INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A COST EFFICIENT SECURITY MECHANISM USING BLOW FISH ALGORITHM

Venshila S
Post-Graduate Student
Department of Computer Science and Engineering, Karunya University
Vencyjulie20@gmail.com
India

Jeno Lovesum
Assistant professor
Department of Computer Science and Engineering, Karunya University
jenolovesum@karunya.edu.in
India

Abstract

In cloud computing environment there are various algorithms designed for the data security. Most of the encrypting algorithms is less secure, or fails in any of the cryptographic parameters. Advanced encryption standard algorithm overcomes this drawback. Main disadvantage of algorithm Advanced encryption standard is, mainly because of its key size of length 256 bits, it takes more time for ciphering the data. Proposed algorithm overcomes the disadvantages of advanced encryption standard algorithm. In order to overcome the drawback of Advanced encryption standard algorithm, another algorithm called Blow fish algorithm is used for the security and it is faster than previous. And the uploading time of the data is also calculated which is not calculated in the existing system.

Keywords: security, cryptographic parameters encryption, uploading**.**

1. Introduction

Cloud computing actually represents the convergence of many evolutionary developments and trends in IT and in many ways is a realization of the last 20 years of architecture development. According to Research, cloud computing emerged as three major trends converged:[13] service orientation, virtualization and standardization of computing through the Internet. It starts to all come into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.

Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities. Users are faced with choosing between two different flavors of cloud computing: public versus private. The difference is simple. Where is the cloud deployed? A public cloud is one in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform [13].

1.2 Types of Cloud computing

Cloud computing applications can be broadly divided into the following categories: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[14].

SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere [14].

PaaS in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use application program interfaces (APIs), Website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and Google Apps are examples of PaaS[14].

IaaS like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's API to start, stop, and access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and brings more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed; it's sometimes referred to as utility computing [14].

The benefits of cloud computing to customers are very tangible. The increasing adoption of cloud computing is in recognition of its potential to usher in a new era of responsiveness, effectiveness and efficiency in IT service delivery. With cloud computing, IT professionals can devote more energy to enhancing the value of using IT for their enterprises and less on the day-to-day challenges of IT [14].

2. Related Works

Cloud has started in the year 1960. But it came into use on 1990 as synchronous transfer mode networks. In the year of 21centuries it has the major focus on Software as a Service (Saas). The related author applied many technologies websites like Google and yahoo. This Saas provided in the real time business and successful customers. And finally, after its growth in step by step in the year of 2011. Technique provides new way to authenticate in 3-dimensional approaches. The cloud also uses ASE and SSE techniques. The earlier works were done regarding reliability, integrity and security. Security has not achieved in proper manner. It fails in efficiency also. It lacks in retrievability and cryptographic data storage and in security.

The proposed work provides complete security. And it has good efficiency and availability of data. Although single cloud has enough of security it is less popular, This paper tells about the less security of cloud in the multi clouds of the user[1]. Securing a cloud service and providing privacy protection to customer and his data can be quite a dashing task [2]. Only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it uses RSA algorithm [3]. This tells about the authentication of user in network and also discussed about confidentiality, integrity, write-serializability and read Freshness but double authentication has not discussed here [4]. this paper tells about the security using virtualization, but integrity, availability were not discussed much [5].

3. Introduction

3.1.1 Loading the Data: In loading the data, the load denotes the data storage is and divided into sub sections which are mentioned below such as Classification, Index Building and encryption, Message Authentication Code (MAC) which provide stepwise details of action on the data.

- **Owner Data Classification**
- **Encryption using blowfish**
- **MAC Generation**

3.1.1.1 Registration Process

To access and to upload the data in cloud, the user has to reposit his details for registration in cloud. The details must be included like User id, User name and ip address. Unique user id should be entered. If the given details were satisfied by cloud, the registration will be done successfully, or else until the process gets over that is until the cloud gets satisfied by the details given by the user, he has to perform the same scenario.

