Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Encryption for Secure Data Sharing in Public Clouds Using Cryptography

Sangeeta Kumari
Dept. of Computer Science & M.TECH, IPEC
(UPTU) Uttar Pradesh, India

Alok Katiyar
Dept. of Computer Science & Asst. Prof – IPEC
(UPTU) Uttar Pradesh, India

Abstract*— Cloud computing is a globalized concept and there are no borders within the cloud. Computers used to process and store user data can be located anywhere on the globe, depending on where the capacities that are required are available in the global computer networks used for cloud computing. Because of the attractive features of cloud computing many organizations are using cloud storage for storing their critical information. The data can be stored remotely in the cloud by the users and can be accessed using thin clients as and when required. One of the major issues in cloud today is data security in cloud computing.Storage of data in the cloud can be risky because of use of Internet by cloud based services which means less control over the stored data. One of the major concern in cloud is how do we grab all the benefits of the cloud while maintaining security controls over the organizations assets.Organizations are showing great interest in storing data on public clouds. This could be a result of the unprecedented growth of data recorded in the last few years. However the security issues associated with data storage over cloud is a major discouraging factor for potential adopters. Hence the focus of today is to find cryptographic techniques that will offer more than confidentiality. The objective is to manage and protect the data from the users of a client organization which wants to store the data on untrusted public clouds. In this thesis ahybrid cloud framework is proposed that addresses the privacy and trust issues and provides encrypted storage with public clouds. The proposed method uses Cryptography and Diffie hellman key exchange mechanism for protecting the user data.

Keywords*— Cloud Computing,CertificatelessCryptography,Confidentiality,Authentication,Access Control.

I. INTRODUCTION

The internet is a new technology now days, for business and current users already part of everyday life. Any information is available anywhere in the world at any time. That was not possible few years ago. Nowadays it have arisen a lot of possibilities of access to public and private information like internet speed access or the deployment of mobile dispositive that allow the connection to Internet from almost everywhere. Today a lot of people are consulting their mail online through webmail clients, writing Collaborative documents using web browsers, creating virtual albums to upload their photos of the holidays. They are running applications and storing data in servers located in Internet and not in their own computers. Something as simple as enter in a web page is the only thing a user needs to begin to use services that reside on a remote server and lets him share private and confidential information, or using computing cycles of a pile of servers that he will ever see with his own eyes. And every day it is being used more this services that are called cloud computer services. That name is given because of the metaphor about Internet, as something than the user see like a cloud and cannot see what is inside.

This services can be offered by free or by paying by demand, can be simply like a function calling (like asking the temperature in some city in the world for include it in a web page) or complex (like the usage of a virtual machine with its own operating system, applications and storage space for running applications). This means that many users and organizations can avoid install some applications in their computer or can have more computational power using cloud computer through internet, or they can make their own private cloud to manage it completely, or they can use both options for the moments of high demand of consume.

II. INTRODUCTION TO CLOUD COMPUTING

The internet is a new technology now days, for business and current users already part of everyday life. Any information is available anywhere in the world at any time. That was not possible few years ago. Nowadays it have arisen a lot of possibilities of access to public and private information like internet speed access or the deployment of mobile dispositive that allow the connection to Internet from almost everywhere. Today a lot of people are consulting their mail online through webmail clients, writing Collaborative documents using web browsers, creating virtual albums to upload their photos of the holidays. They are running applications and storing data in servers located in Internet and not in their own computers. Something as simple as enter in a web page is the only thing a user needs to begin to use services that reside on a remote server and lets him share private and confidential information, or using computing cycles of a pile of

servers that he will ever see with his own eyes. And every day it is being used more this services that are called cloud computer services. That name is given because of the metaphor about Internet, as something than the user see like a cloud and cannot see what is inside.

- This services can be offered by free or by paying by demand, can be simply like a function calling (like asking the temperature in some city in the world for include it in a web page) or complex (like the usage of a virtual machine with its own operating system, applications and storage space for running applications). This means that many users and organizations can avoid install some applications in their computer or can have more computational power using cloud computer through internet, or they can make their own private cloud to manage it completely, or they can use both options for the moments of high demand of consume

