International Journal of Grid Distribution Computing
Vol. 8, No.4, (2015), pp. 269-276
http://dx.doi.org/10.14257/ijgdc.2015.8.4.26

Data Protection in Clouds using Two Stage Encryption

Pallav Sharma, Varsha Sharma, Sanjeev Sharma and Jitendra Agrawal

School of Information Technology, UTD
Rajiv Gandhi Proudyogiki Vishwavidhyalaya, Bhopal, India
pallav.20@gmail.com, varshasharma@rgtu.net, sanjeev@rgtu.net, jitendra@rgtu.net

Abstract

Cloud Computing has been an emergent technology that has opened the space for virtualization, as it provides many computational services and storage services over the Internet with the help of a browser. Cloud computing's core comprises of services like platform, infrastructure and software as a service. The unpredicted boom in cloud computing is driven by its simple economic benefit. It helps in reducing capital expenses and minimizes operating expenses. This move however, has increased a major concern about the protection of data, as against the traditional system the data is now stored online and is far easily exposed than we realize. This raises a major security issue for data protection. Many techniques for protection of data have been proposed so far. However, the best available option till date is to encrypt user data before storing it over the cloud environment and decrypting it again before handing the data back to the cloud user. In this paper, we introduce a more efficient and stronger encryption process that allows a cloud service provider to protect user data more efficiently.

Keywords: *Cloud Computing, Data Protection, RSA, IDEA*

1. Introduction

For so long the internet was shown in the form of a cloud symbol in any network diagram until in the year 2008 many services started to merge the permitted computing resources to be accessed over the internet which then came to be known as cloud computing. Cloud computing is a model, in which a huge pool of systems are linked in private, public, hybrid or community networks. This provides a dynamically accessible infrastructure for running applications and storage of data as well as files. The emergence of cloud computing has significantly reduced the costs associated with computation, content storage, application hosting and delivery. Cloud computing enables its users to experience direct cost benefits [10][17]. Cloud computing is based on the basic principle of 're-usability of IT facilities'. The definition of cloud computing as proposed by National Institute of Standards and Technology(NIST) states that, "Cloud Computing is a model to enable convenient, uninterrupted, on-demand network access to a pool of shared configurable computing resources (like storage, application, networks, servers, services) that can be rapidly provisioned and released with minimum management effort or service provider interaction"[1].

The customers of cloud computing do not own a physical infrastructure or resources; rather they rent their usage from a third-party provider. Customers use the resources as a service and make payments only for the resource that they are using. Cloud computing infrastructure mainly consists of services delivered via common data centres and servers. Resource sharing among users is improved, as servers are not allowed to be idle. This reduces the cost significantly and at the same time increases the application development speed [11].

ISSN: 2005-4262 IJGDC

The third-parties offer users or customers an affordable and flexible computing service that they would otherwise not afford alone. This new method of service provisioning has evolved from the research stemming from networking, distributed systems, utility computing, and the web and software services [10]. This paradigm shift has prompted many businesses and individuals to migrate parts of their IT Infrastructure to the cloud which is managed by Cloud Service Providers (CSPs). A broad range of definitions exits for Cloud Computing, each of which differs depending on the originating authors' learning [12-13]

The major reason behind the global move towards cloud computing is the reduction in cost of setting up small business ventures and/or hardware/software expenditure in case the old one is outdated or in insufficient. This can be understood by the following example, suppose a person has a 2TB Hard Disk Drive (HDD) and he/she needs 100MB more storage space because of a project work that he/she is doing. Now for this purpose buying a new HDD for a temporary task is meaningless and costly, rather he/she can rent storage from a Cloud Service Provider (CSP) until his/her task is completed. This is cheaper and desirable. From the above example it can be understood that the cost effectiveness is major driving force behind cloud computing. However, the move towards cloud has unfortunately introduced an overhead for the security and privacy of user data that is stored online. The reason behind this is, CSPs mostly store their data using a third party data server over which they have no control whatsoever. There are various news about someone losing or getting corrupted data, which was stored on a cloud. There have been many security techniques introduced so far for the protection of user data. However, one can never be too cautious. In this paper, we have proposed a new encryption system to protect user data over the cloud.

2. Preliminary

2.1. Data Encryption

Data Encryption is the process of encrypting data by using an encryption algorithm for conversion of the original meaningful data into non-human readable format, so as to safeguard it against illegal access, theft or misuse, cryptography, as defined, is the act of achieving security of original user data by encoding it to make it non-readable. Nowadays, more and more data is in digital form rather than the traditional paper file system. With data being available online over the internet it is more important now to safeguard this data from illegal access or unauthorized reading. For this purpose the user data is now encrypted before storing it, so as to make it nothing more than some garbage value to those who try to steal it or gain access illegally. Data Encryption is performed using one of the many available encryption algorithms either alone or in combination with other encryption algorithms. Some of the encryption algorithms are DES, AES, IDEA, Blowfish or RSA etc.

