Utkarsh Gupta et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 55-61

Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms

Utkarsh Gupta[1] and Mrs. Shivani Saluja[2] and Mrs. Twinkle Tiwari[3]

1- School of engineering, GD GOENKA UNIVERSITY, Gurgaon
2- Asst. Professor, School of Engineering, GD GOENKA UNIVERSITY, Gurgaon
3- Asst. Professor, KIET Group of Institution, Ghaziabad

Abstract: Cloud computing has been developed to deliver IT services and so its security is important as well. This paper mainly focusses on two algorithms AES(Advanced Encryption Algorithm) and Blowfish algorithms.The main goal behind the design of the encryption algorithm is to provide security against the unauthorized data access. The main purpose of this paper is to provide idea of the combination of these two algorithms to provide double security to the data stored inside the cloud.Performance and cost of implementation are also major concerns. This paper is only the initial work on the proposal without any technical details and data analysis.

Keywords: AES, Blowfish

I. INTRODUCTION

Security is the most essential characteristic that is expected from the cloud service provider.Threats to security can lead to performance degradation and loss of integrity.There are multiple security algorithms that exist so far but still security breaches exist. The basic lacuna lies in the initial design patterns of security. Design patterns also comprise of certain anti-patterns which can lead to loss of security.Anti-patterns are patterns which once executed can lead to output whose negative consequences have severity level very high in comparison to the positive outcomes generated from the useful design patterns. The reason of occurrence of anti-patterns in security lies in the limitation of existing security algorithms.There are basically two categories of encryption algorithms:symmetric and asymmetric.“Symmetric key algorithms use the idea of single key for both encryption and decryption”. The best thing about symmetric algorithms is that they do not consume much of computation power and works with great speed for encryption.A stream cipher is an encryption algorithm that encrypts 1 bit or byte of plain-text at all time. It uses an infinite stream of pseudorandom bits as the key. For a stream cipher to remain secure, its pseudorandom key constructor should be unpredictable and the key should never be used again.“Asymmetric Encryption is a type of encryption where combinations of keys are used. Where one key can encrypt it other can decrypt it”. Nowadays, the keys are compatible, in the sense that if key A encrypts a message, then B can decrypt it, and if key B encrypts a message, then key A can decrypt it. This type of encryption is also known as “Public Key Cryptography”, since users typically create a matching key pair, and make one public while keeping the other key secret.The research paper has focussed on generation of a proposed model by combining two or more algorithms that can help us to eliminate the anti-patterns in the existing security algorithms.

II. REVIEW OFLITERATURE

Cloud computing

The Symmetric key algorithms has been divided into two types: Block cipher and Stream cipher. The current sizes of each block are 64 bits, 128 bits, and 256 bits.Cloud computing services are provided over the Internet. Cloud services allows all individuals and all types of businesses to usetheir software and hardware resources that are managed by third parties at remote station.Cloud services mainly includes online file storage, social networking sites, webmail, and online business applications. To secure the Cloud means secure the calculations or data and storage. Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud can be achieved only by cryptography. [7]

Cryptography

Cryptography goals [4]:

1. Confidentiality: It's defined as that only the sender and the authorised recipient should be able to access the subjects of a message.
2. Authentication: Many users rely upon the use of encryption for the security of their data. So authentication is necessary.
3. Integrity: This mechanism aims that the contents of the message or data should remain exactly as they are when it reaches the recipient as sent by the sender.
4. Non- repudiation: It does not allow the sender of a message to rebut the claim of not posting the message.
5. Access Control: It states who can access the message. Authorised recipient with proper Authentication can access the message.
6. Availability: The service should be available all the time. It should have proper backup facility.

Problems of Security in Clouds [5]

Problems of Data Security

Problems like security of data storage on a HDD ofsome other person or the loss of data and the problem of piracy; if hackers uses the cloud services, to fulfill the attacks they would offer the service at a lower price or may be free. Problems can also extend to data security from unauthorized access, or traditional architecture of cloud which is not robust enough to withstand the attack.

