ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Framework to Enhance Cryptographic Parameter for Data In Cloud

R.Sivaranjani[1], R.Radhika[2]

[1]M.E., Computer Science and Engineering, Parisutham Institute of Technology &Science,Affiliated to Anna University Chennai,Tamil Nadu-India

[2] Parisutham Institute of Technology &Science,Affiliated to Anna University Chennai,Tamil Nadu-India

Abstract--Cloud computing is a forthcoming revolution in information technology (IT) industry because of its performance, accessibility, low cost and many other luxuries. It provides gigantic storage for data and faster computing to customers over the internet. Cloud computing is a computing model in which tasks are assigned to a combination of connections, software and services accessed over a network. It essentially shifts the data base and application software to the large data centre where the management of data and services may not be completely trustworthy. A CSF (Cloud Security framework) comprising of different techniques and specialized procedures is proposed that can efficiently protect the data from the beginning to the end, i.e., from the owner to the cloud and then to the user .This strategy followed to protect the data, utilizes various techniques such as classification, Indexing of data. Encrypting the data carry forward by through 256-bit AES of SSL, Generation of MAC and XML signature. In this CSF approach, certain drawbacks in the existing system have been overcome by using cluster based index algorithm instead of sensitive rating and 256-bit AES instead of 128-bit RC4 of SSL.

Keywords--Advanced Encryption Standard, Cloud Security Framework, Message Authentication Code, Secure Socket Layer.

I . INTRODUCTON

Cloud computing is a combination of various traditional computing techniques like grid computing, distributed computing, virtualization, load balancing and so on. It combines the functionalities of traditional computing techniques and evolve as a new model on which users can rely for accessing various utility applications as a service [1].

The providers of the cloud software environments supply the developers with a programming language level environment with a set of well defined APIs to facilitate the interaction between the environments and the cloud applications, as well as to deploy and support the scalability needed of those cloud applications [4] .

Cloud provides an offsite storage system that is maintained by a cloud provider to store the user's data. Client can save the data to a cloud database instead of storing information on user computer's hard disk or other storage devices, where internet provides the connection between user computer and the cloud provider database. This network of servers and connections is collectively known as the cloud [3].

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the integrity and availability of the data files being stored on the distributed cloud servers must be guaranteed. In the distributed environment when such inconsistencies are successfully detected, finding out which server the data error lies in is also of great significance, since it can be the first step to recover the storage errors immediately. In order to achieve assurance of data storage integrity and data error localization simultaneously, the pre-computed verification tokens has been used [2].

A proof of retrievability (POR) is used for file system retrieval by client that target file say F is intact, in the sense that the client can fully recover it without any modification in content data. As PORs incur lower communication

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

complexity than transmission of F itself, it provides a block for high assurance remote storage systems. A POR is a protocol in which a server proves to a client that a target file F is not modified, in the sense that the client can retrieve all of F from the server with high probability [1].

Cloud provides the user's data security by using the firewalls, virtual private networks and by implementing the security policies with set of rules within its own periphery or perimeter. Since the concept of cloud computing requires resource polling with other cloud owners, the important data of client is not only available to particular cloud but also to third party cloud. This poses a major security threat in cloud computing that need to be addressed [6].

II . EXISTING SYSTEM

In existing model, the entire process of cloud computing deals with transmitting the encrypted data in the data centre of cloud and retrieving the data by digital signature .The encryption of data carried by the owner with various techniques such as Classification of data by sensitivity rating, Indexing by the index builder, Encryption of data by 128-bit RC4 algorithm, Message Authentication code for Integrity. The retrieval process has been achieved by keyword and digital signature.

The data in the cloud is stored in three different sections as public, private, limited access. This classification was carried calculating the sensitivity rating with values of Availability, Confidentiality, Integrity provided by owner. The data in the three different sections uses the Index Builder to generate the keyword for each file. The encryption of the data uses the 128-bit of RC4 algorithm and generation of message authentication code with small fixed size of data.

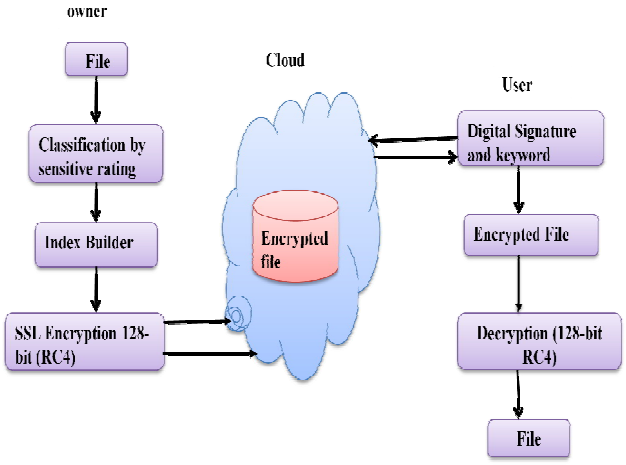

Fig. No:1 Process in existing system

In this model, the Index Builder can generate the unique value for data classified by the sensitivity rating. The generation of the key for the RC4 algorithm uses the Swapping function of the Initialization vector and temporary vector. The encryption of the data has been done by XOR the value of Key with next plaintext. The decryption process carried by XOR the key value with the next byte of the plaintext and cipher text. If the key is transparent, the data can be easily decrypted [5].

