Journal of Scientific Research and Development 2 (2): 30-36, 2015
Available online at www.jsrad.org
ISSN 1115-7569

Presenting a new data security solution in cloud computing

Aysan Shiralizadeh, Abdulreza Hatamlou *, Mohammad Masdari

Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

Abstract: The world of information technology is constantly expanding. In line with the needs of community members such as security, processing, fast access and most importantly, saving money is very important. These days a solution to such problems has been introduced by the concept of cloud computing. Despite of its unique advantages, the security challenges such as data disclosure, privacy, attacks on servers, unsafe communication and resource sharing, can't be ignored. Thus, security is one of the main issues in cloud computing. In this paper, the proposed solution will be introduced to increase security in cloud computing. The encryption is a method to secure data from access of unauthorized users to the network. In this paper, we have provided a strong solution by combining hybrid encryption and digital signature. This method guarantees data protection and data integrity.

Key words: Cloud Computing; Security; Encryption; Digital Signature; Cryptool2

1. Introduction

Cloud computing can be provided as a service by the service provider assessment. Users do not need to know about how services are provided (e.g. network, storage and software) and kept there. Instead, the user's only concern is that services are available whenever needed. The term cloud computing is chosen for that all the details are hidden from the user's perspective. The user doesn't need to have knowledge about the infrastructure of the cloud which is used. Due to the novelty of this technology is not yet a precise definition for it (Jansen and Grance, 2011).

Institute of Standards and Technology has proposed definition is as follows (Mell et al., 2011): "Cloud computing is a model for providing easy access to the application's user. Through a changeable series of computational grid, such as nets, servers, storage space of applied program, and services." This access can be provided and released immediately with minimal need to resources management or direct involvement of Service Provider.

Three aspects of security are confidentiality, integrity and availability. Confidentiality is hiding information and resources. Integrity refers to the trustworthiness of data or resources, which usually prevents any incorrect or unauthorized changes. Availability refers to the ability to use the information or resource (Bishop, 2004). Thus, security is one of the main issues in cloud computing, as originally expected only people whose identities have been authenticated by client can access data. Given the above comments, there will be two main concerns in this area:

External attackers: Any person whose identity is authenticated to access the data by the client.

Cloud Providers: These centers can break their pledge, to gain unauthorized access to data. Cryptographic are methods or techniques to protect data by changing its format to other formats, which is not easily understood by unauthorized users. Also, methods such as, microdots and combining words with images can be used. Encryption methods can be divided into two sets of symmetric key algorithm and asymmetric key algorithm. Symmetric key algorithm is also known as the private or secret key. In symmetric key algorithm sender or receiver use one key to encrypt and decrypt the data (Seth and Mishra, 2011). Symmetric key algorithm is divided to the stream ciphers and block ciphers split encryption.

Cryptography objectives: 1) Confidentiality: This service is used securely to protect the contents of the message and not allow to access information to any third person other than the person (Surya and Diviya, 2012). 2) Authentication: It is related to the identification and authentication. Parties that communicate with each setup will be able to identify each other. Information receiver system, verifies the identity of the sender to see whether the information was sent by the authorized person or another person (Surya and Diviya, 2012). 3) Data integrity: This service prevents unauthorized modification of data. This means that neither the sender nor the receiver will not be able to change the message (Surya and Diviya, 2012). 4) Non repudiation: This service allows the sender and receiver not to deny sending and receiving messages (Surya and Diviya, 2011). 5) Access Control: This service controls information access and only allows authorized persons to access data.

* Corresponding Author.

Encryption techniques can be broadly classified into three categories as follows: symmetric key algorithms (Private Key), the asymmetric key algorithm (public key) and hybrid key algorithm. In symmetric algorithm, the transmitter and receiver both use the same key to encrypt or decrypt. This algorithm is divided into block ciphers and stream ciphers. Symmetric key algorithm is very fast due to its relatively low complexity, is easy to implement and run. Some of the most symmetric key algorithms include: DES, 3DES, AES, Blowfish, Twofish, Serpent, SEED, IDEA, RC2, RC4 and RC6.

