International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 8 (August '2017)

GENERATED OTP VALUE IS ENCRYPTED USING BLOWFISH ALGORITHM IN CLOUD SECURITY

S.Meena,
M.Phil Research Scholar,
PG & Research Department of Computer Science,
Vivekanandha College of Arts & Sciences for Women (Autonomous),
Tiruchengode, Tamil Nadu, India.

Dr.N.Kowsalya,
Assistant Professor,
Department of Computer Science &Applications,
Vivekanandha College of Arts & Sciences for Women (Autonomous),
Tiruchengode, Tamil Nadu, India.

Abstract: Today most of the sensitive data are stored in a third party systems may cause severe security problem. Security as a service in a cloud model integrates their security services into a corporate infrastructure. The proposed Work focused on the security platform to store and retrieve files on the cloud with onetime password protection. To enhance the security level of One Time Password by Encrypting it and logging the user by forwarding the encrypted OTP with Password to the system. It increases the security level of the system. The web server generates the Encrypted OTP using Blowfish algorithm sends it to the users mobile. OTP is an encrypted format, so users can't read it. In this approach user's information are verified in many levels. It avoids the unauthorized logging.

Keywords: Security, OTP, Encryption, Blowfish algorithm.

I.INTRODUCTION

Cloud Computing is associated with a new paradigm for the provision of computing infrastructure. This paradigm shifts the location of this infrastructure to the network to reduce the costs associated with the management of hard-ware and software resources [1]. The Cloud is drawing the attention from the Information and Communication Technology (ICT) community, thanks to the appearance of a set of services with common characteristics, provided by important industry players. Depending on the type of provided capability, there are three scenarios where Clouds are used in following services.

- **Infrastructure as a Service:** IPs manage a large set of computing resources, such as storing and processing capacity. Through virtualization, they are able to split, assign and dynamically SPs, that will deploy on these systems the software stacks that run their services. This is the Infrastructure as a Service (IaaS) scenario.
- **Platform as a Service:** Cloud systems can an additional abstraction level instead of supplying a virtualized infrastructure, they can provide the software platform where systems run on. The sizing of the hardware resources demanded by the execution of the services is made in a transparent manner. This is denoted as Platform as a Service (PaaS). A well-known example is the Google Apps Engine [2].
- **Software as a Service:** Finally, there are services of potential interest to a wide variety of users hosted in Cloud systems. This is an alternative to locally run applications. An example of this is the online alternatives of typical applications such as word processors. This scenario is called Software as a Service (SaaS).

The vast spread of Internet resources on the web and fast growth of service providers enabled cloud computing systems to become a large scaled IT service model for distributed network environments [3]. Single static passwords are also vulnerable to social engineering, i.e., people asking for passwords or guessing them correctly. It is having many chance to others can accessing their personal accounts, otherwise we need to change the password repeatedly. To overcome these drawbacks new method is invented that is called "One Time Password (OTP)". OPT is a password that is valid for only one login session or transaction.

At the system end encrypted OTP is decrypted and verify the OTP, Password and mobile number for a particular username One Time passwords as the name suggests are passwords that can be used only one time, you need not remember the same. It has an expiry Time on how long after it has been issued, the password remains valid. It can be valid for 5 minutes only. One time passwords are not vulnerable to replay attacks, since the password cannot be used again. It is sent to a person's registered cell phone via SMS, Hence the name SMS based OTP and they are expected to enter it on a website.[4] The introduction of OTP is intended to reduce the possibility of fraudulent transactions and safeguard customers. However, SMS OTP as a form of online security is fraught with few deficiencies and is not difficult to hack.