3.1.1.2 Request Access:

The user has to access the data which he needs, from cloud. Cloud will look in to the directory, if the user name get satisfies with cloud, it directs the user to owner/cloud. If the authentication process is not satisfied by the cloud, the process should be continued till it matches. Fig 3.2 shows the scenario of request access in detail.

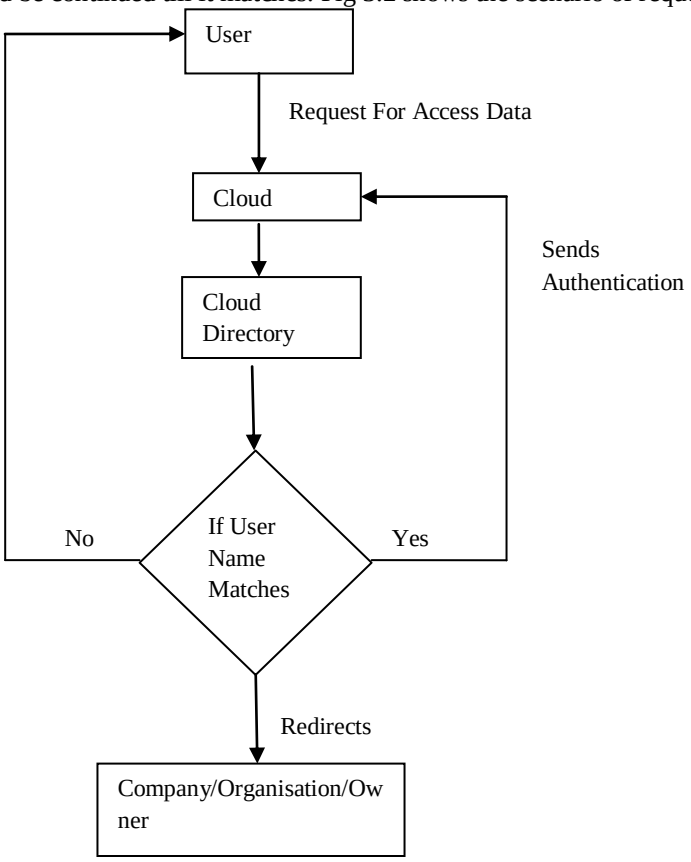

Fig 3.2 Access request

3.1.1.3 Owner Data Classification:

Data to be stored in cloud is sent by the owner. Each and every data uploaded in the cloud must be rated based on some priorities. There should be some priority values Customized by Data-owner for the data upload. Rating can be calculated by using priority rating algorithm. By means of priority values of CIA(Confidentiality, Availability, Integrity), Sensitivity rating(Cr) is calculated. Based on the sensitivity rating, data are classified in the form of Public, Private and Limited Access which in Public data can be access by the public without any authentication. Private accesses are authenticated and Limited Access are more secured, ciphered and authenticated.

Sensitivity score calculation Algorithm:

According to the below given algorithm [9] the data classification is done.

1. Input: Data, protection section, D[]array of n integer size. Where D[] array consisting of C,I,A,SR,R of n integer size.
2. Output: Categorized data for corresponding section.
3. For i=1 to n

Enter the values for confidentiality, integrity and availability.

```
// sr = sensitivity rating;// rin=resuts in
      sr = (c + ((1 / a) * 10) + i) / 2;
         if (sr == 1 || sr == 2 || sr == 3)
            rin = "Public";
          else if (sr == 4 || sr == 5 || sr == 6)
            rin = "Private";
          else if (sr == 7 || sr == 8 || sr == 9)
            rin = "Limited";
```

3.1.1.2 Encryption Using blowfish:

Data files are collected from Data Owner, and send it through encryption process for outsourcing. Assign Index for each data file, send this too outsourcing. Data files which are collected from data owner encrypt with keyword. Safely send keyword and Store to Cloud storage. For each and every data file the list of indexes are generated.

The encryption of data is done by using the blowfish algorithm. After encrypting the data and the index, Mac is generated and combining all that is encrypted data and encrypted index and Mac code the data is stored in cloud.