2.2. RSA

RSA algorithm is one of the most famous and robust asymmetric key cryptographic algorithms. This algorithm was designed by Rives, Shamir and Adleman and proposed in 1977. It works on the idea of public and private key. RSA was the first implemented public-key cryptosystem. Here, a public key is used for data encryption. Public key is known to everyone concerned. Encrypted data can be decrypted only by using the private key known to intended user only. The basis of RSA algorithm is the mathematical fact that it is simple to find and multiply large prime numbers, but it is very difficult to factor their product. The private and public keys in RSA depend on very large prime numbers. The RSA algorithm itself is quite simple. However, the real challenge lies in the task of selection and generation of both the public and private keys.

RSA uses a key size of 1024 bits (standard key size), however a larger size key can also be used. The key size in RSA is based on the how large the file is to be encrypted. For so long RSA has been used for communicating over the internet i.e. sharing private/confidential information using RSA encryption. The idea behind working of RSA is quite simple. The algorithm selects two large prime numbers at random and multiplies them to get a new number. Then a random value is chosen based on the fact that this number and the previous number are co-prime and are in the given range. Then based on these two numbers a third number is calculated to generate the final term for the key. Both public and private keys are a combination of these numbers used in pairs.

2.3. IDEA

The International Data Encryption Algorithm (IDEA) is a cryptographic algorithm which was designed by Xuejia Lai and James Massey of ETH Zurich. It was launched in 1990. IDEA is classified as a block cipher and like Data Encryption Standards (DES), it works on 64-bits blocks of plain text. The key used in IDEA is longer and consists of 128 bits. Like DES, IDEA is reversible i.e. same algorithm is used for encryption as well as decryption. Both diffusion and confusion are used for encryption by IDEA. IDEA breaks the whole data into blocks of 64 bits each and processes a single block of 64 bits at a time i.e. plain text of 64 bits is given as input and cipher text of 64 bits is generated as output. The input 64-bit plain text block is split into four portions of 16-bits each. These four plain text blocks are input for the first round. The algorithm has eight such rounds. There are 128 bits in the key. 52 sub-keys each of size 16 bits are generated from the 128 bit key. In each round, six sub-keys are generated from the original key. 48 sub-keys are used till round eight. The final step is an output transformation, which uses just four sub-keys. This step produces the final output which is four blocks of cipher text. These four blocks are combined to generate the final 64 bit cipher text block.

In each round, the algorithm mixes three basic algebraic operations and performs on the four blocks (16-bit blocks):

1. Bitwise XOR

2. Addition modulo 216(=65536)

3. Multiplication modulo 216+1(=65537).

Assuming the plaintext 64 bits block is divided into four 16 bits sub-blocks say, P1 to P4, and the six sub-keys of first round are say, K1 to K6. Then, a single round of IDEA performs the following steps:

1. Perform Multiplication* of sub-block P1and sub-key K1.
2. Perform Addition* of sub-block P2 and sub-key K2.
3. Perform Addition* of sub-block P3 and sub-key K3.
4. Perform Multiplication* of sub-block P4 and sub-key K4.
5. Perform XOR on results of step 1 and step 3.
6. Perform XOR on results of step 2 and step 4.
7. Perform Multiplication* of the results of step 5 with sub-key K5.
8. Perform Addition* of results of step 6 and step 7.
9. Perform Multiplication* of results of step 8 with sub-key K6.
10. Perform Addition* of the results of step 7 and step 9.
11. Perform XOR on results of step 1 and step 9.
12. Perform XOR on results of step 3 and step 9.
13. Perform XOR on results of step 2 and step 10.
14. Perform XOR on results of step 4 and step 10.

Here Multiplication* and Addition* refers to multiplication modulo and addition modulo. The remaining 7 rounds also perform the same steps.

Decryption process of IDEA is exactly the same as that of encryption process. There are some alterations in the generation and pattern of sub-keys. The sub-keys for decryption are actually in verse of the sub-keys for encryption.

3. Related Work

Plenty of works have been done in the direction of data encryption. Today, huge amount of data is stored online over the cloud daily. These data are available online through the internet. Therefore it is of utmost importance that this data is accessed only by its intended user. Even if data is secured from unauthorized access from outside, the data can still be accessed by some insider. Data encryption takes an important role in these situations. In the literature, plenty of works are already done in this field.