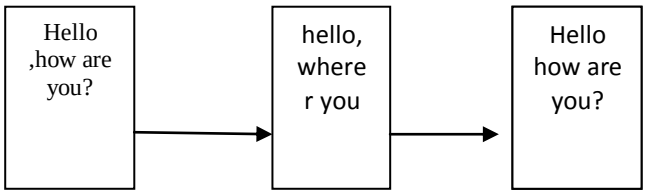


Figure 1: Encryption Decryption Process

II.RESEARCH OBJECTIVES

For the development of security solutions vast challenges have been faced in the cloud computing environment In particular, an organization faces challenges on files security

and it tries maximum authentication over files while distributing to the user. Cloud data should be secure and reliable otherwise unauthorized user can easily get the cloud user's confidential information. In cloud all the accounts were accessed with the same password which is very insecure& third party cloud computing doesn't provide proper security to the cloud data . This is the serious issues in cloud computing environment because static password can be hacked by hackers .This may lead to data find out that exact user who communicates with third party that is through any guilt agent[5].

AES is based on a design principle known as a substitution-permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits . AES operates on a 4×4 column-major order matrix of bytes, termed the state. Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128 bit keys.
- 12 cycles of repetition for 192 bit keys.
- 14 cycles of repetition for 256 bit keys.

Each round of encryption process requires the following four types of operations: Sub Bytes, Shift Rows, Mix Columns, Xor Round key. Decryption is the reverse process of encryption and using inverse functions: InvSub Bytes, InvShift Rows, InvMix Columns [6].

The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption.DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. Once the go-to, symmetric-key algorithm for the encryption of electronic data, DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm. The simplicity of DES also saw it used in a wide variety of embedded systems, smart cards, SIM cards and network devices requiring encryption like modems, set-top boxes and routers.

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key.

III. BLOWFISH ALGORITHM

Generated OTP value is encrypted using powerful Blowfish algorithm and sends it to users. Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc. Blowfish is a symmetric block encryption algorithm designed in consideration with,

Fast: It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
Compact**:** It can run in less than 5K of memory.
Simple: It uses addition, XOR, lookup table with 32-bit operands.
Secure: The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length.

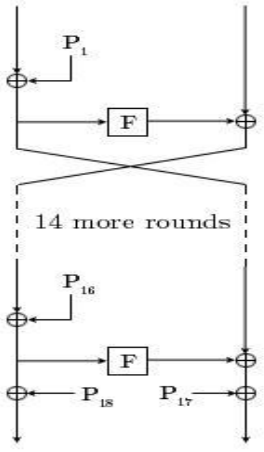
It takes a variable length key, ranging from 32 bits to 448 bits; default128 bits.

Algorithm	Block size	Key size	performance	security
DES	64	56	low	less
3DES	128	168	low	less
AES	128	128-256	medium	secure
Blowfish	64	32-448	fast	More secure

Figure 2: comparison of encryption algorithm

Security Analysis:
A change in one bit of the plain text or one bit of the key should produce a change in many bits of the cipher text. A desirable feature of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. If the changes are small, this might provide a way to reduce the size of the plaintext or key space to be searched and hence makes the cryptanalysis very easy. So, in order to say that any cryptographic algorithm is secure, this is the reason why we have considered Avalanche effect for comparing security of our modified algorithm with that of original Blowfish algorithm.

Its working is almost similar to DES but in DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key is large [7] and it can vary from 32 to 448 bits. Blowfish also consists of 16 rounds like DES [8]. Blowfish algorithm can encrypt data having size multiple of eight and if the size of the message is not multiple of eight than bits are padded. It is suitable for applications where the key does not change often, like communication link or an automatic file encryption. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks.



A) Description of Algorithm:
Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follow the feistel network and

this algorithm is divided into two parts: key expansion, Data encryption

B).Key-expansion:
It will converts a key of at most 448 bits into several sub key arrays total 4168 bytes. Blowfish uses large number of sub keys. These keys are generate earlier to any data encryption or decryption. The p-array consists of 18, 32-bits subkeys:P1,P2….,P18. Four 32-bit S-Boxes consists of 256 entries .

C) Data Encryption
It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution all operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

In Blowfish algorithm also 64 bits of plain text is divided into two parts of size 32 bits. One part taken as the left part of message and is right part of message. The left part is XOR with the elements of P-array which creates some value, then that value is passed through transformation function F. The value originated from the transformation function is again XOR with the other half of the message i.e. with right bits, then F| function is called which replace the left half of the message and P| replace the right side message.

