Study on Cryptographic Algorithms for Cloud Data Security

Hnin Mya Aye, Si Si Mar Win, Thin Thin Soe
University of Computer Studies, Mandalay
hninmyaaye26@ gmail.com, sisimarwin@gmail.com, thinthinsoe.cumdy@ gmail.com

Abstract

Cloud computing is a distributed computing paradigm in which computing resources, software, applications, information, and infrastructures are dynamically offered as services over the internet. Since distributed services are shared via the open network, the security of cloud data is required to be considered as a major issue in the cloud computing environment. Therefore, there is a need to protect cloud data against unauthorized accesses, or denial of service, modification, etc. To provide secure cloud data, cryptography can play as a technical control to address security issues undergone in cloud computing. In this paper, we have studied some of existing, well-known cryptographic algorithms that are adoptable to provide better security of data in cloud computing.

Keywords: *cloud computing, security issues, cryptography, encryption, decryption*

1. Introduction

Cloud computing is the fastest evolving information technology in the modern computing area. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [13]. It has the potential to transform a data center from a capital-intensive set up to a variable priced environment. With the increasing development of this computing technology, the cost of computation, application hosting, content storage and delivery are significantly reduced [18].

Cloud computing deployment models can be classified as different forms depending on customers' needs such as public cloud, private cloud, community cloud and hybrid cloud. **A public cloud** is a kind of cloud which can be accessed by any subscriber with an internet connection and access to the cloud space. **A private cloud** is one which can be created for a specific group or organization and limits access to just that group. **A community cloud** is a type of cloud that is shared among two or more organizations that have similar cloud requirements. **A hybrid cloud** is a hybrid form which is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community [1].

Cloud service models describe how cloud services are made available to clients. There are three types of service models in cloud computing environment including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The **SaaS** model provides ready online software solutions. SaaS application examples include online mail and social media platforms. The **PaaS** model delivers a pre-built application platform to the client; clients do not need to spend time building underlying infrastructure for their applications. Google AppEngine is a popular PaaS provider. The **IaaS** model also provides infrastructure components to clients. Amazon Web Service is one of largest IaaS providers [5].

In cloud computing, resources are shared and pooled to serve multiple customers using a multi-tenant model, with different physical and virtual resources. At the same time, trust, security, and privacy issues are major obstacles in cloud computing adoption [12]. Therefore, cloud service providers must be ensure their data to be secure whether any type of cloud or any service model is applied.

Cryptography has evolved from the earliest forms of secret writing to current era of computationally secure protocols, addressing range of security issues. In modern age, cryptography is not only about encryption, but it has larger objective of ensuring data protection from adversary's activities. Therefore, cryptography is one of the key contributors to provide technical controls to deal with such challenges and enhance confidence of cloud service customers [12]. In this paper, we have studied existing cryptographic techniques to address these issues.

2. Related Works

Anjana Chaudhary, Ravinder Thakur, and Manissh Manna have provided a solution to protect various attacks that can be undergone in accessing

cloud services [2]. In this framework, the Third Party Auditor is assigned to check the user is an authorized person or not on behalf of the data owner to ensure the security of cloud data storage. If the user is an authorized person, data is transferred to the user in encrypted form. In data encryption, RSA is applied.

Miss. Ashwini A. Dongre, Mr. Falesh M. Shelke, and Mr. Pravin D. Sonihave investigated a protocol for private cloud, in which the cluster digital signature is generated [9]. Diffie Hellman algorithmic rule is used to produce the secret key for sharing between cluster manager and cloud provider. Within the cluster, the cluster manager selects the general public key and generates personal key (used for signature) for the member with relation of RSA algorithmic rule. After verifying the member's signature, the cluster manager sends the encrypted member's data to the cloud provider. And then, the cloud supplier decrypts and stores data in the private cloud. In the future, this protocol can be re-modified with member's freedom to send and receive information directly in the cloud, but traceability of user by the cluster manager must be kept at constant time.