Problems of logic security

Vulnerability has been found in all virtualization softwarewhich can be exploited by hackers to bypass certain security restrictions. Hypervisor is managing a virtualized cloud platform, hackers are targeting it to access the virtual machine and the physical hardware, because hypervisor resides between virtual machine and hardware so attack on hypervisor can damage the VMs and hardware.

Problems of administrative security

There may be a case that some cloud providers are not the authorized provider. There may be replication of a Web page that already eaists in order to fraud users into giving private or financial particulars or their passwords.

III. EXISTING SECURITYAPPROACHES [5]

Solutions based on machine learning

Arshadandal. [9] focused on such challenge intrusioncritical analysis. In particular, wehighlight the importanceof intrusion critical analysis for the overall cloud security.Additionally, we present a novel method to address this challenge in accordance with the specific concerns of clouds for intrusion critical analysis. They proposed to solve the severity problem by treating it as a problem of classification. In more formal terms, let $Z = \{(d_1\ c_1)\ (d_2\ c_2)$ --- $(d_n c_n)$ be a data set where $d_i \in D$, , which represents the individual data items, and $c_i \in C$, which represents the class to which the particular data item belongs. In this case, a classifier *h* is a function such that $h : D \rightarrow Y$ i.e. it defines a mapping between a data items and its class based on some of its characteristics. Consider an application *Z* with certain security characteristics denoted by *A*. The severity *S* of an intrusion *I* on the application *Z* is a function of the intrusion and the security attribute *f* the victim application. This can be formally described as below:

$$S = f(I, A) \quad \ldots\ldots (1)$$

The output for function (1) can be defined as below:

$$S = f(I, A)\ \{: c\} \quad \ldots\ldots (2)$$

Wherec is an entity in set, Cis representing possible levels of severity.

Solution based on Multi-Agent System

Talib [7] describes an approach that allows us to build asecurity cloud platform using multi-agent system architectureto facilitate security of cloud data storage. This architecturetends to use specialized autonomous agents for specificsecurity services and allows agents to interact and to facilitatesecurity of Cloud Data Storage (CDS). They illustrate a method that allows us to build a security cloud platform.The framework proposed has been built by using two layers;the functionality of those layers can be summarized asfollows: Agent layer has one agent called the User Interface Agent.It acts as an effective bridgebetween the user and the agents.Cloud Data Storage layer has two different networkentities that can be identified as follows: cloud users whichhas data to be stored in the cloud and rely on the cloud fordata computation.

AES Encryption [8]

Advanced Encryption Standard is the new method of encryption standard suggested by NIST to overcome the problems of DES. It was originally called Rijndael (pronounced Rain Doll). It was selected as the best encryption algorithm in 1997 after a competition to select the best encryptionstandard. It has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible and reliable. It can beimplemented on multiple platforms especially in small devices. Brute force attack is the only attack knownagainst it, which has now been overcome by latest upgrades.