D) The sub keys are calculated using the Blowfish algorithm:

i. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
ii. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
iii. Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).
iv. Replace P1 and P2 with the output of step (3).
v. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.
vi. Replace P3 and P4 with the output of step (5).

Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm. In total, 521 iterations are required to generate all required sub keys. Applications can store the sub keys rather than execute this derivation process multiple times.

Algorithm: Blowfish Encryption
Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and

Blowfish algorithm over other algorithms in terms of the processing time. It can also be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES[9]. It requires always more time than DES because of its triple phase encryption characteristics.

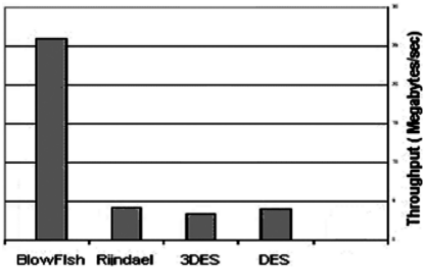


Figure4: Throughput of each encryption algorithm

We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. Finally, Triple DES (3DES) still requires more time than DES.

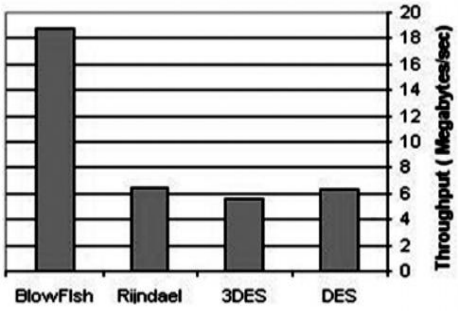


Figure5: Throughput of each decryption algorithm

In mobile based technology user no need to enter OTP manually, because of security reasons OTP is encrypted and sends to mobile. User just read the mail for verification and type application password with that encrypted OTP and sends it to the system Web server is used to send mail to user. In this technology others can't try to enter OTP, if others can mean they don't know the application password. Using this we can verify users OTP, Password and mobile number also. It provides the highest level of authentication for the system.

Performance:
Blowfish is still one of the more efficient algorithms due to the fact that it can be implemented using simple operations that a microprocessor can execute quickly. Quality implementation of Blowfish do not use variable length shifts or conditional jumps that take more processing time for a microprocessor to execute. The goal of the experiment was to see whether fake objects are accesses from the distributed data sets yields significant improvement in our chances of detecting a guilt agent. After that we evaluate onetime

password technique to detect the data leakage and it helps to prevent the data to be leaked.

IV. CONCLUSION

Data security and privacy are the major challenges in cloud computing for data forward in cloud computing. In this paper, the first step performs data encryption and decryption which ensures data security. To enhancing the performance of the One Time Password to provide Authentication for System. This approach provides the high level authentication to the system by verifying the user's Password, OTP and mobile number. In this method somewhat system load is increased by encrypting and decrypting of OTP for multiple users. In the future, how to reduce the system load and increase system performance while using this approach.

V.REFERENCES

[1] Michael Miller, "Cloud Computing Web-Based Applications that change the way you work and Collaborate Online", Pearson Education, 2012 .
[2] Ahmad Alamgir Khan, "Preventing Phishing Attacks using One Time Password and User MachineIdentification",International Journal of Computer Applications (0975 – 8887) vol. 68– No.3, April 2013
[3] Papadimitriou P and Garcia-Molina, "Data Leakage Detection" Knowledge and Data Engineering, IEEE Transactions on vol.23, No.1, Pp (51-63), Jan 2011.
[4] William Stallings, cryptography and network security, pearson prentice hall, 2006, 4th edition.
[5] Pratap Chandra Mandal, 'Superiority of Blowfish Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X vol. 2, No. 7.
[6] G. Devi and M. Pramod Kumar, 'Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm', International Journal of Computer Trends and Technology. (2012) vol. 3 No. 4, ISSN:2231-2803,Pp.592-596.
[7] Brian Hayes.Cloudcomputing. Communications of the ACM, July 2008.
[8] Pratap Chandra Mandal, 'Superiority of Blowfish Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X vol. 2, No. 7.
[9] Schneier, "The Blowfish Encryption Algorithm",Dr.Dobb's Journal, Pp.38-40, April1994.

