ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 443- 446 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

A Secure Self-Destructive Active Storage Framework for Data Confidentiality

[1]Balla Rajendra, **[2]V.Sangeeta**
[1]Final M.TechStudent ,[2]Associate professor
[1,2]Dept of Computer Science and Engineering
[1,2]Pydah College of Engineering, Visakhapatnam, AP, India

Abstract:One of the most important services provided by cloud is backend support or data storage area.Obviously it leads to data confidentiality issues while we are storing data in remote locations. Self-destructing system gains most importance in recent days of technology. Entire data and its duplicates will become disturbed after end users specified time without any user interval. Any user cannot get the cipher key after expiration of timeto the sender or the receiver.

Wepropose a novelmethod in this paper referred as Safe Destruction to avoidnetwork attacks by way of decreasing,exchanging of the key size range increases the attack on the cost substantially and to achievemore results with the algorithm of Shamir secret sharing algorithm implemented in the Original Destruction system. We propose an improved approach against sniffing attacks by using the public key cryptosystem to protect from sniffing operations. In addition, we evaluate analytically the functionality of the proposed Safe destruction system.

INTRODUCTION

Cloud Computing is defined as both the applications delivered as services in the Internet and the hardware and systems software in the data centers that provide those services. The providing services themselves have very huge and it linked to Software as a Service. When a Cloud is available as a pay and use service inpublic,we referred it as Public Cloud. The service being shelled is Utility Computing [1][2] . We can use the token as Private Cloud to mention internal datacenters of a business or other organization not made available to the general public. Therefore Cloud Computing is the integration of Software as a Service and Utility Computing.

Data Owner: Data Owner or User is a person stores more amount of data on server which is maintained by the service provider or the individual who is storing data or data component to the service provider. User has a privilege to upload their data on cloud without bothering about storage and maintenance. A service provider will provide services and privileges to the user. The major goal of cloud data storage is to achieve the exactness and probity of data stored in cloud.

Third Party Auditor: Third party auditors acts as verifier, verifies on users request for storage exactness and probity of data. This Auditor Communicates with Cloud Service Provider and monitors data components which are uploaded by the data owner.

Private Clouds.People in society can be users or providers of Software as a Service or users or providers of Utility Computing. We mainly discuss on Software as a Service Providers (Cloud Users) and Cloud Providers which is receive less focus than Software as a Service[3][4].

From hardware, there are three main features are new in Cloud Computing.

1. The mirage of infinite computing resources available on request andtherebyremoving the need for Cloud Computing users to plan very long time for provisioning.
2. The avoiding of a commitment by Cloud users and allowing companies or organizations to start small and large hardware resources only when there is an increase in their requirements.
3. The capability to pay for use of computing resources on a short term periods as needed and release them as required and rewarding conservation by letting machines and storage go when they are no longer usage.

Self-destruct is a protocol or device that can be a source of an object to destroyitself,in predefined rules of circumstances. The self-destruct process is generally the complete passage to destroy the object in it. For that reason the self-destruct process can be used to destroy objects that are meant to be avoided. Self-destruct methods are found on devices and systems where mal-process could cause danger to large numbers of people[5][10].

RELATED WORK

Items are composed of data user-accessibleproperties and devicemanaged metadata.The user-accessiblefeatures explains the characteristics of the object, some of them will be opaque and others not.Consider an example a quality of service (QoS) feature may explains the latency and output requirements

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 443- 446 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

for a multimedia object. Finally the device managed metadata, managed by the storage device for the purpose of maintaining the physical storage of data.

We mention a device that stores objects as anobject-based storage device (OSD). OSDs are classified as many formsstart from a single diskdrive to an array ofdrives. These are not restricted to different accessor even writable devices; tape drives and opticalmedia also be used to store objects. Thedifference between an OSD and a block-baseddevice is the interfaceis not the physical media.The next effect of object-basedstorage is the off-loading of memory managementthat is allocation and tracking of used and freeblocks from storage applications.Block-based file systemsare divided into two sections: auser component and a storage component. Theuser component maintains presenting theuser applications with logical data structuresand those are files and directories and a media foraccessing these data structures. The storagecomponent routes the data structures to the physicalstorage [6][7].

The self-destructive system is classified into two modules. A self-destruct method is associated with every secret key part and survival time parameter for each secret key part. In this situation theSystem can achieve the need of self-destructing data with survival time control while users can use this system as a general data storage system [8][9].

1) To achieve the related key algorithm we mainly focused on Shamir Secret Share key method worked as a base algorithm for the client distributed key object repository system, for the key to be distributed equally and to provide safe from demolish.

2) Depending on active storage framework we use an object based storage interface to store and manage the equally divided key.

3) By using this functionality and security properties evaluation of this prototype the results tested that system is practical to use and it achieves all the privacy preserving features and goals.

4) The System supports security removing while the encryption happens unselectively in the physical storage devices or solid state drive respectively.