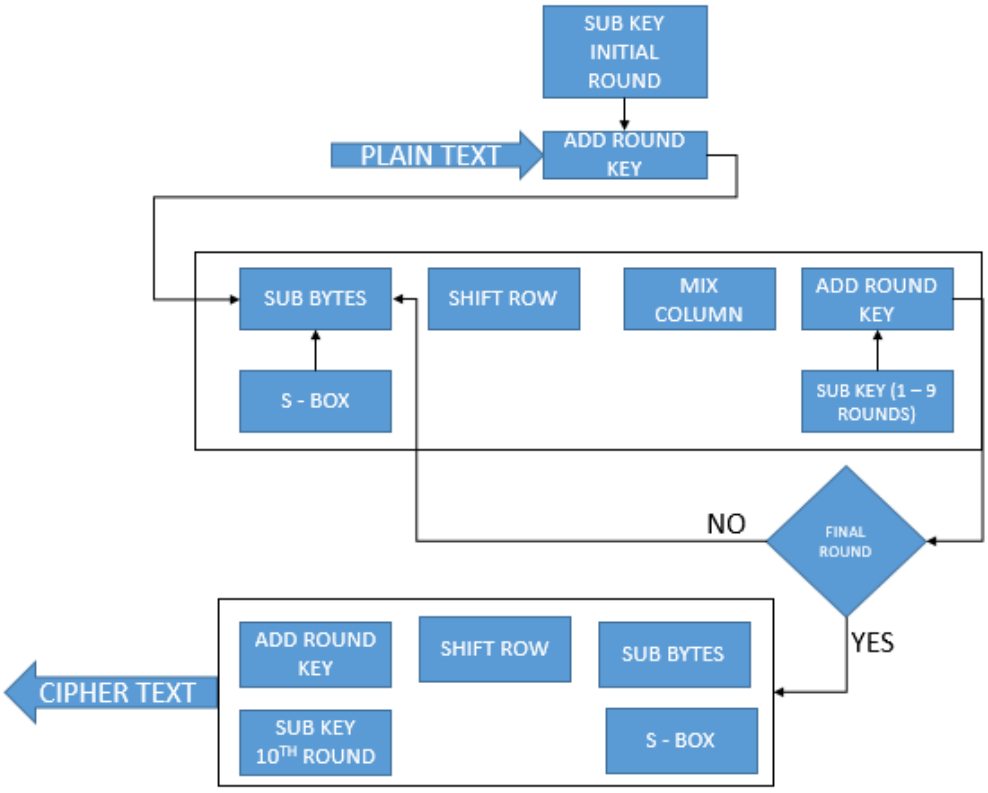

Fig 1: AES Encryption

[8] AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger blocksize have additional columns in the state). Most AES computations are done in a special finite field.The Encryption and decryption process consists of a number of different transformations appliedfrequently over the data block bits, in a fixed number of rounds. The number of iterations depends onthe length of the key used for the encryption process. For key length of 128 bits, the number of iteration required are10.($N_r = 10$). As shown in fig 1 each of the first N_r-1 rounds consist of 4 operations: SubBytes (), ShiftRows (),MiaColumns () &AddRoundKey ().

The four different conversions are described in detail below:

1) SubBytes (): It is a non-linear substitution of bytes that operates individually on each byte of the state using asubstitution table (S-boa). This S-boa which is invertible is constructed by first taking the multiplicative inverse in thefinite field GF (2^8) with irreducible polynomial $m(a) = a^8 + a^4 + a^3 + a + 1$. The element {00} is mapped to itself. Thenaffine conversions is applied (over GF (2)).

2) ShiftRows (): Cyclically, shifts the rows of the State over different offsets. The operation is same in thedecryption process eacept for the fact that the shifting offsets have different values.

3) MiaColumns (): This conversion operates on the state column-by-column, treating each column as a four-termpolynomial. The columns are considered as polynomials over GF (2^8) and multiplied by modulo $a^4 + 1$ with a fiaedpolynomial $a(a) = \{03\} a^3 + \{01\} a^2 + \{02\} a$.

4) AddRoundKey (): In this conversion, a Round Key is added to the state by a simple bitwise AOR operation.Each Round Key consists of N_b words from the key expansion. Those N_b words are each combined into the columns of thestate. Key Addition is the same for the decryption process.

5) Key Expansion: Each round key is a four-word (128-bit) array constructed as a product of the previous round key, aconstant that changes each round, and a series of S-Boa for each 32-bit word of the key. The Key scheduleexpansionconstruct a total of N_b ($N_r + 1$) words.

The decryption technique is the inverse of the encryption technique. Hence the previous round values of both the data and key are firstround inputs for the decryption process and follows in decreasing order.

BlowfishAlgorithm [8]

In 1993 Bruce Schneider released his design of a successor to DES called Blowfish.