Asymmetric key algorithms, also called public key algorithm (Kaur and Mahajan, 2013), (Solanki and Patel, 2012). In this algorithm, both the sender and receiver used two different keys, public key and private key, to encrypt and decrypt data. Sender used receiver's public key to encrypt the plain text to cipher text. Receiver used their own private key, to descript cipher text to original text. The private key which is used is always confidential. Asymmetric key algorithms are slower than symmetric key algorithms, and have higher computational burden. RSA is the most famous asymmetric key algorithm. Other asymmetric key algorithms include: Diffe_Hellman, DSA, EIGamal, XTR, and ECDSA.

In modern encryption system combination of a symmetric key asymmetric key algorithm is used for encryption and decryption process. Asymmetric key algorithm is used to distribute a symmetric key at the start of the session. When the symmetric key was known in session, encryption is able to operate very quickly. This algorithm is mainly having the problem of key distribution (Kaur and Mahajan, 2013), (Solanki and Patel, 2012). In each section or subsection, there are one or several paragraphs. Note that the sentences in each paragraph chain together and pursue a topic.

2. Related works

The basic concept of cloud computing history back to the early 1991, those mainframe computers came into the companies and educational environments. Encryption on the server side means that providers of cloud services after receiving the data from the user encrypted and then stored them. Since the cloud providers themselves are unaware of the place of stored data, so users still fear loss of data, so they will not store critical data in the cloud servers. The best solution is that before sending the data, they have been encrypted in client side and then encrypted data have been sent therefore we will not worry about hack or damage of data because in the encryption systems in client side private key is accessible to the user. In this section, we will discuss the proposed algorithms. The proposed algorithm vary with each other based on architectural structures, the key size, block size and number of processing cycle.

In 1972, Data Encryption Standard designed by IBM and the U.S. Government adopted it as standard encryption technique. This symmetric key block cipher encryption algorithm based on heterogeneous structure. It uses 64 bit block of text, 56 bit key length. It performs total 16 rounds of processing to encrypt data (Mandal et al., 2012). Rivest Cipher4 is a stream cipher from RSA Data Security. It was one of the common and fastest symmetric key algorithms invented in the year 1987. The algorithm uses a variable sized key from 1 to 256 bits (Dawson et al., 2002), (Singhal and Raina, 2011). In 1991, Xuejia Lai and James Massey designed International Data Encryption Algorithm. It is also identified as Improved Proposed Encryption Standard. This symmetric key block cipher algorithm based on substitution-permutation structure. It uses 64 bit block, 128 bit key and performs 8.5 round (Alam and Rafeek Khan, 2013). In 1993, Bruce Schneier designed Blowfish. It is fast and simple block encryption algorithm used in the Secure Socket Layer and other program. Blowfish is based on heterogeneous structure supports 64 bit block and key size of 32- 448 bit (Mushtaque et al., 2014), (Zahang and sun, 2011).

Rivest Cipher5 is a symmetric block cipher algorithm published in the year 1994. This algorithm is planned to be suitable for both hardware and software. This algorithm can be 32, 64, or 128 bits. The key size is also can be between 0 and 2048 bits. The number of rounds can be between 1 and 255. In 1996, Carlisle Adams and Stafford Tavares designed CAST-128. It is a block cipher algorithm used in different applications. It is based on heterogeneous structure. CAST-128 performs total 12 or 16 rounds. CAST-128 uses 64 bit block, key length of 40-128 bit (Nie et al., 2010). 3DES was published in 1998 which is from Data Encryption Standard. 3DES uses 3 different keys total size of 168 bits. All keys are identical or first key and third key may be same in 3DES. 3DES is also accepted by the U.S. Government to use because of its higher security (Halas et al., 2012). In 1998, Ron Rivest designed Rivest Cipher6; it derived from its predecessor Rivest Cipher5. It is also based on heterogeneous structure and takes block size of 128 bits, key size 128, 192 or 256 bits and, it performs total 20 rounds of processing to encrypt data. It uses 4 registers and it performs multiplication operation (Aggarwal et al., 2013), (Hashim et al., 2010). MARS is a block cipher designed by IBM in 1998 and selected as one of the five finalists in AUGUST 1999. MARS is based on type-3 heterogeneous structure, it uses 128 bits block, key size of 128, 192, 256 bits (Singh et al., 2014). In 1998, Vincent Rijmen and Daemen, Designed Advanced Encryption Standard which is a symmetric key block cipher encryption algorithm. It is based on heterogeneous network and support 128 bit block size and key length 128, 192 and 256 bits. AES performs 10, 12 or 14 rounds of processing to encrypt data (Mandal et al., 2012).