PROPOSED WORK

Web based computing leads to more importance in business community and normal end user, due to its wide variety of services. Mainly it includes Cloud Computing, Web 2.0 and Mash-ups which are based on complete service oriented architectures. It involves handling of multiple platforms to achieve effective service experiences and reduced management loads. It will make the system self-dependent and quantifiable in terms of web based computing capabilities and resources management constraints. Along with high performances and efficient computing, these web based must acquire secure data transition characteristics. For making the system secure and robust, stronger confidentiality and integrity policies must be implemented. Such policies generate temporary data which is stored and exchanged between the various entities and actors. After their usages these metadata and objects needs to be removed from the system and networks.

Thus to make the exchanges of information more secure, deleting or removing each and every view of information from the networks and systems. But in most of the cases it is not defined with the creation of the objects. Self-data removal or destruction is the configured policy of the system which enables the instances of objects to be removed from system automatically after their usage time or lifecycle is over. By implementing such solution the storage capacity is also saved along with improvements in security. Thus this paper proposes self-data destruction and handling (SDD-H) based on active storage for improving the security aspects of web based computing and service architectures. At the analytical evaluation and measurement, the approach is serving the user's needs for improved security and optimized storage. The work had also focused of specific designed synchronous operations.

Rijandael Algorithm

Key and Block Size

A key feature of Rijndael is its ability to process on different sizes of keys and data blocks. It provides moreeasily in that both the key length and the block lengthsuch as 128, 192, or 256 bits. It specifies three key sizes; that are there are at least 3.4 x 1038 possible 128-bit keys, 6.2 x 1057 possible 192-bit keys and 1.1 x 1077 possible 256-bit keys. The Sub key and the Key Schedule the sub keys are defined from the cipher key using the key schedule. The cipher key is enlarged to generate an expanded key and the sub key is generated by deriving a round key by round key. The required round key length is equal to the data block length multiplied by the number of rounds plus 1. So the round keys are taken from the expanded key.

```
Rijndael(State,Cipher_Key) {
Key_Expansion(Cipher_Key,Expanded_Key);
Add_Round_Key(State,Expanded_Key);
For( i=1 ; i Final_Round(State,Expanded_Key + Nb*Nr);
```

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 443- 446 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

}
And the round method is defined as:
Round(State,Round_Key) {
Byte_Sub(State);
Shift_Row(State);
Mix_Column(State);
Add_Round_Key(State,Round_Key);
}

The round transmission is divided into layers. These layers are the linear combination layer which provides high diffusion over various rounds. The non-linear layer which are generally applications of the Rijndael S-box. And the key addinglayers which is easily exclusive or the round key and the initial state. Every layer is designed to have its own well-defined method which increases resistance to linear and differential cryptographic method.

Shamir secret sharing
Key Generation Process

Example:

- Let us consider S=1234 (Secret key)
- Consider n=6 and k=3 and obtain any random integers a_1=166 and a_2=94
  $f(x)=1234+166x+94x^2$
- Secret share points D_0=(1,1494),D_1=(2,1942)D_3=(3,2598)D_4=(4,3402)D_5=(5,4414)D_6=(6,5614)

We give each participant a different single point (both x and f(x)). Because we use D_{x-1} instead of D_x the points start from (1, f(1)) and not (0, f(0)). This is necessary because if one would have (0, f(0)) he would also know the secret (S=f(0))

Re-construction:

- In order to reconstruct the secret any 3 points will be enough
- Let us consider

$(x_0,y_0)=(2,1924),(x_1,y_1)=(4,3402),(x_2,y_2)=(5,4414)$
Using Lagrange's polynomials
$L_0=x-x_1/x_0-x_1*x-x_2/x_0-x_2=x-4/2-4*x-5/2-5=(1/6)x^2-(3/2)x+10/3$
$L_{1=}x-x_0/x_1-x_0*x-x_2/x_1-x_2=x-2/4-2*x-5/4-5=-(1/2)x^2-(7/2)x-5$
$L_2=x-x_0/x_2-x_0*x-x_1/x_2-x_1=x-2/5-2*x-4/5-4=(1/3)x^2-2x+8/3$

$f(x)=\sum_{j=0}^{2} y_j * l_j(x)$ $=1942((1/6)x^2-(3/2)x+10/3)+3402(-(1/2)x^2-(7/2)x-)+4414((1/3)x^2-2x+8/3$)

$f(x)=1234+166x+94x^2$

now we can Recall that the secret is the free coefficient, which means that secret key is 1234.