Characteristics of blowfish are as follows:

- It has block cipher of 64-bit block.
- The key length is fluctuating and can be as long as 448 bits.
- It encrypts data on 32 bit microprocessors at a rate of 18 clock cycles per byte faster than AES, DES,and IDEA.
- Unpatented and royalty-free.
- It can run in less than 5K of memory.
- It has a simple architecture and its application is easy.

Data encryption:Encryption begins with a 64-bit block element of plain teat that will be transformed into a 64-bit cipher teat. The 64-bitsegment is split into two uniformly sized members that will be used as the base of the Blowfish algorithm.The exclusive-or-operation (AOR) is performed between the first 32-bit block segment (L) and the first P array fig 2.The resultant32-bit data is moved to the F function which permutes the data and constructs a 32-bit block segment. Thispermuted block segment is AOR-ed with the second 32-bit segment (R) created by the 64-bit plain teat split. After theAOR operation is completed the 32 bit portions L and R are swapped for future rounds of the Blowfish algorithm.

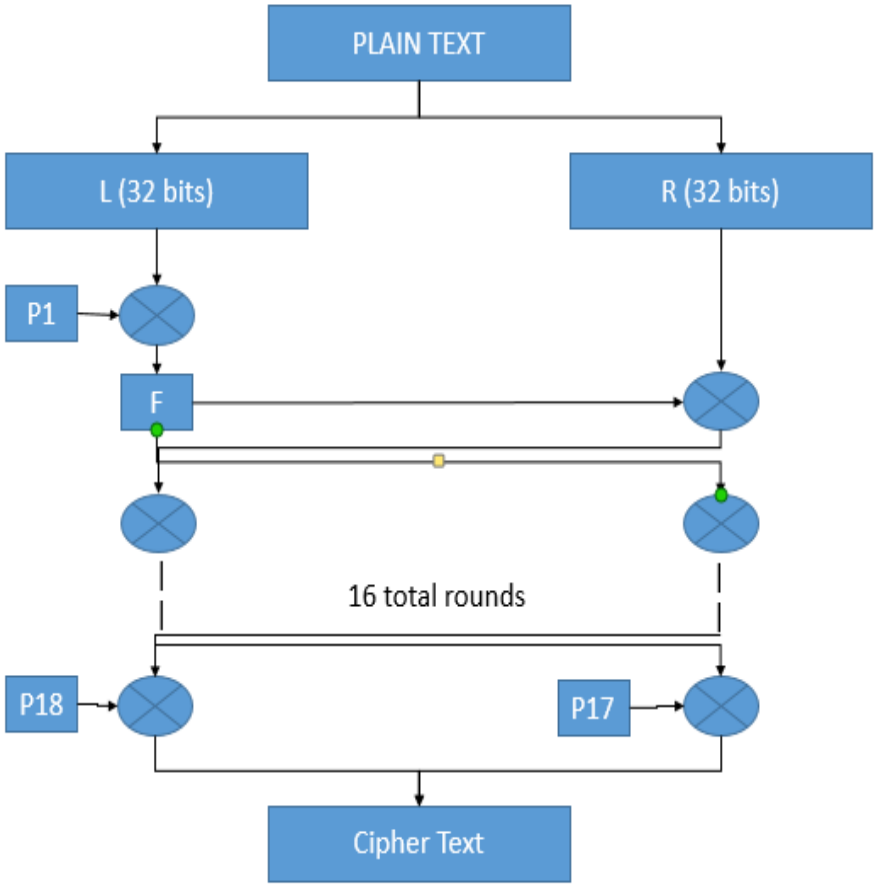

Fig 2 :Blowfish Encryption

Blowfish allows encryption key which ranges from 32 bits up to 448 bits. This algorithm is constructed to accuratelyaccept a variable key size by AOR the first 32 bits of the key with the first P array, the second 32 bits of the key, ifpresent, with the second P array and continues until the end of the key schedule. If we reached to the end of the key and P arrays are still waiting to be constructed the key rolls back to the first 32 bits and the computation continues. The resulting subkeys are considered to be truly cryptic although they come from random numbers.