3. Proposed method

Cloud computing is an easy and available method for a collection of the security sources in internet

and is even presented new security challenges such as private security, information theft, confidentiality, integration and identity confirmation in storing data of cloud computing. Cryptography toward server means that the presenters of cloud services are ciphered and stored them after receiving the data from the user. Because cloud presenters are not aware of the store place, they do not store, therefore, the salient data in the cloud servers. The best solution is that data should be ciphered towards client before sending them to the server. Afterward, encrypted data will be sent. There will consequently be no need to worry about the theft or impairment of data, for client side of private code key is given to user in the cryptography systems.

The proposed method in this paper, is using the hybrid encryption algorithm and digital signature scheme. We use both symmetric key algorithm and asymmetric key algorithm in order to transfer and save the data in the network. The encryption process has the private key. Using the SHA1 algorithm, we can achieve the integrity by producing the brief message. We can encrypt data and provide the privacy by using the AES algorithm and we can verify the users' identity by using RSA algorithm. This section describes the selected algorithms and crytool2 and we will propose a new method by combining these algorithms in a particular way. According to the Fig. 1, EM, Ek2, EH and digital signatures D are as follows:

EM=AES (M)
Ek2=RSA (AES key)
EH =SHA-1(EM)
D=RSA-Sign (EH)

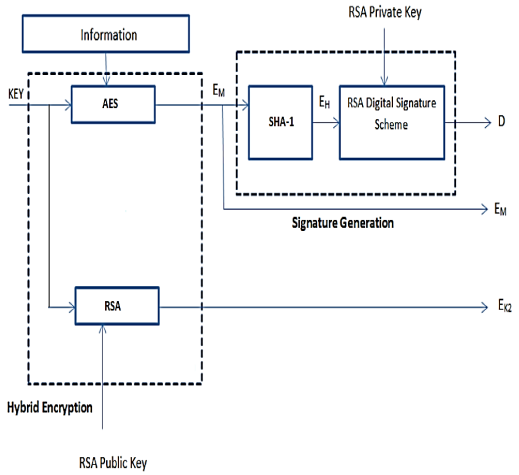

Fig. 1: The encryption of the proposed method

At first, information is converted to Encrypt message by the application of AES algorithm and generated key for the cryptography of proposed model. Then, encrypted message (EM) is delivered to the part of signature generation. RSA algorithm is continuously produced EK2 & RSA public key by the use of generated AES. RSA is used in this design, inasmuch as the increase of key length intensifies the security against attacks. A digital signature is an electronic tool with authenticity which results in authenticity of an electronic record through cryptography with public key. The main characteristics of digital signatures include:

A) In providing them, the unique information is used which a signatory has.
B) They are produced automatically by the computer.
C) The signature of each message is dependent to all bits of messages. It should be noted that any kind of minor changes in the text of document cause alternation in the signature of signatory.
D) The signature of each document id different with other ones.
E) It must be analyzable and verifiable in order to prevent any probable forgery as well as provides non-repudiation.

The main structure of digital signature is that the writer of electronic information has signed the information by his/her own secret cryptography key. This key must be kept secretly by the user. The signature is under control through public key which is related the signatory of document. This public key is visible and available for the public. A digital signature is created as following processes:

First step: It is about the creation of data unit which must be signed. For example, an informative object can be a text, shape, or any kind of digital information in a digital way.

Second step: it deals with the creation of intricate amount are usually called the summary of message. This outcome is resulted in the mathematical processing of one algorithm which creates a compact digital form. The intricate amount will be altered if a bit of the unit even changes. This technique causes a digital signature with constant and predictable length.

Third step: the signatory must encrypt the intricate amount with his/her own secret key and then creates his/her own digital signature for data. It is noticeable that the unique amount must connect or join the data unit.