With the arrival of cloud computing paradigm and the increased aptness of decision makers to visualize a staged departure to cloud services, many enterprises are opting to outsource their data to cloud storage providers which results in improved management of their IT resources with respect to security, control, space and costs. In this situation, assuming that the CSP may not be trustworthy, assuring data privacy in all processes performed on data while these data lie in the Cloud is a challenge.

Many works have been proposed in this field till date i.e. for encrypting user data before storing them on cloud server. Some of the previous works are discussed below.

N. Saravanan et al. [4] presented system for data security using RSA algorithm in cloud computing. The authors implemented RSA algorithm in google app engine using cloud SQL.

M. Sudha, Dr. Bandaru Rama Krishna Rao [18], implemented a data protection framework. The framework performed authentication, verification and encrypted data transfer for maintaining data confidentiality.

Neha Jain [2], presented a system for data security using DES algorithm in cloud computing. The designing of security architecture of the system was done using DES cipher block chaining, which eliminates the frauds with data. To ensure security the system communication among modules was encrypted by using a symmetric key.

Sonal et al. [5] proposed a technique to increase the security of the multimedia data by using crossbreed algorithm. The authors proposed an ontology framework for access control in cloud environment to assist the construction of security system and at the same time reducing the complexity related to security system design and implementation. The authors used the ability of RSA to support public key cryptography and digital signatures. The idea behind the technique was to design algorithm based on the combination of RSA and DES which will provide better security than either DES or RSA alone. This technique enhanced the data security and successfully prevented replay attacks.

Priyanka et al. [6] proposed a technique in the form of a secure cloud framework. This technique proposed security on the cloud side and also made client data secure. The authors proposed architecture for providing cloud and user data security.

Rajiv et al. [7] presented a model for encryption of data using the services of one service provider and storage of data at another service provider’s side. So, as soon as the data is encrypted, it is moved from the encryption service providers’ side to the storage providers’ side. The data is stored in the encrypted form and the administrators and the employees will not be aware of keys or the service provider responsible for encryption and decryption. Here, the algorithm used for encryption/decryption is Blowfish Algorithm.

4. Proposed Scheme

In this paper we propose an encryption technique that ensures the security of user data over the cloud. Here in our approach we assume that the data on client side is safe. For our technique, we proposed an architecture that safeguards a cloud users' data against security issues such as unauthorized access or insider access which are major security concerns at the CSP's side. The proposed technique uses a mix of both RSA and IDEA to encrypt the data before it is stored at CSP's side.

RSA generates public-key and private-key using two large prime numbers for the purpose of encryption and decryption. Data encryption is done using public-key and data decryption is done using private-key. The RSA here uses a 1024 bit key.

IDEA (International Data Encryption Standard) is used as the second encryption/decryption algorithm in our proposed encryption system. IDEA is a block cipher algorithm. IDEA uses a key size of 128 bits. These 128 bits are used for generation of 52 sub-keys each of length 16 bits. The sub-keys are generated using left circular shift of the original bits of 128 bits key whenever the key bits are completely exhausted. The encryption process has eight rounds and one-half round. Each round uses 6 16-bits sub-keys to operate on four 16-bits plaintext blocks. After the eight rounds, the last round also called as final transformation round uses four sub-keys to generate the cipher block as output. Here in each round a single MA block (multiplicative-additive block) performs confusion and diffusion which are the core aspects of IDEA.

IDEA is a strong algorithm and it is nearly impossible to crack, but the large classes of weak keys have been found in IDEA. The weak key problems in Daemon's report are dealt with by performing exclusive-OR of each sub-key with a constant such as, 0x0DAE.

Following are the steps of our proposed Encryption method –

1. First the User logs in to the system with their credential. New User are redirected to Signup page.
2. After receiving login information, the user is validated.
3. Both keys (public-key and private-key) for RSA are generated one time i.e. only at the time of first encryption, and then the public-key is stored at Customer Relation Module (CRM) along with users' ID. The private key is sent to user via email.
4. After logging in to the system the user uploads a file, which is then sent to CRM.
5. CRM sends this file to RSA Encrypt or along with the users' public key, where this file is encrypted using RSA encryption technique.
6. After successful RSA encryption the CRM is updated with completion message.
7. Then this encrypted file is sent to the Cloud Server, where this file further encrypted using IDEA encryption algorithm. After successful encryption the cloud server is updated and the file is sent to cloud storage for storing.
8. After this, the cloud server and CRM are updated with the knowledge of new file.
9. At last the cloud user is notified of the successful completion of the process.
10. The 128 bit key used for IDEA is stored along with the user's ID at CSPs' side.
11. Every time the user encrypts a new data, a new key for IDEA is used.