Dr. L. Arockiam and S. Monikanda have proposed a hybrid symmetric encryption algorithm by integrating substitution cipher and transposition cipher for secure storage of cloud user data [4]. Both substitution and transposition techniques have used alphabet for cipher text. In encryption, the plain text is converted into corresponding ASCII code value of each alphabet. By using square matrix (S x S, where the square of S is greater than or equal number of characters in plain text), the plain text is permuted. The decryption process is reverse of the encryption.

Geethu, Prem Jose V and P.Afsar have proposed a method in which the key and the data have to be encrypted before transmission [6]. For this encryption, RSA algorithm or any other algorithm can be used. This method can move far away from a chance of theft or getting the key by another person and imitating like the owner.

Neha Tirthan and Ganesan R have proposed a new cloud architecture using Diffie Hellmann Key Exchange and Elliptic Curve Cryptography to be better security and reliability on the cloud servers [11]. In this architecture, four step procedures are required for ensuring authenticity of user. The first step is to establish the connection, the second is account creation, the third is authentication and the last one is data exchange. Elliptic Curve Cryptography is used for data encryption in data exchange phase. Diffie Hellman protocol is used for better establishment of connections.

3. Data Security Issues in the Cloud

Security is a major challenge in cloud computing because of its nature of outsourced computing. Different nodes in the cloud environment may be controlled or administered by different entrusted parties. So, cloud data could be vulnerable by attacks from other cloud tenants, malicious insiders or external adversaries. When data owners release control of their data to a cloud environment, they require guarantees that their data are appropriately protected [16]. The chief concern in cloud computing is to provide security by giving customers more trustful services.

The major issues faced by cloud computing can be categorized as follows [19]:

Privacy and Confidentiality: Once the client host data to the cloud, there should be some guarantee that access to that data must be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that is posing potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users for the safety of data. The cloud seeker should be assured that data hosted on the cloud will be confidential.

Data integrity: With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity which is the necessary thing and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

Data Location and Relocation: Cloud computing offers a high degree of data mobility. Consumers of the data 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 the location of it. They may also wish to specify a preferred location for that data to be kept where. This, then, requires a contractual agreement, between the cloud provider and the consumer that data should stay at a particular location or reside on a given known server.

Data Availability: Customer data is normally stored in chunk on different servers often residing in different locations or in different clouds. In such case, data availability becomes a major legitimate issue as the

availability of uninterruptible and seamless provision becomes relatively difficult.

Among these issues, we emphasize on data confidentiality and integrity. Because these two issues are at the top of the security challenges in cloud computing. To overcome these issues, cryptographic based security algorithms can be utilized. Applying these security algorithms is one of the best and most efficient ways to protect secret or sensitive data and to ensure confidentiality and integrity.

4. Cryptography

Cryptography is derived from Greek word in which 'crypto' means "hidden or secret" and 'graphy' means "writing". It is a study of technique for secure communication to maintain information securities such as data integrity, confidentiality, and authentication. It is also an art to transform the messages to make them secure and immune against security attacks.

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 or storage is called **encryption**. The reverse process of getting back the original data from encrypted data is called **decryption**, which restores the original data. There are some goals of cryptography such as authentication, confidentiality, integrity, non-repudiation, and service reliability [3]. To encrypt data at cloud storage, both symmetric-key and asymmetric-key algorithms can be used [14].

4.1. Symmetric-key Algorithms

Symmetric encryption is a cryptographic technique in which encryption and decryption are performed using the same key. It is also referred to as conventional encryption or single-key encryption. There are two requirements for secure use of conventional encryption. The first one is need of a strong encryption algorithm which means that the opponent should be unable to decrypt ciphertext or discover the key even if he or she possesses a number of ciphertexts together with the plaintext that produced each ciphertext. The second one is that sender and receiver must have obtained copies of the secret key in a secure fashion. If someone can discover the key and knows the algorithm, all communication using this key is readable [20].Symmetric-key algorithms used in cloud computing include: Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Blowfish.