Fig.1.Cloud Computing User Devices

III. USED TECHNIQUESFOR ENCRYPTION OR DECRYPTION

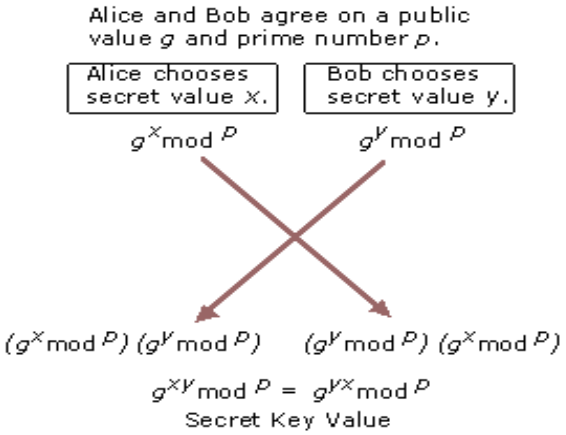
A. Diffie–Hellman key exchange (D–H)

The Diffie-Hellmann key exchange is a secure method for exchanging cryptographic keys. This method allows two parties which have no prior knowledge of each other to establish a shared, secret key, even over an insecure channel. The concept uses multiplicative group of integers modulo, which without knowledge of the private keys of any of the parties, would present a mathematically overwhelming task to a code breakerThe general idea of the Diffie-Hellmann key exchange involves two parties exchanging numbers and doing simple calculations in order to get a common number which serves as the secret key. Both parties may not know beforehand what the final secret number is, but after some calculations, both are left with a value that only they know about which they can use for various purposes like identification and as a secret key for other cryptographic methods. It is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

The Diffie-Hellmann key exchange is a secure method for exchanging cryptographic keys. This method allows two parties which have no prior knowledge of each other to establish a shared, secret key, even over an insecure channel. The concept uses multiplicative group of integers modulo, which without knowledge of the private keys of any of the parties, would present a mathematically overwhelming task to a code breakerThe general idea of the Diffie-Hellmann key exchange involves two parties exchanging numbers and doing simple calculations in order to get a common number which serves as the secret key. Both parties may not know beforehand what the final secret number is, but after some calculations, both are left with a value that only they know about which they can use for various purposes like identification and as a secret key for other cryptographic methods.

Diffie-Hellman key agreement is not based on encryption and decryption, but instead relies on mathematical functions that enable two parties to generate a shared secret key for exchanging information confidentially online. Essentially, each party agrees on a public value g and a large prime number p. Next, one party chooses a secret value x and the other party chooses a secret value y. Both parties use their secret values to derive public values, g x mod p and g y mod p, and they exchange the public values. Each party then uses the other party's public value to calculate the shared secret key that is used by both parties for confidential communications. A third party cannot derive the shared secret key because they do not know either of the secret values, x or y.

For example, Alice chooses secret value x and sends the public value g x mod p to Bob. Bob chooses secret value y and sends the public value g y mod p to Alice. Alice uses the value g xy mod p as her secret key for confidential communications with Bob. Bob uses the value g yx mod p as his secret key. Because g xy mod p equals g yx mod p, Alice and Bob can use their secret keys with a symmetric key algorithm to conduct confidential online communications. The use of the modulo function ensures that both parties can calculate the same secret key value, but an eavesdropper cannot. An eavesdropper can intercept the values of g and p , but because of the extremely difficult mathematical problem created by the use of a large prime number in mod p, the eavesdropper cannot feasibly calculate either secret value x or secret value y . The secret key is known only to each party and is never visible on the network.



B. Data Encryption Standard (DES)

There are two main types of cryptography in use today –**symmetric**or secret key cryptography and **asymmetric** or public key cryptography. Symmetrickey cryptography is the oldest type whereas asymmetric cryptography is only beingused publicly since the late 1970's. Asymmetric cryptography was a major milestonein the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here.It involves the use of only one key which is used for both encryption and decryption(hence the use of the term symmetric). Figure 2.1 depicts this idea. It is necessary forsecurity purposes that the secret key never be revealed.

To accomplish encryption, most secret key algorithms use two main techniques knownas substitution and permutation. Substitution is simply a mapping of one value toanother whereas permutation is a reordering of the bit positions for each of the inputs.These techniques are used a number of times in iterations called rounds. Generally,the more rounds there are, the more secure the algorithm. A non-linearity is alsointroduced into the encryption so that decryption will be computationally infeasible without the secret key. This is achieved with the use of S-boxes which are basicallynon-linear substitution tables where either the output is smaller than the input or viceversa.