Figure 1 shows a flow diagram of the proposed encryption process.

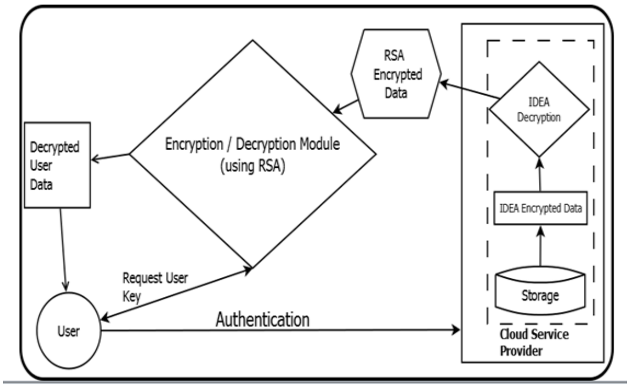

Figure 1. Flow Diagram Depicting the Encryption Process

Following are the steps used for decryption of user data –

1. The user logs in to the system using his/her credential and requests the data retrieval.
2. After receiving login information, the user is validated.
3. CRM sends data retrieval request to cloud server along with user id.
4. The cloud server then retrieves user file from cloud storage and decrypts it, using IDEA algorithm.
5. Then this decrypted file is sent to RSA Decrypt or for further decryption.
6. The CRM establishes a secure connection and asks the user to enter private key for RSA.
7. Then the file is decrypted to return the original file.
8. After this, the CRM sends the completely decrypted file to user and the connection from module to user is terminated.

Figure 2 shows a flow diagram of the proposed decryption process.

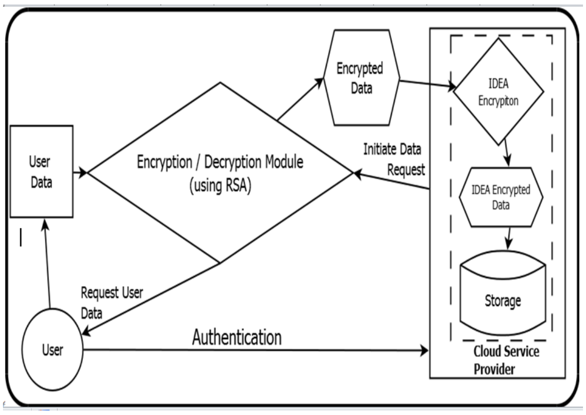

Figure 2. Flow Diagram Depicting Decryption Process

5. Results

Numerous files with text, audio and video have been considered and successfully encrypted, uploaded, decrypted and downloaded. A graph plotted between data size and time taken to encrypt the data using various encryption techniques is shown in figure 3. From figure, it is clear that encryption by proposed algorithm (RSA+ IDEA) is faster as compared to other algorithms.

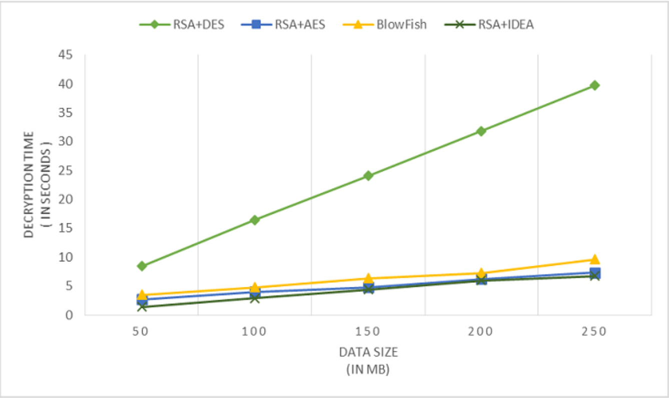

Figure 3. Comparison of Encryption Time for Various Encryption Algorithms

A graph between different data size and time taken to decrypt the data using various decryption techniques is shown in figure 4. The figure shows that the decryption by proposed algorithm (RSA+IDEA) is faster compared to other techniques

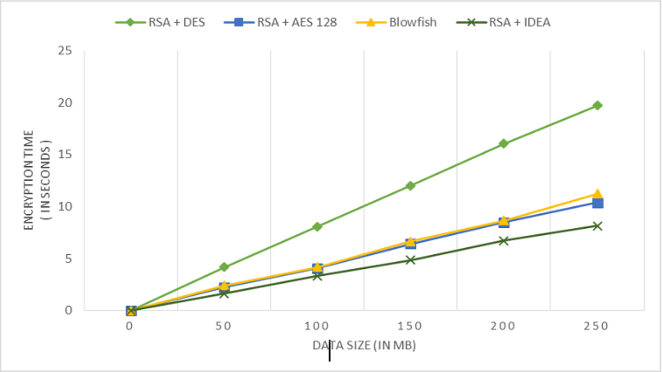

Figure 4. Comparison of Decryption Times for Various Decryption Algorithms

Table 1 shows average time of our algorithm as compared to other algorithms over the same data size (i.e. 250 MB).

