software & Data Engineering ,Volume 13 Issue 5 Version 1.0 Year 2013.

[2] S. Singla & J. Singh, “Implementing Cloud Data Security by Encryption using Rijndael Algorithm,” Global Journal of Computer Science and Technology Software & Data Engineering ,Volume 13 Issue 5 Version 1.0 Year 2013.

[3] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham, M. A. Mehmood, “Implementation of Eap with RSA for Enhancing The Security of Cloud Computing,” IJBAS, 1(3), pp. 177-183, 2012.

[4] S. Ravindran, P. Kalpana, “Data Storage Security Using Partially Homomorphic Encryption in a Cloud,” International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3 Issue 4, pp. 603-606, April 2013.

[5] M. Gomathisankaran, A. Tyagi, K. Namuduri, “HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System," 45th Annual Conference on Information Sciences and Systems, USA, 2011.

[6] J. Sen, “Security & Privacy Issues in Cloud Computing” Innovation Labs, TCS, IGI Global, USA, 2013.

[7] G. Thomas & P. J. V, “Cloud Computing Security Using Encryption Technique” CoRR abs/1310.8392 (2013).

[8] D. Meng, “Data Security in Cloud Computing”, ICSSE, pp. 810- 813, 2013.

[9] Y. Lee, W. Kang, H. Son, “An Internet Traffic Analysis Method with MapReduce”, Network Operations and Management Symposium Workshop, IEEE/IFIP 2010.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.