Data Encryption Standard (DES) – DES is the most widely used symmetric-key block cipher adopted as Federal Information Processing Standard (FIPS-46) by the National Institute of Standards and Technology (NIST) in January 1977.DES exhibits the classic Feistel structure [20]. The two main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part [3]. At the encryption site, DES takes 64-bit plaintext block as input and produces 64-bit ciphertext block. At the decryption site, it takes 64-bit ciphertext block and reproduce original 64-bit plaintext block. A 56-bit single key is used in both sites.

Advanced Encryption Standard (AES) – AES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 2001. It is also called Rijndael which is the names of the two inventors (Joan Daemen and Vincent Rijmen). It is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware [8]. It is intended to replace DES as the approved standard for a wide range of applications. It does not use a Feistel structure. In AES, all operations are performed on 8-bit bytes, known as state. It uses a fixed block size of 128-bit and a variable key length of 128, 192, or 256 bits: by default 256 is used. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

Blowfish - Blowfish is a symmetric block cipher algorithm designed in 1993 by Bruce Schneier. Blowfish operates on 64-bit data block size. It uses a variable key length from 32 bits up to 448 bits. It is provides a good encryption rate in software and a very secure cipher and to use encryption free of patents and copyrights [3]. It is a 16-round Feistel cipher and uses large key-dependent S-boxes, and highly complex key schedule.

The performance and comparison among DES, AES and Blowfish are measured with various parameters. The block size and key length are measured in terms of bits used. The throughput and power consumption are measured as high and low. The speed is defined in terms of fast, moderate and slow. Table 1 shows the experimental results of DES, AES and Blowfish [15].

Table 1. Comparison among DES, AES and Blowfish

Parameter	DES	AES	Blowfish
Key Length	56 bits	128,192, or 256 bits	32 bits to 448 bits

Throughput	Lower Than AES	Lower than Blowfish	Very high
Power Consump-tion	Higher than AES	Higher than Blowfish	Very low
Speed	Fast	Fast	Fast
Security Against Attacks	Brute force attack	Chosen plain, known plain text	Diction-ary attack

4.2. Asymmetric-key Algorithms

Asymmetric encryption is a cryptographic approach in which encryption and decryption are performed using the different keys. The two keys used for asymmetric encryption are referred to as public key and private key. The public key is used for encryption of data by the sender and the private key is used for decryption of data by the receiver. This type of encryption is also known as public-key encryption. In cloud computing, asymmetric-key algorithms are used to generate keys for encryption [14]. The most common asymmetric-key algorithms for cloud are: RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman Key Exchange.

RSA – RSA is the most widely used public key cryptosystem. It was published in 1978 and stands for Ron Rivest, Adi Shamir, and Leonard Adleman. It is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits [20].

Elliptic Curve Cryptography (ECC) – ECC was proposed by Koblitz and Miller in 1980s. ECC is a public key cryptographic scheme. It uses properties of Elliptic Curves to develop cryptographic algorithms. Security of ECC is based on the intractability of Elliptic Curve Discrete Logarithm Problem. Elliptic Curve Cryptography is defined with help of following parameters as:

$$P = (q,FR,a,b,G,n,h) \quad (1)$$

where q is the prime number that defines curve's form; FR is field representation; a and b are the curve coefficients; G is the base point (Gx, Gy); n is the order of G and h is cofactor co-efficient [11].

Diffie-Hellman Key Exchange–Diffie-Hellman key exchange is the first published public key algorithm by Whitfield Diffie and Martin Hellman in 1976. The aim of this algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages [20]. Finally, this generates an identical key that is computationally difficult to reverse for another party that might have been listening in on sensitive data. The algorithm itself is limited to the exchange of secret values. This algorithm depends on the difficulty of computing discrete logarithms for its effectiveness.

Table 2 shows the experimental results of RSA, ECC and Diffie-Hellman [7][10][15][17].