ARCHITECTURE

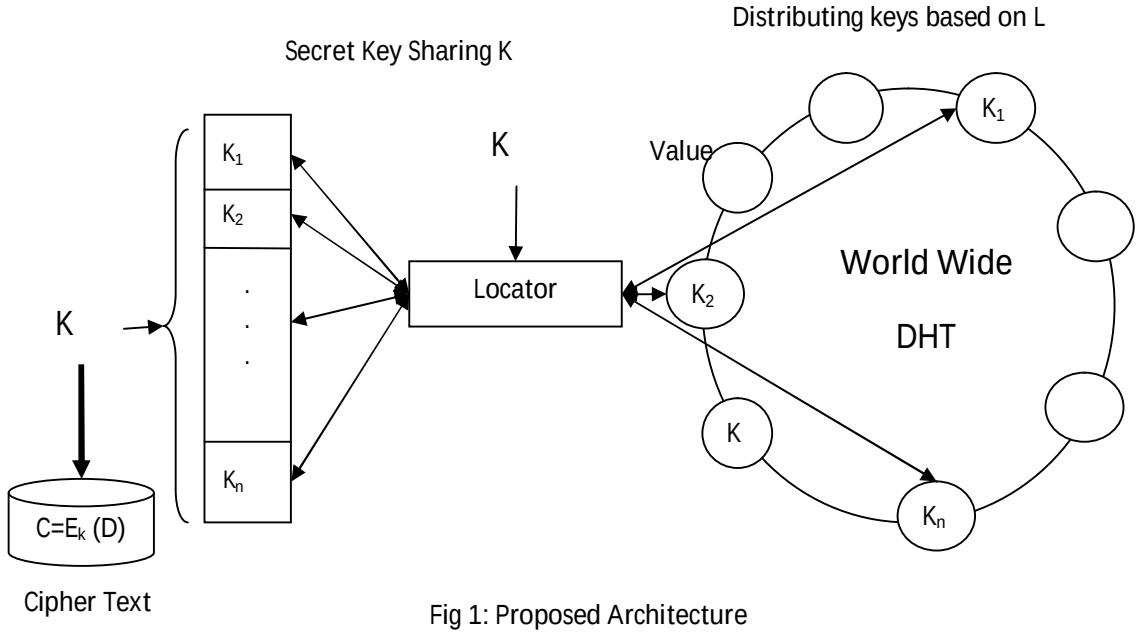

Fig 1: Proposed Architecture

Here we given stipulated time stamp in the time stamp the user can download that file without any obstacle. Every user can download data component with in the period of time stamp, otherwise download not available to the destination user. Data upload is done manually and a user can select the data they wish to share, and this

information is propagated on the network. However, since we would anticipate large numbers of users and file.A small multithreaded downloader is created to easily download the data without any delay. For both encryption and decryption mechanism key can be retrieved securely and uploads to the server securely by reconstructing the share.

CONCLUSION

We are concluding our research work with efficient data transmission technique with time stamp based self-destructive system. Shamir secret sharing mechanism makes the data secure by generating and distributing the key securely from/to server by maintain in multiple locations. Our proposed approach is self-destructive for the online users when they are not authenticated and destroys the file while time stamp expires.

REFERENCES

[1] M. Mesnier, G. R. Ganger, and E. Riedel, "Object-based storage," IEEECommunications Magazine, vol. 41, no. 8, Aug. 2003.

[2] G. A. Gibson, D. F. Nagle, K. Amiri, F. W. Chang, E. Feinberg,H. Gobioff, C. Lee, B. Ozceri, E. Riedel, and D. Rochberg, "A Case forNetwork-Attached Secure Disks," Carnegie Mellon University, Schoolof Computer Science, Pittsburgh, PA, Tech. Rep. CMU-CS-96-142, Sep.1996.

[3] G. A. Gibson and R. Van Meter, "Network attached storage architecture,"Communications of the ACM, vol. 43, no. 11, pp. 37–45, Nov. 2000.

[4] P. H. Carns, W. B. Ligon, III, R. B. Ross, and R. Thakur, "PVFS: Aparallel file system for linux clusters," in Proceedings of the AnnualLinux Showcase and Conference, Oct. 2000, pp. 317–327.

[5] P. J. Braam and R. Zahir, "Lustre - A scalable high performance filesystem," Cluster File Systems, Inc., Mountain View, CA, Tech. Rep.,July 2001.

[6] H. Tang, A. Gulbeden, J. Zhou, W. Strathearn, T. Yang, and L. Chu, "ThePanasasActiveScale storage cluster - delivering scalable high bandwidthstorage," in Proceedings of Supercomputing, Pittsburgh, PA, November2004, p. 53.

[7] Information Technology - SCSI Object Based Storage Device Commands-2 (OSD-2), ANSI, Jan. 2008.

[8] H. Boral and D. DeWitt, "Database machines: An idea whose timehas passed?" in Proceedings of International Workshop on DatabaseMachines, Sep. 1983.

[9] D. DeWitt and P. Hawthorn, "A performance evaluation of databasemachine architectures," in Proceedings of International Conference onVery Large Data Bases (VLDB), Sep. 1981.

[10] E. Riedel, "Active disks - remote execution for network-attached storage,"Ph.D. dissertation, Electrical and Computer Engineering, CarnegieMellon University, 1999, tech. Report no.CMU-CS-99-177.