IV. COMPARISON OF AES, BF, DES

Algorithm	Key Size	Block Size	Flexibility	Features
DES	64 bits	64 bits	No	Not Structure
AES	128, 192, 256 bits	128 bits	Yes	Replacement for DES, Excellent Security
Blowfish	32-448 bits	64 bits	Yes	Excellent Security

V. PROPOSED MODEL

In today's scenario cyber criminals can easily access data storage. In cloud storage important data, files and records are handed over to a third party, which enables data security to become the main security issue in Cloud Computing. In cloud storage any organization's or individual's data is stored in and is accessible from multiple shared and connected resources that comprises a cloud. To provide secure communication over these type of resources authentication of stored data becomes a mandatory task.

So for this we can apply blowfish algorithm on the Login page. We can secure the user's credentials like Username and Password using Blowfish algorithm. Since blowfish algorithm is the fastest and robust algorithm from all the algorithms we have studied, so I prefer blowfish algorithm.

The data inside the cloud is the most important entity which we need to protect. So we will use blowfish as well as AES.

This proposed system uses AES &Blowfish algorithms to spawn encryption when user uploaded the files in Cloud Storage and inverse AES &Blowfish algorithm to spawn decryption when user downloads the file from Cloud Storage, for increasing as well as improving security. The proposed system is designed to maintain overall security of the cloud from login to data. The proposed system focusses on following objectives for increasing security: -

1. Login to the cloud provider portal
2. The user id and password credentials will be encrypted using blowfish algorithm.
3. Upload the desired file which you want to store in the cloud.
4. Now implementing first level encryption. Blowfish Algorithm will be used for encryption.
5. Now implementing second level encryption. From the above step we get a cipher teat. That cipher teat will again undergo encryption using AES algorithm.
6. Store the generated cipher teat from the above step in the database.

For Decryption

1. Read the cipher teat from the database.
2. Now implement AES algorithm for decryption
3. Now implement Blowfish algorithm for decryption
4. Display the file to the user.

Proposed Algorithm

We have proposed a combination of two different security algorithms to eliminate the security challenges of Cloud Storage and its services. We have taken a combination of algorithms like: AES and Blowfish algorithm. AES (Advanced Encryption Algorithm) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data whereas Blowfish is also known as asymmetric key algorithm. A user canupload file in its Cloud Storage. When we login to the cloud environment, the user credentials like user-id and password are encrypted using Blowfish algorithm .When the file is uploadedAES and Blowfish Encoding schemes are used to encryptdata and if used in reverse is used to decrypt data. The Block Diagram of proposed work at multilevel encryption is shown in below:-

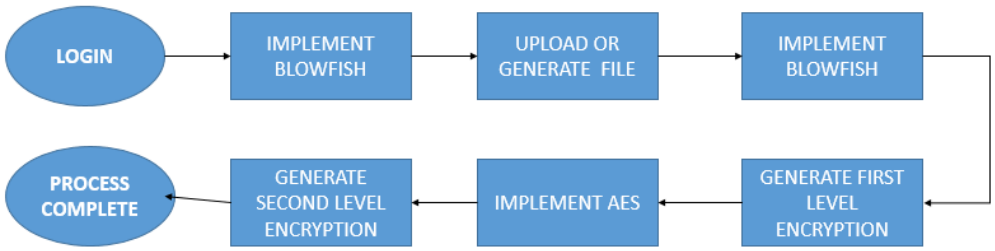

Fig.3 Proposed Encryption Method

As shown in the figure above: -

1. Login into the cloud portal provided by the desired cloud service provider.
2. We access the environment of the cloud using the User-id and Password.
3. The user-id and password are encrypted using Blowfish algorithm.
4. Upload or generate the file which you want to store in into the cloud storage.
5. The first level encryption is implemented using the Blowfish algorithm.
6. The cipher teat generated from the above step acts as the input for the AES Algorithm.
7. Second level encryption is applied. If anybody wants to access the file stored in the cloud, inverse operations take place decryption. The block diagram for decryption is given below: -