III . PROBLEM STATEMENT

The cloud environment has number of data centre to store the data. The entities can access the resources after the verification. Since it provides enormous storage space the level of security policies should be high. Security is a major issue in any cloud computing infrastructure. It is essential to provide secure service (i.e. authorized access to resources)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

in cloud computing. External attacker can enter into the critical section without knowledge of the owner. Cloud Service Provider himself can breach the owner access rights, as data is kept in their location. Any kind of security and privacy violation is critical and can produce dire consequences. The Cloud Service Provider (CSP) stores the data in encrypted form at cloud. The encrypted data can be transformed into original data by the corresponding key and algorithm. The encrypted data will be stored anywhere and it can be accessed from any place. The owner is not aware of the data location where it is stored .

3.1 GOAL OF THE PROJECT

In this computing model, owner sends the encrypted data to cloud where it is stored and then the data can be retrieved from the cloud by user upon request. The Cloud Security Framework provides the end to end security from the owner to the user. The keyword to retrieve the data from the cloud and key to be used for the decryption are sent to the E-mail of the corresponding entities. The owner can identify the location of data where they stored. This is achievable only after when they provides the authentication details to cloud Administrator.

IV . PROPOSED SYSTEM

4.1 PROPOSED FRAMEWORK

The proposed Cloud Security Framework (CSF) has been structured to provide complete security to the data throughout the process of cloud computing. In system, multiple mechanisms and available techniques are applied to shield the critical information from unauthorized parties. The proposed Cloud Security Framework (CSF) is divided into two phases. First phase deals with process of transmitting and storing data securely into the cloud. Second phase deals with the retrieval of data from cloud and shows the generation of requests for data access, double authentication, verification of digital signature and integrity, thereby providing authorized user with data on satisfying all security mechanisms.

In cloud the data are stored in the large data center with Classification based on Sensitivity Rating (SR).The Sensitivity Rating uses the value of the confidentiality, Integrity, Availability provided by the owner. It classifies the data into three sections as public, private, Limited Access. The cluster Index Building generates the unique index value for the data stored in the cloud. The Secure Socket Layer (SSL) encryption uses the 256-bit encryption of AES. The 256-bit AES algorithm processed by fourteen steps and four transformation as Substitute Bytes, Shift Rows, Mix columns and Add Round key.

Message Authentication Code (MAC) and XML Signature are generated for the encrypted data to check the integrity in cloud. Socket Layer (SSL) Encryption provides the key to decode the data for the authenticated user. The Retrieval of data from the cloud is achieved by authentication of the user in the cloud and accessed by the levels of the storing data. The Double Acknowledgement Scheme will send the details of the data retrieval to the owner and the user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

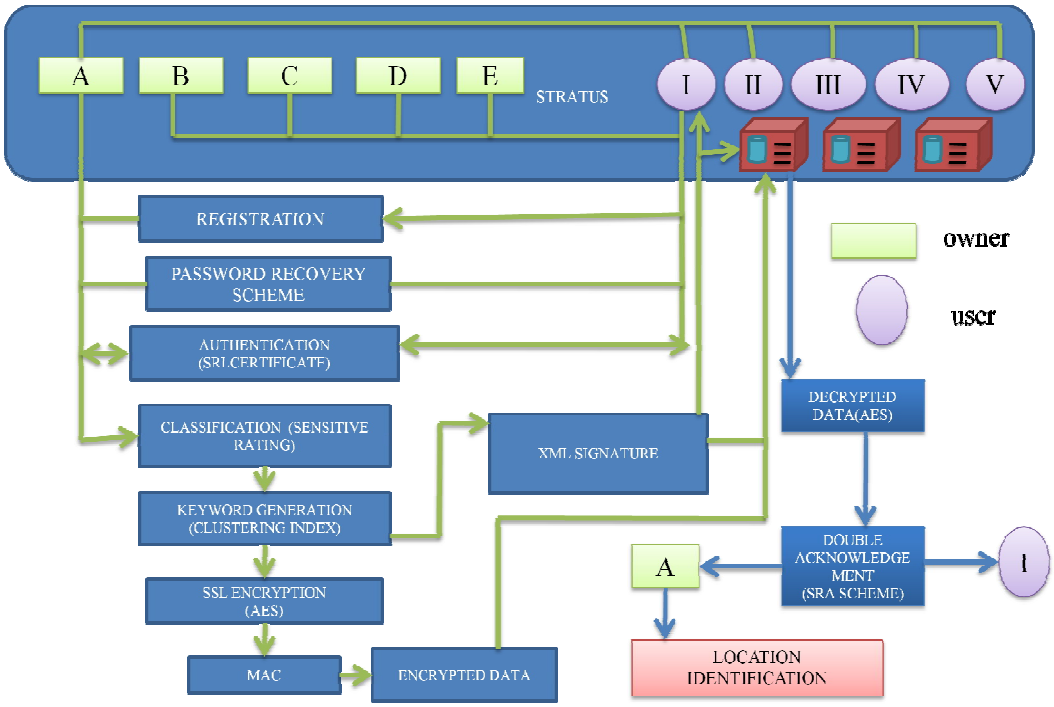

Fig. No: 2 System Architecture

The stratus Admin can control the cloud environment with multiple owner and user. The SRL(Sender Receiver Login) includes the registration, password recover scheme with the admin.

