Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.295 – 301

SURVEY ARTICLE

A Survey on Secure Cloud Computing using AES Algorithm

Roshani Raghatate[1], Sneha Humne[2], Roshna Wadhwe[3]

Department of Computer Engineering   Sevagram, RTMNU, India

roshaniraghatate27@gmail.com

snehaprashantramteke@gmail.com

nivwadhave91@gmail.com

Abstract: with the tremendous growth of sensitive information on cloud, cloud security is getting more important than even before. The cloud data and services reside in massively scalable data centers and can be accessed everywhere. The growth of the cloud users has unfortunately been accompanied with a growth in malicious activity in the cloud. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services. The future of cloud, especially in expanding the range of applications, involves a much deeper degree of privacy, and authentication. We propose a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security.

Keywords: Cloud Computing, Cloud Security, Cryptography, AES, Cloud Data

I. INTRODUCTION

Cloud computing is emerging as a key computing platform for sharing resources that include infrastructure, software, applications, and business processes. It is a technology that uses the internet and central remote servers to maintain data and applications. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing have aimed to allow access to large amounts of computing power in a fully virtualized manner, by aggregating resources and give a picture of a single system. A computing cloud has networks of nodes. Therefore scalability should be a quality feature of the computing cloud. In addition, an important aim of these technologies has been delivering computing as a utility.

Cloud computing can be seen as the requirement of three users which are categorized in three modules: -

End user : - just wants to use the application softwares such as Ms Office, Paint Brush, and Image Processing Software etc. This sort of service is provided by Software as a Service model of cloud computing which gives freedom to the user from getting license of software.

Commercial organization : - who wants to spread his business with the help of website then he/she has to set up the servers and maintenance of servers which leads to the high cost. But the cost of infrastructure can be removed by having Infrastructure as a Service model of cloud computing because the storage and security of data maintenance of servers etc is handled by the cloud service provider. Developer: - It also takes care of the needs of developer by providing the platform on which developer wants to work such as Operating System etc. This is also provided by the Platform as a Service model.

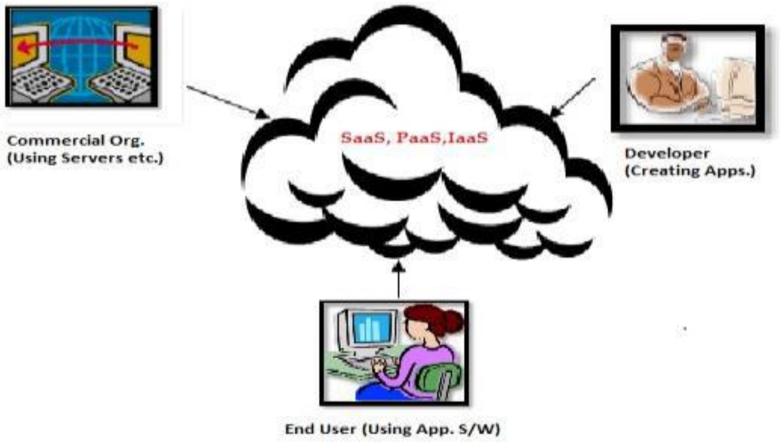


Fig : cloud computing

II. RELATED WORK

V. Sathana and J.Shanthini Proposed a system to achieve secure data sharing for dynamic groups in the cloud, they expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. Unfortunately, each user had to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users.

B. Bhavani Bai Proposed Cloud architecture is enhanced security model for data storage within cloud environment. It consists of various users with local availability of mail server and cryptographic application. A cryptographic application installed on client side will connect user with samba storage and allows for encryption and decryption operation on data. As the cryptographic application is installed on client's machine it will increase speed-up ratio and mean processing [5] for encryption and decryption process. The authentication server used for authenticating users to enter into server environment and use available functionalities. The various steps followed are explained in terms of communication among Client machine provided with cryptographic module and samba server storage.