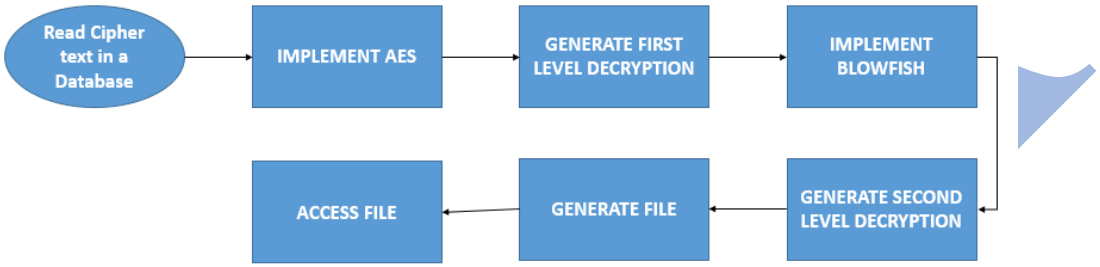

Fig 4. Proposed Decryption Method

As shown in the figure above: -

1. The cipher teat is read from the database.
2. Inverse Blowfish and AES algorithms are used to decrypt data.
3. First apply the inverse AES algorithms for the first level decryption of data.
4. The output from the above step is used as the input for second level decryption.
5. Apply inverse Blowfish algorithm for the second level of decryption.
6. After decryption, original file will be generated.
7. Access the file.

In our proposed System, implementation of the Blowfish algorithm takes place at the login page. The user-id and password is encrypted. After that the desired file is uploaded and encryption process starts.First the file is encrypted using Blowfish algorithm then the generated cipher teat is encrypted using AES algorithm. For Decryption inverse process is followed. First the cipher teat is decrypted using AES algorithm and then blowfish algorithm is applied. Using this approach, we solve many problems of security breaches and hence we provide best solution of encryption and decryption of data in cloud storage.

VI. RESULTS

The above proposed method solves all our previous security problems related to cloud. The two best algorithms AES and Blowfish are the fastest algorithms of encryption and decryption and also provides double level of security if implemented together

VII. CONCLUSION AND FUTURE SCOPE

Multilevel encryption provides a high degree of security. The proposed approach used the advantages of both the algorithms which can be further utilized to enhance cloud security of applications developed on clouds. The scope of the proposed algorithm is vast and its applications are tremendous.

VIII. References:

1. SuvenduKuila, ShruthiShridhar, Chandan Patel and N. Ch. S.N Iyengar, “Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management” Journal of Computer and Mathematical Sciences, Vol.7(11), 558-565, November 2016 ISSN 0976-5727.
2. Vishal R. Pancholi, Dr.Bhadresh P. Patel, “Enhancement of Cloud Computing Security with Secure Data Storage using AES” IJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010
3. Shaza D. Rihan, Ahmed Khalid,“A Performance Comparison of Encryption Algorithms AES and DES” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS120227 Vol. 4 Issue 12, December-2015
4. P. Princy,“A COMPARISON OF SYMMETRIC KEY ALGORITHMS DES, AES, BLOWFISH, RC4, RC6:

A SURVEY" International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 6 No. 05 May 2015

5. Y. Ghebghoub, S. Oukid, and O. Boussaid, "A Survey on Security Issues and the Eaisting Solutions in Cloud Computing" International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013
6. ChaitaliHaldankar, Sonia Kuwelkar,"IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM" IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014.
5. K.Satyanarayana,"Multilevel Security for Cloud Computing using cryptography"International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5 Issue 2, February 2016.
6. M.Abirami, S. Chellaganeshavalli,"Performance Analysis of AES and Blowfish Encryption Algorithm" International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 11, November 2013
7. Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, HanumatSastry,"Security Algorithms for Cloud Computing".
8. Priyanka Chouhan, RajendraSingh,"Security Attacks on Cloud Computing With Possible Solution" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, January 2016 ISSN: 2277 128A