4.2 ALGORITHM AND TECHNIQUES

4.2.1 Classification of data

The classification of the data provides the level of access of the data storage. It will be stored in public, private and limited access. The sensitive rating will be calculated by the value of availability, confidentiality and integrity. The value for this parameter is assigned by the owner [9].

SR[i]=(C[i]+(1/A[i]*10+I[i]))/4

C[i]= Confidentiality, A[i]= Availability, I[i]= Integrity

4.2.2 SSL Encryption (256-bit AES)

Secure Socket Layer Encryption provides the security of the data while transferring from owner to user. The certificate Authority is responsible for the exchange of the key between the owner and the user. The protocol layers consist of secure socket layer which may be placed between a reliable connection oriented network layer protocol and the application protocol layer. SSL provides secure communication between the client and server by allowing mutual authentication, the use of digital signature for integrity and encryption for privacy.

Advanced Encryption Standard

The AES cipher uses the block length and the key length that are independently specified to be 128, 192, 0r 256 bits. It uses the same three size alternatives but limits the length to 128-bits.It has the following characteristics:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- Resistance against all known attacks
- Speed and code compactness on different type of platforms
- Design simplicity

The input to the encryption and decryption algorithm is a single 128-bit block. The block is copied into the state array and it is modified at each stage of encryption or decryption. It processes the entire data block in parallel during each round using substitutions and permutation.

The key that is provided as input is expanded into an array of forty four 32-bit words, W[i].

Four different stages are used, one of permutation and three of substitution:

- Substitute bytes: Uses an S-box to perform byte-byte substitution of the block
- ShiftRows**:** A simple permutation.
- Mixcolumns: A substitution that makes use of arithmetic over GF(2^8).
- AddRoundKey: A bitwise XOR of the current block with a portion of the expanded key.

4.2.3 Message Authentication code

Message authentication is also called data origin authentication. Message authentication is said to protect the integrity of a message, ensuring that each message that it is received and deemed acceptable is arriving in the same condition that it was sent out, without interleaving, missing, or modified [10].

MAC=C(K,M)

C- Fixed Length Authenticator

M- Variable Length Message

K- Secret Key

The MAC with the sender and receiver will be compared with each code to ensure the integrity of the message. These details can be shared through the E-mail of the entities.

4.2.4 XML Signature

XML Signatures are digital signatures used in XML transactions. An XML Signature may be applied to the content of one or more resources. It may be used to sign only a portion of an XML document.

XML Signature Creation:

In this, the <KeyInfo> element is added. It is used to Identify the resources to be signed. The public key information is takes place in the Key Information.

XML Signature Verification:

The <SignedInfo> element is calculated by using <Signature Value>. This value is compared with the digest value.

4.2.5 Location Identification

The location of the data which is stored by the corresponding owner can be tracked by them. The MAC address of the Storage system can be retrieved.

V EVALUATION

5.1Encryption Throughput

The encryption for the data packets can be performed with different size. The AES algorithm provide high throughput for the small size data compare to RC4 algorithm. The longer key size of AES algorithm provides stronger security than the RC4 algorithm.

5.2 CPU Work Load

The AES algorithm reduce the workload of the CPU . It tends to consume much less time for the process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI .CONCLUSION

The proposed framework provides the security to the data from the owner to the cloud and the cloud to the user. The Secure Socket Layer provides the security by exchanging the certificate between owner and the user. The classification and indexing by sensitive rating of the data increase the efficiency of the retrieval process .The integrity of the data is achieved by the generation of the XML signature and the Message Authentication Code (MAC). The AES algorithm uses the mathematical function for the encryption and decryption process. The Algorithm can be raised to 512-bit to compute more data. Proposed method achieves the integrity, availability, reliability of the data in the cloud. It provides more flexibility and capability to meet the requirements over cloud environment and enable the user to retrieve files form cloud by searching over an encrypted data. The storage location of the data is known to the owner.

REFERENCES

[1] Bowers KD, Jules A, Opera A,"Proofs of retrievablity: theory and implementation," Cryptology e-print Archive, Report 2008/175; 2008a.
[2] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou,"Ensuring Data Storage Security in Cloud Computing,"US National Science Foundation 2009.
[3] Manoj Prabhakar Darsi , K.Suresh Joseph, Dr. S.K.V.Jayakumar," A New Approach for Providing the Data Security and Secure Data Transfer in Cloud Computing," International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013.
[4] Priyanka Arora, Arun Singyagi," Evaluation and Comparison of Security Issues on Cloud Computing Environment,"World of computer science and Information Technology journal,2012.
[5] Sandeep K.Sood.."A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications,2012
[6] Sudha .M, Dr.Bandaru Rama Krishna Rao, M. Monica," A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment," International Journal of Computer Applications, 2010.