Table 2. Comparison among RSA, ECC and Diffie-Hellman

Parameter	RSA	ECC	Diffie-Hellman
Key Length	> 1024 bits	Variable key length	Key exchange manage ment
Throughput	Low	Higher than RSA	Lower than RSA
Power Consump-tion	High	Low	Lower than RSA
Speed	Fast	Faster than RSA	Slow
Security Against Attacks	Timing attack	Index-calculus attack	Eaves-dropping

5. Conclusion

Although cloud computing has rapidly become a widely adopted paradigm for delivering services over the internet, it has several security issues varying from network level threats to application level threats. In order to keep the cloud secure, these security issues need to be controlled. The cryptographic techniques can help to address cloud security issues. In this paper, we have studied various cryptographic algorithms that can be used in cloud computing environment. It is found that some amount of work has been done relating with cloud computing security issues and appropriate cryptographic based security algorithms. However, there is still more scopes for future researches of secure data sharing in the cloud.

References

[1] Alexa Huth and James Cebula, "The Basics of Cloud Computing", United States Computer Emergency Readiness Team, Carnegie Mellon University.

[2] Anjana Chaudhary, Ravinder Thakur, and Manissh Manna, "A Review: Data Security Approach in Cloud computing by using RSA Algorithm", *International*

Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782 (Online), Volume 1, Issue 7, December 2013.

[3] Anjula Gupta and Navpreet Kaur Walia, "Cryptography Algorithms: A Review", ISSN: 2321-9939, Volume 2, Issue 2, 2014.

[4] Dr. L. Arockiam and S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", *International Journal of Advanced Research in Computer and Communication Engineering*, ISSN (Print): 2319-5940, ISSN (Online): 2278-1021, Vol. 2, Issue 8, August 2013.

[5] Eugene Gorelik, "Cloud Computing Models", Working Paper CISL# 2013-01, January 2013.

[6] Geethu, Prem Jose V, and P.Afsar, "Cloud Computing Security using Encryption Technique".

[7] Gururaja.H.S, M. Seetha, Anjan K Koundinya, Shashank.A.M and Prashanth.C.A, "Comparative Study and Performance Analysis of Encryption in RSA, ECC and Goldwasser Micali Cryptosystems", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, ISSN 2319 – 4847, Volume 3, Issue 1, January 2014, pp. 111-118.

[8] Leena Khanna and Prof. Anant Jaiswal, "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them", *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 3, Issue 3, March 2013.

[9] Miss. Ashwini A. Dongre, Mr. Falesh M. Shelke, and Mr. Pravin D. Soni, "Clustered Digital Signature for Data Storage Security in Private Cloud", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, ISSN 2319 – 4847, Volume 3, Issue 2, February 2014.

[10] Muhammad Yasir Malik, "Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor'', *ICACT 2010*, National University of Science and Technology (NUST), Pakistan, ISBN 978-89-5519-146-2, February 2010.

[11] Neha Tirthan and Ganesan R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography".

[12] Nitin Singh Chauhan and AshutoshSaxena, "Cryptography and Cloud Security Challenges", CSI Communications, May 2013.

[13] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov), version 15, October 2009.

[14] Rashmi Nigoti, Manoj Jhuria, and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing", *International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)*, ISSN (Print): 2279-0047, ISSN (Online): 2279-0055,4(2), March-May 2013, pp.141-146.

[15] Ritu Tripathi and Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, National Institute of Technical Teachers' Training and Research Bhopal, India, ISSN 2348 – 4853, Volume 1, Issue 6, June 2014, pp. 68-76.

[16] Sophia Yakoubov, Vijay Gadepally, Nabil Schear, Emily Shen, and Arkady Yerukhimovich, "A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud".

[17] Tim Guneysu, Christof Paar and Jan Pelzl, "On the Security of Elliptic Curve Cryptosystems against Attacks with Special-Purpose Hardware", Horst Gortz Institute for IT Security, Ruhr University Bochum, Germany.

[18] Torry Harris, "CLOUD COMPUTING – An Overview", http://www.thbs.com/knowledge-zone/cloud-computing-overview.

[19] Vijendra Rajendra Augustine and Prof. Prabhaker L. Ramteke, "Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Volume 3, Issue 3, March 2014, pp. 209-213.

[20] William Stallings, *Cryptography and Network Security, Principles and Practice*, Pearson, Fifth Edition.