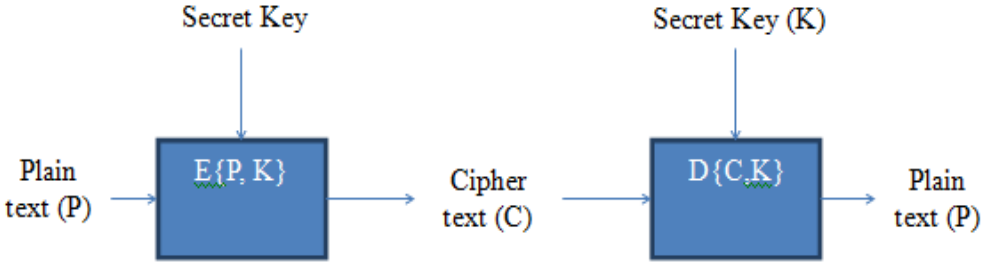


FIG. 2: SECRET KEY ENCRYPTION

One of the main problems with secret key cryptography is key distribution. For this form of cryptography to work, both parties must have a copy of the secret key. Thiswould have to be communicated over some secure channel which, unfortunately, is not that easy to achieve. As will be seen later, public key cryptography provides a solution to this.

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure(known as a feistel network).

C. Overall Structure

The algorithm's overall structure is shown in Figure 1: there are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). IP and FP have no cryptographic significance, but were included in order to facilitate loading blocks in and out of mid-1970s 8-bit based hardware.

Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes — the only difference is that the subkeys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

The $\oplus$ symbol denotes the exclusive-OR (XOR) operation. The F-function scrambles half a block together with some of the key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.

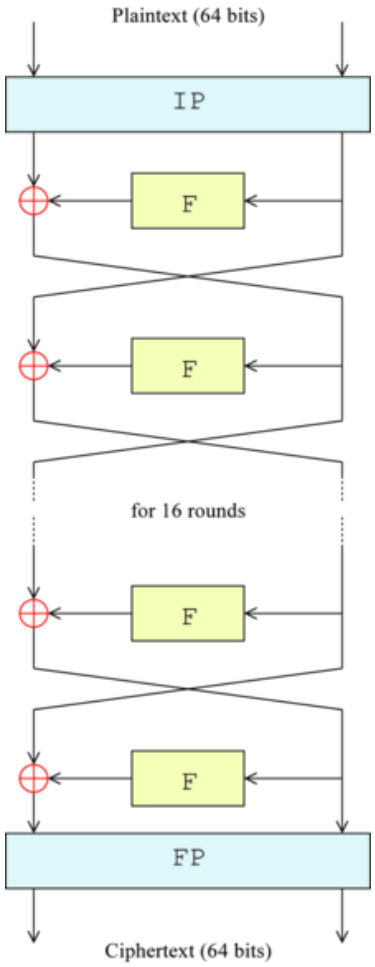


Fig.3. Overall feistel structure of DES

The F-function, operates on half a block (32 bits) at a time and consists of four stages:
Expansion — the 32-bit half-block is expanded to 48 bits using the *expansion permutation*, denoted *E* in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 * 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.
Key mixing — the result is combined with a *subkey* using an XOR operation. 16 48-bit subkeys — one for each round — are derived from the main key using the *key schedule* (described below).
Substitution — after mixing in the subkey, the block is divided into eight 6-bit pieces before processing by the *S-boxes*, or*substitution boxes*. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES — without them, the cipher would be linear, and trivially breakable.
Permutation — finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the *P-box*. This is designed so that, after permutation, each S-box's output bits are spread across 4 different S boxes in the next round.
The alternation of substitution from the S-boxes, and permutation of bits from the P-box and E-expansion provides so-called "confusion and diffusion" respectively, a concept identified by Claude Shannon in the 1940s as a necessary condition for a secure yet practical cipher.