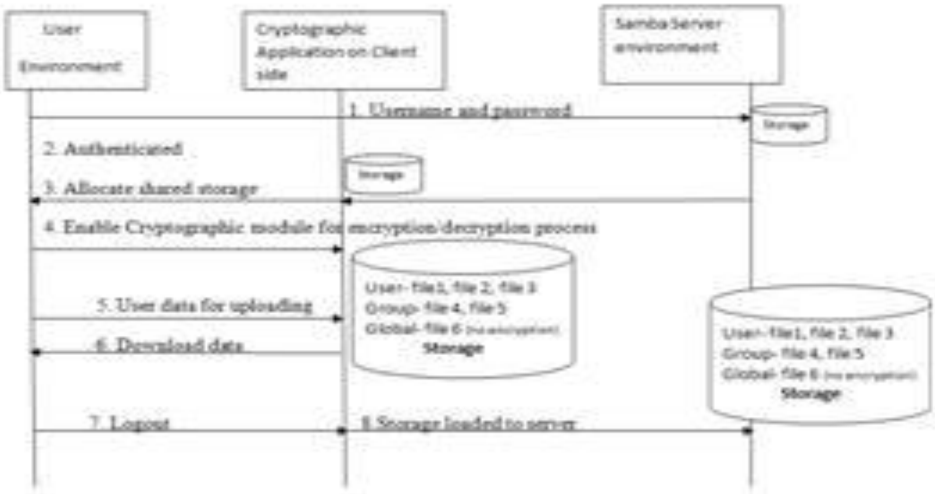

User Environment
Cryptographic Application on Client side
Samba Server environment
1. Username and password
Storage
2. Authenticated
Storage
3. Allocate shared storage
4. Enable Cryptographic module for encryption/decryption process
User- file1, file 2, file 3
Group- file 4, file 5
Global- file 6 (no encryption)
Storage
5. User data for uploading
6. Download data
User- file1, file 2, file 3
Group- file 4, file 5
Global- file 6 (no encryption)
Storage
7. Logout
8 Storage loaded to server

Fig . Sequence diagram or describing interaction among samba server and use

Anurag singh Tomar proposed in this paper, group key agreement with node authentication has been proposed. Any group member wants to contribute in group key agreement, firstly, the member will multicast the certificate parameters to his group so that any group member can authenticate any that group members. After successful authentication, member computes the contribution of the sender with these certificate parameters to compute the group key.

Anu Kumari and Krishna Bansal proposed in this section they was present the approach which can used to set up resource location more accurately and then restricting them on the basis of locality. For this they were using Phoenix coordinate system with host authentication. For this approach there is a need of creating landmarks which help in calculating coordinates more accurately. For this purpose they used available locations like universities or schools to act as landmarks to increase their accuracy.

K.Sripriasadh ,Saicharansrinivasn,O.Pandithurai proposed that the data must be secure when it travels between your site and the cloud and must be protected in the cloud, step in the process is making sure that the data is also protected during transactions, such as if an employee or customer is able to access data in an application transaction processing