Proposed Algorithm:

Input: A = plaintext M. {128-bit data
element}.
Step1: D= P (A, P [0]). {P-function to
performed initial permutation}
Step2: Divide D into two 64-bits XL, XR
Step3: For i =1, …, 16 do
Z = F (XLi)
XRi = P[i] XOR Z XOR XRi
Swap XLi and XRi
Step4: Swap Li and Ri undo the last round
Step5: Recombined A=(XL| XR}.
Step6: D=P (A, P[18]).
Output: Ciphertext D.

The proposed blow fish algorithm is used for data encryption [11].

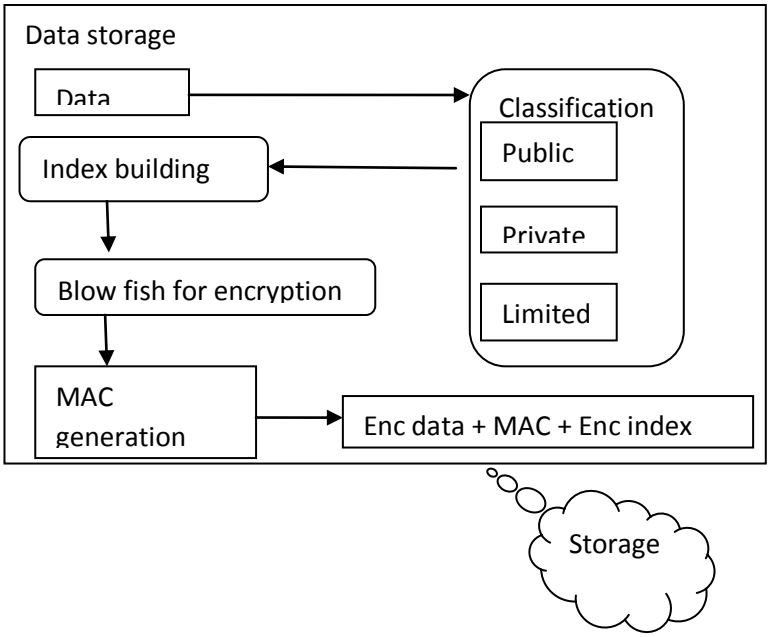

Fig 3.2 Architecture Diagram For Data Storage

3.1.1.3 MAC Generation and Cloud Storage:

MAC – Message Authentication Code is generated for the encrypted data. MAC is a small fixed size block of data that is generated based on message/file F of variable length using any secret key. Once MAC is generated, the data is stored in the cloud. Having Remote database, the Security problems arises there. So, In order to maintain data integrity, Proposed design consist of efficient methods that enable on-demand data correctness verification. Mac code is generated to ensure the data Integrity Checking It helps to ensure the data owner's data being stored in the cloud is valid or not. So finally Encrypted data and index along with the Mac code is to be outsourced to enhance the combined data security which is form of both data security and data integrity process in the cloud security system.

3.2 Data Retrieval:

When user needs to access the data, data request is sent to the cloud. Public data is provided by the cloud without authentication. User receives the encrypted data and it will be decrypted using the public key that is provided by the cloud. when the user requires accessing the data in cloud, he sends a request along with the username to cloud. If the request is for private section and limited access(LA) section, authentication is necessary and cloud looks for username provided by user into its directory of user- names, provided by the owner. If the existing user name and the private key matches, then the cloud provides data to the user.