IV. ADVANTAGES OF CLOUD COMPUTING

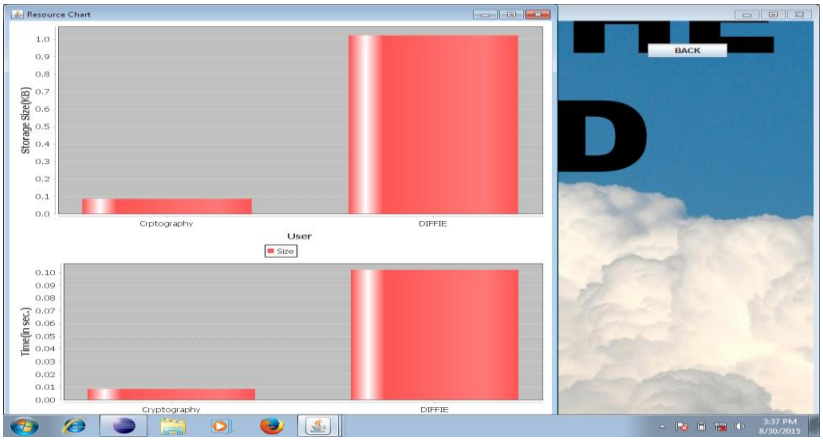
- **Reduced Cost**: Cloud technology is paid incrementally, saving organizations money.
- **Increased Storage**: Organizations can store more data than on private computer systems.
- **Highly Automated**: No longer do IT personnel need to worry about keeping software up to date.
- **Flexibility**: Cloud computing offers much more flexibility than past computing methods.
- **More Mobility**: Employees can access information wherever they are, rather than having to remain at their desks.
- **Allows IT to Shift Focus**: No longer having to worry about constant server updates and other computing issues, government organizations will be free to concentrate on innovation.
- **Bonus advantage**: In a cloud computing environment resources can be shared across applications as well as customers resulting in greater use of the resources for a similar energy cost. For corporations spread over different time zones the computing power lying idle at one geographic location (during off-work hours) could be harnessed at a location in a different time zone. This reduces not only the power consumption but also the

amount of physical hardware required. With cloud computing, virtual offices can be quickly set up and employees can easily work from home.

- **Reliability:** With a managed service platform, cloud computing is much more reliable and consistent than in-house IT infrastructure. Most providers offer a Service Level Agreement which guarantees 24/7/365 and 99.99% availability. Your organization can benefit from a massive pool of redundant IT resources, as well as quick failover mechanism - if a server fails, ***hosted applications and services can easily be transited to any of the available servers.***

Manageability: Cloud computing provides enhanced and simplified IT management and maintenance capabilities through central administration of resources, vendor managed infrastructure and SLA backed agreements. IT infrastructure updates and maintenance are eliminated, as all resources are maintained by the service provider. You enjoy a simple web-based user interface for accessing software, applications and services – without the need for installation - and an SLA ensures the timely and guaranteed delivery, management and maintenance of your IT services.

V. COMPARATIVE ANALYSIS OF TWO METHODS USED ON THE BASIS OF STORAGE AND TIME



VI. CONCLUSIONS & FUTURE SCOPE

This paper uses the concept of AES and 3DES to obtain a model which can be used for uploading the data into the cloud server by encrypting data and downloading the data from cloud server by decrypting the same data. Nowadays as the power of computers is growing day by day, it is very important to design strong encryption algorithms. Thus the model gives a better non linearity to the plain AES and as it is merged with 3DES, there is better diffusion. Hence the possibility of an algebraic attack on the model is reduced.After performing the comparative analysis for Cryptography and Diffie Hellman algorithms, we found that Cryptographic methodology is better to use. According to the final results achieved by us, the cryptographic methodology proved to be superior on the basis of two parameters, storage space and time taken to achieve the results.

ACKNOWLEDGMENT

I am grateful to numerous local and global peers who have contributed towards shaping this thesis. At the outset, I would like to express my sincere thanks to Assistant prof., Mr. Alok katiyar for his advice during my thesis work. As my supervisor,he has constantly encouraged me to remain focused on achieving my goal. His observations and comments helped me to establish the overall direction of there search and to move forward with investigation in depth. He has helped me greatly and been a source of knowledge.

I am really thankful to my all friends and to everyone who has provided me with kind words, a welcome ear, new ideas, useful criticism, or their invaluable time, I am truly indebted.

I would also like to thank my parents and sister for standing beside me all the time and support me morally and ethically.

I must acknowledge the academic resources that I have got from IPEC.I would like to thank administrative and technical staff members of the department who have been kind enough to advise and help in their respective roles.

Last, but not the least, I would like to dedicate this thesis to my family, fortheir love, patience, and understanding.

REFERENCES

[1] Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing(draft)." NIST special publication 800.145 (2011): 7.

[2] Jaydeep. "Security and Security and Privacy PrivacyPrivacy Issues in Cloud Computing." http://arxiv.org/.

[3] "Cloud Computing Architecture".http://communication.howstu works.com/cloud- computingl.htm.

[4] Brodkin, Jon. "Gartner: Seven cloud-computing security risks." Infoworld(2008): 1-3.

[5] Calheiros, Rodrigo N., et al. "Cloudsim: A novel framework for modelling and simulation of cloud computing infrastructures and services." arXiv preprintarXiv:0903.2525 (2009)

[6] Ogbu, Richard Chukwu, and IfeanyiUgbagaNkole. "Cloud Computing: A review."

[7] Shamir, Adi. "How to share a secret."Communications of the ACM 22.11 (1979): 612-613.