At last stage, the control of digital signature with renewed produce of intricate amount start with the same data unit by previous algorithm. After that, digital signature attached to document is encrypted by the public key of signatory and finally the consequences are corresponded. If the consequence is uniform, the signature will be accepted and it will be rejected if the outcome is not alike. Here, the aim of the application of cryptography methods is to make sure of data integration, authenticity and data confidentiality. Secure hash EH, SHA-1 is produced by the algorithm and then by the application of RSA producing signature, the signature of message m (D) is directly produced from powering by the use of hash message and RSA private key. Public key of writer must be encrypted in order to determine the confirmation of signature D for signature m. the operation of decoding is unlike cryptography. The proposed design with a tool named cryptool2 is operated. EM, Ek2 and D are available for decryption.

The proposed decryption method in Fig. 2 is as follows:

K=RSA-Decrypt (Ek2)
M=AES-Decrypt (EM)
EH =SHA-1 (EM)
EH =RSA-verify (D)

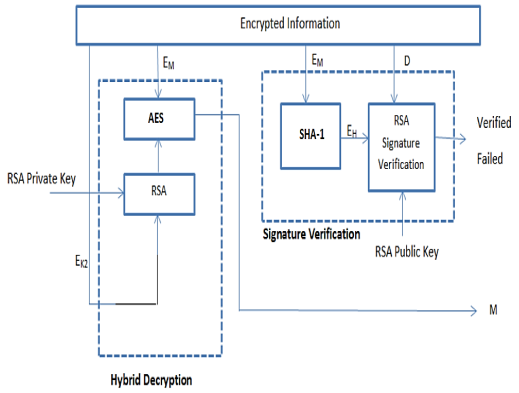

Fig. 2: The decryption of the proposed method

4. Evaluation

In 1998, Vicente Rijman Joan Damoun designed an advanced encryption standard algorithm (AES) which is the symmetric encryption algorithm of cipher block. This algorithm has Feistel structure and it can encrypt by using 128-bit block size and 128,192 and 256-bit key size. Pseudo-code of AES algorithm is as follows:

A: the first step

- AddRoundKey

B: the following four functions are periodically repeated

- SubByte
- ShiftRow
- MixColumn
- AddRoundKey

C: final step

- SubByte
- ShiftRow
- AddRoundKey

RSA algorithm is the method of encryption by using public key. This method is the first reliable method among other methods and it is one of the greatest advances in the field of cryptography. RSA continues to be widely used in electronic transactions and it seems safe if it is used properly with long keys. This algorithm is known as RSA algorithm after the Ron Rivest, Adam Shamir and Len Adleman have designed it in 1977. Although the primary techniques of this algorithm which was designed by Clifford Cocks were confidential, it was not as simply as what we mention in the following: RSA is generally composed of two keys, public key and a private key. Numerical key is fixed and it is used in computing the encryption. Public key to encrypt the message is clear to all. This message is opened only by the private key. In other words, anyone can encrypt a message but only the owner of the private key can open the message and read it. Suppose that the sender of the message has a pair of integers (e, n) as a public key to encrypt at his disposal. In contrast, the receptor of the message uses pair of (d, n) to decrypt the message. It is evident that two pairs of (e, n) and (d, n) have subtle relationship. This relationship is not in a way that we can simply deduce d by possessing e and n . All steps of the RSA algorithm are as follows:

The production of a key:

- Select p and q both prime numbers
- Calculate n=p * q
- Calculate $\phi(n)=(p-1) * (q-1)$
- Select integer e such that $GCD(\phi(n),e)=1;1<e<\phi(n)$
- Calculate d, $d=e-1 \bmod \phi(n)$
- Public key KU=[e,n]
- Private key Kr=[d,n]

Encryption:

- Plain text M, M<n
- Cipher text C=Me mod n

Decryption:

- Cipher text C
- Plain text M=Cd (mod n)

In order to determine the authenticity of the message in sending and in order to ensure that no manipulation of the signed message is occurred, we can use the digital signature. It is necessary to use the digital signature in order to verify the message. The digital signature can also be used in the electronic voting and in the virtual education. The importance of digital signatures in communication leads to a new encryption system. In this project, we will use the RSA which increases the security against

attacks because of the increased length of key. Pseudo-code of RSA algorithm is as follows:

The production of a key

- Select p and q both prime numbers
- Calculate n=p * q
- Calculate ϕ(n)=(p-1) * (q-1)
- Select integer e such that GCD(ϕ(n),e)=1;1<e< ϕ(n)
- Calculate d, d=e-1 mod ϕ(n)
- Public key KU=[e,n]
- Private key Kr=[d,n]

Encryption

- Plain text M, M<n
- Cipher text C=Me mod n

Decryption

- Cipher text C
- Plain text M=Cd (mod n)

The secure hash algorithm (SHA1) is a hash function in cryptography. This function is designed by National Security Agency in the United States of America and it is published by the National Institute of Standards and Technology Foundation. The hashing algorithm is the most used algorithm and it is used in lots of software and security applications. Since 2005, the security errors of this algorithm which were identified in applied mathematics have shown that this algorithm may be broken. And since then, a better algorithm in this field was necessary. However this is not likely to become a reality and any successful attack to this algorithm has been occurred and nowadays this algorithm is used in numerous softwares and protocols. The detection of degradation data, the alternation of data and the verification of the signature are used in revision control systems. The original structure of the SHA-1 algorithm is as follows:

for i from 0 to 79

if 0 ≤ i ≤ 19 then

f = (b and c) or ((not b) and d)

k = 0x5A827999

else if 20 ≤ i ≤ 39

f = b xor c xor d

k = 0x6ED9EBA1

else if 40 ≤ i ≤ 59

f = (b and c) or (b and d) or (c and d)

k = 0x8F1BBCDC

else if 60 ≤ i ≤ 79

f = b xor c xor d

k = 0xCA62C1D6

temp = (a leftrotate 5) + f + e + k + w[i]

e = d

d = c

c = b leftrotate 30

b = a

a = temp

Cryptography is a branch of computer science it has attracted the attention of many researchers because it is widely used in many fields. Therefore, it is necessary to analyze the provided encryption algorithms. Cryptools2 are the tools for analyzing, learning and implementing algorithms with usual and practical manner. These tools enable us to create digital signatures and to analysis and implement the algorithms.

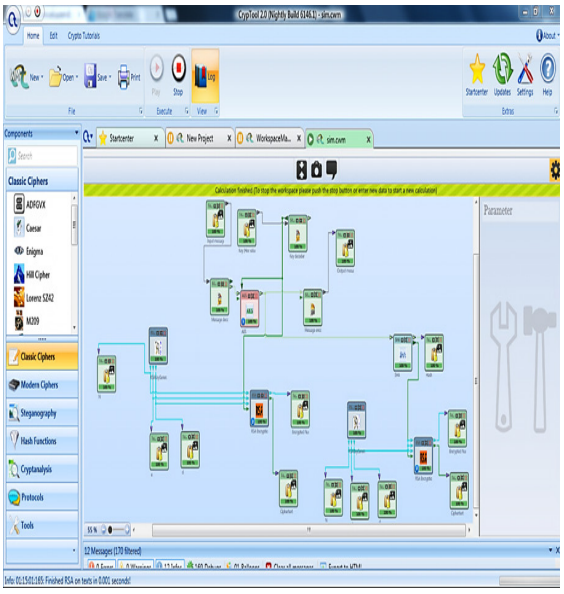

Fig. 3: The working environment of cryptools2

The horizontal space on the top and on the left of toolbox is shown in this figure. Some of the

advantages of this application are as follows: There is a free version on the Internet which is easily accessible for everyone 2) it can be easily installed and it requires no special equipment. 3) It provides the user-friendly environment for the users in order that the users can easily use information sources. 4) It covers all encryption methods and it is very widespread. We will implement the proposed algorithm by the means of presented tools and we will analyze the proposed algorithm.