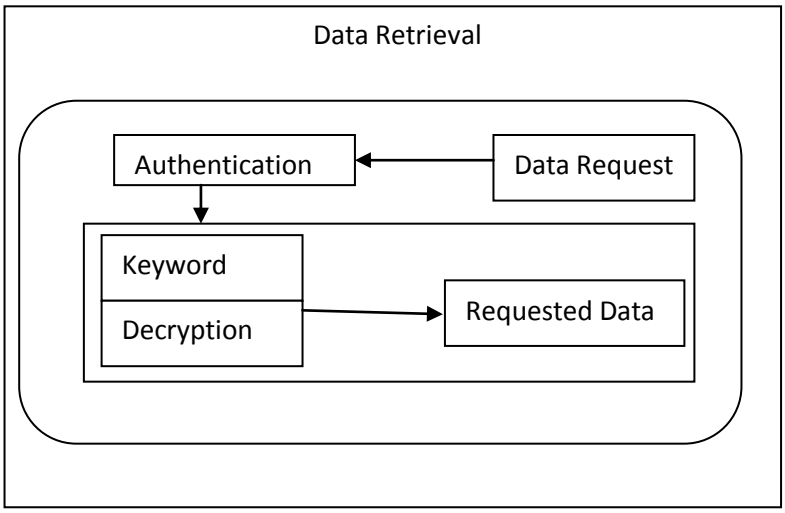

Fig 3.3 Architecture Diagram For Data Retrieval

4. Uploading Time:

The uploading and downloading time of data for each file is calculated . And the uploading time of the data is stored in the database. And the time is calculated in milli seconds. The uploading time of data for AES takes some more time, but the uploading time of blowfish takes less time compared with AES.

Comparison Graph:

5. Encrypting Time Evaluation:

The time taken by the blowfish algorithm for encryption is faster, where the fastness is one of its advantages. When it is compared with the existing technique. Blowfish shows the less time utilization for encrypting the data. The time is calculated in milli seconds.

6. Performance Metrics:

It avoids the unauthorized user, and unauthorized server, and in the tampering of data, from Brute force attack and losing of data, and in the loss of user identity and password. The above graph tells about the uploading

time of the data and the difference is also denoted. Whereas the blowfish algorithm works faster as compared to AES algorithm. The blowfish algorithm proves its features, by working faster than other algorithm. Time is calculated in milli secs, and time is the parameter compared here.

7. Conclusion:

There are various algorithms designed for the data security in cloud computing. Most of the encrypting algorithms is less secure, or fails in any of the cryptographic parameters. Advanced encryption standard algorithm overcomes this drawback. Main disadvantage of algorithm Advanced encryption standard is, mainly because of its key size of length 256 bits, it takes more time for encrypting the data. Proposed algorithm overcomes the disadvantages of advanced encryption standard algorithm. In order to overcome the drawback of Advanced encryption standard algorithm, another algorithm called Blow fish algorithm is used for the security and it is faster than previous. And the uploading and downloading time of the data is also calculated.

8. References

[1] Cloud Computing Security: From Single to Multi-Clouds,Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom*h Hawaii International Conference on System Sciences 2012.

[2] Survey Paper on Security & Privacy Issues in Cloud Storage Systems, Anup Mathew ,SURVEY PAPER, APRIL 2012.

[3] Data Security in Cloud Computing using RSA Algorithm, Parsi Kalpana ,et al, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[4] Survey paper on cloud storage security, Sunita Sharma1, Amit Chugh2

[5] Secure virtualization for cloud computing Flavio Lombardi a, RobertoDiPietro b,c Chairin Data Privacy.

[6] Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoSattacks Ashley Chonka,YangXiang n, WanleiZhou, AlessioBonti.

[7] Addressing cloud computing security issues, Dimitrios Zissis Dimitrios Lekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece, Future Generation Computer Systems 28 (2012) 583–592.

[8] Ensuring data storage security in cloud computing with effect of Kerberos, Mehdi Hojabri, International Journal of Engineering Research & Technology (IJERT) , volume 1issue 5,july ,2012.

[9] Comparison of Workflow Scheduling Algorithms in Cloud Computing, IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 10, 2011.

[10] Towards Secure and Dependable Storage Services in Cloud Computing, Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE.

[11]http://www.uotechnology.edu.iq/depcse/papers/journals/computer/fulltext/ashwaq/Design%20and%20Implementationa.pdf

[12]http://firstweb.promise.com/product/cloud/PROMISETechnologyCloudWhitePaper.pdf.

[13] http://blog.appcore.com/blog/bid/168247/3-Types-of-Cloud-Service-Models