Table 1. Comparison of Proposed Method with Previous Known Methods

Algorithm	Data	Time (in Sec)	Average MB/Sec	Performance
RSA + DES	250MB	20	12-13	Medium
RSA + AES	250MB	9.2	27-28	High
Blowfish	250MB	11.24	22-23	High
RSA + IDEA	250 MB	8.16	30-31	Very High

6. Conclusion

In this paper an encryption technique is proposed that protects user data over the cloud from being illegally accessed. The technique proposed here presents a more sophisticated and complex algorithm that makes it harder to perform cryptanalysis on it. Although the use of IDEA increased the complexity of the system but the overall achievement of encrypting user data which is nearly impossible to crack, covers up for the minor overheads. The proposed algorithm removed the shortfalls of the predecessor systems. Using two algorithms in succession allowed maintaining the credibility of the data, as the data is processed by two different parties.

References

[1] W. Jansen and T. Grance, “Guidelines for security and privacy in pubic cloud”, Draft Special Publication, **(2011)** September pp. 800-144.

[2] N. Jain and G. Kaur, “Implementing DES Algorithm in Cloud for Data Security”, VSRD-IJCSIT, vol. 2, Issues 4, **(2012)**, pp. 316-321.

[3] A. Kahate, “Cryptography and Network Security”, Tata McGraw-Hill.

[4] N. Saravanan, A. Mahendiran and N. Venkata Subramaniuan, “An implementation of RSA Algorithm in Google Clouds using Cloud SQL”, Research Journal of Applied Sciences, Engineering and Technology vol. 4, no. 19, **(2012)** October 01, pp. 3571-3579.

[5] S. Guleria and Dr. S. Vatta, “To Enhance multimedia security in cloud computing environment using crossbreed algorithm”, International Journal of Application or Innovation in Engineering and Management (IJAIEM), vol. 2, Issue 6, **(2013)** June.

[6] P. Gupta, A. K. Brar, “Multimedia Content Storage with Hybrid Encryption over Cloud Server”, International Journal of Advance and Innovative Research (IJAIR), vol. 2, Issue 7, **(2013)** July.

[7] R. R. Bhandari and Prof. N. Mishra, “Cloud Computing A CRM Service Based on Separate Encryption and Decryption Using Blowfish Algorithm”, International Journal on Recent and innovation Trends in Computing and Communication (IJRITCC), vol. 1, Issue 4, **(2013)** April.

[8] S. Patil and V. Bhusari, “An Enhancement in International Data Encryption Algorithm for Increasing Security”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, Issue 8, **(2014)** August, pp. 2319-4847.

[9] H. Mahajan and Dr. N. Giri, “Threats to cloud computing security”, VESIT, International Technological Conference, **(2014)** January 03-04.

[10] AWS Cloud HSM. http://aws.amazon.com/cloudhsm/

[11] Amazon EC2. http://aws.amazon.com/ec2/

[12] Google Drive. http://drive.google.com/

[13] Amazon Glacier. http://aws.amazon.com/glacier/

[14] Amazon S3. http://aws.amazon.com/s3/

[15] Z. W. –O. Hearn and B. Warner, “Tahoe the least-authority file system”, In Proceedings of the 4th ACM international workshop on Storage security and survivability, **(2008)**, pages 21–26.

[16] Amazon Web Services. http://aws.amazon.com/.

[17] J. Pettitt, “Hash of plaintext as key?”, http://cypherpunks.venona.com/date/1996/ 02/msg02013.html

[18] M. Sudha, Dr. B. R. K. Rao, “A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment”, International Journal of Computer Applications (0975-8887), vol. 12, Issue 8, **(2012)** December.

[19] “The RSA algorithm”, J. S. Song, **(2017)** November 13, Yonsei University.

[20] Y. Kadam, “Security Issues in cloud computing a transparent view”, International Journal of Computer Science and Emerging Technologies (IJCSET), E-ISSN, vol. 2, Issue 5, **(2011)** October, pp. 2044-6004.