5. Conclusion

In this paper, we used cryptography in order to solve the security problems in the cloud computing and to achieve confidentiality, integrity and availability of data. At the beginning of the study, we discussed the previous studies and then we proposed a new encryption algorithm. This method guarantees data protection and data integrity. Then we conducted the procedure of the study and presented the cryptool2 tools. In this paper, we presented the strong solution by integrating hybrid encryption and digital signature. In order to secure the data, it is necessary to know which algorithm has the best performance in terms of safety, efficiency, accuracy and effectiveness. AES algorithm is chosen because it is the fastest method that has the flexibility and scalability and it is easily implemented. In the other hand, the required memory for AES algorithm is less than the Blowfish algorithm. AES algorithm has a very high security level because the 128, 192 or 256-bit key are used in this algorithm. It shows resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Therefore, AES algorithm is a highly secure encryption method. Data can also protect against future attacks such as smash attacks. AES encryption algorithm has minimal storage space and high performance without any weaknesses and limitations while other symmetric algorithms have some weaknesses and differences in performance and storage space. RSA algorithm can also increase the security of the algorithm. One of the reasons for using combined AES and RSA algorithm, in the proposed algorithm, is the high speed of this method. SHA-1 has the least computational cost among the similar algorithms. RSA digital signature scheme also guarantees the authenticity and integrity of data. In the future studies, we will compare new algorithms and we will study the combination and optimization of them and we will also offer a solution for creating a secure protocol in cloud computing.

References

A ggarwal K, Saini JK, Verma HK (2013). Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers. International Journal of Computer Applications, 68(25): 10-16.

Alam MI, Rafeek Khan M (2013)," Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography". International Journal of Advanced Research in Computer Science and Software Engineering, 3(10): 713-720.

Bishop M (2004). Introduction to Computer Security, 1st ed. Pearson Education.

Dawson E, Gustafson H, Henricksen M, Millan B (2002). "Evaluation of RC4 Stream Cipher", Information Security Research Centre Queensland University of Technology, 1-53.

Halas M, Bestak I, Orgon M, Adrian Kovac A (2012). "Performance Measurement of Encryption Algorithms and Their Effect on Real Running in PLC Networks", 161–64.

Hashim AT, Mahdi JA, Abdullah SH (2010). "A Proposed 512 bits RC6 Encryption Algorithm", 10(1): 11-25.

Jansen W, Grance T (2011). "Guidelines on Security and Privacy in Public Cloud Computing", 1-80.

Kaur G, Mahajan M (2013). "Evaluation and Comparison of Symmetric Key Algorithms". International Journal of Science, Engineering and Technology Research, pp 1960-1962.

Mandal AK, Parakash C, Tiwari MA (2012). "Performance Evaluation of Cryptographic Algorithms: DES and AES". IEEE Student's Conference on Electrical, Electronics and Computer Science, 1-5.

Mell P, Grance T and Timothy Grance T (2011). "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology", 1-7.

Mushtaque MA, Dhiman H, Hussain S , Maheshwari Sh (2014). "Evaluation of DES, TDES, AES, Blowfish and Twofish Encryption Algorithm Based on Space Complexity". International Journal of Engineering Research & Technology (IJERT), 3(4).

Nie T, Li Y, Song Ch (2010) . "Performance Evaluation for CAST and RC5 Encryption Algorithms International Conference on Computing, Control and Industrial Engineering: 106–9.

Seth ShM, Mishra R (2011). "Comparative Analysis of Encryption Algorithms for Data Communication", IJCST , 2(2).

Singh H, Danewalia AS, Chopra D, Kumar N (2014). "Randomly Generated Algorithms and Dynamic Connections", ISROSET International Journal of Scientific Research in Network Security and Communication, 2(1): 1-4.

Singhal N, Raina JPS (2011). Comparative Analysis of AES and RC4 Algorithms for Better Utilization.

International Journal of Computer Trends and Technology, (July): 177-181.

Solanki KH, Patel ChR (2012). "New Symmetric Key Cryptographic algorithm for Enhancing Security of Data". International Journal of Research in Computer Engineering and Electronics, 1(3): 1-5.

Surya, Diviya A (2012). "A Survey on Symmetric Key Encryption Algorithms". International Journal of Computer Science & Communication Networks, 2(4): 475-477.

Zahang Z, sun Sh (2011), "Image encryption algorithm based on logistic chaotic system and s boxes scrambling". Image and Signal Processing (CISP), 4th International Congress on Volume 1.