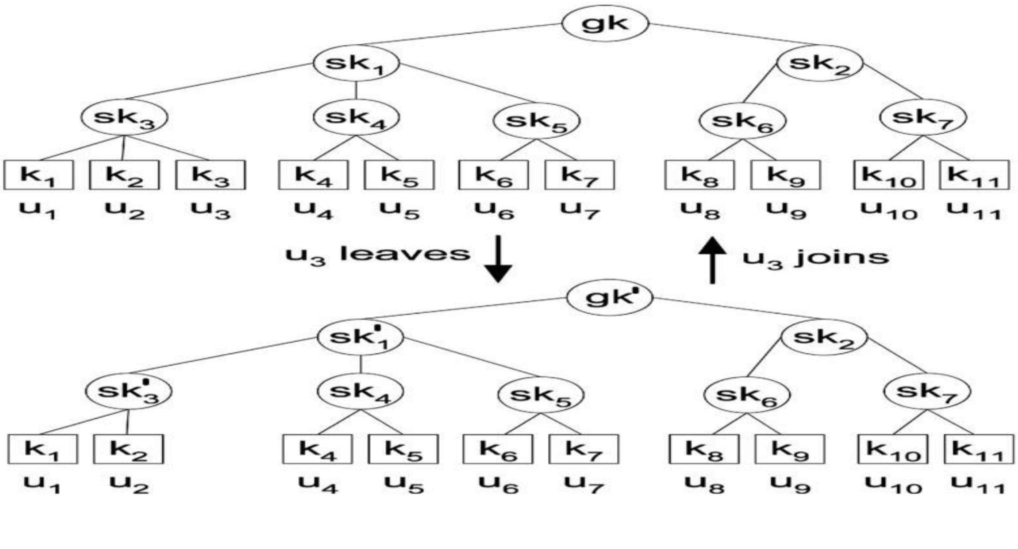

gk
sk1
sk2
sk3
sk4
sk5
sk6
sk7
k1 k2 k3 k4 k5 k6 k7 k8 k9 k10 k11
u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11
u3 leaves
u3 joins
gk'
sk'1
sk2
sk'3
sk4
sk5
sk6
sk7
k1 k2 k4 k5 k6 k7 k8 k9 k10 k11
u1 u2 u4 u5 u6 u7 u8 u9 u10 u11

Fig. Group Multicasting

Navia Jose,Clara Kamani A proposed cloud security data model is based on a three-layer system structure, in which each layer performs its own duty to ensure the data security of cloud layers. The first layer is responsible for cloud user authentication. It is designed as OTP authentication module and uses digital certificates issued by the appropriate users and also manage user permissions. The second layer manages the user's data encryption by using AES algorithm, which is the most secured and faster encryption algorithm. For sensitive data such as one's personal information (ex. credit card number) should be encrypted and sent to the cloud .Data integrity is provided by using algorithms like MD5 and RSA. For non-sensitive data such as one's local information (ex. address details), it should protected by using digital signatures and sent to the cloud. It also protects the privacy of users based on fine- grained attribute based access control policies through access control policy algorithms.Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems. Such mechanisms should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls. The third layer supports the faster user data recovery by using Byzantine fault tolerance algorithm methods.

D.Mounica and Mrs Ch. Radhika Rani proposed the cloud customers may form their expectations based on their past experiences and organizations‟ needs. They are likely to conduct some sort of survey before choosing a cloud service provider. Customers are expected also to do security checks that are centered on three security concepts: confidentiality, integrity and availability.Security in cloud services is based on the following: Strong network security is possible around the service delivery platformData encryption: for data in transit (particularly over wide area networks), and sometimes stored data, but it cannot be applied to data in use. Access controls to ensure that only authorized users gain access to applications, data and the processing environment and is the primary means of securing cloud-based services. Service providers are able to inspect activity in their environment and provide reports to clients.

Ya-Qin Zang proposed that Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. Integrated cloud computing is a whole dynamic computing system. It provides a mandatory application program environment . It can deploy, allocate or reallocate computing resource dynamically and monitor the usage of resources at all times. Generally speaking cloud computing has a distributed foundation establishment, and monitor the distributed system, to achieve the purpose of efficient use of the system. Cloud computing collects all the computing resources and manages them automatically through software. In the process of data analysis, it integrates the history data and present data to make the collected information more accurate and provide more intelligent service for users and enterprises. The users need not care how to buy servers, software, solutions and so on. Users can buy the computing resource through internet according to their own needs.

III. PROPOSED WORK

Cloud computing is likely to suffer from a number of known vulnerabilities, enabling attackers to either obtain computing services for free or steal information from cloud users. In the world of computing, security and privacy issues are a major concern and cloud computing is no exception to these issues. A study ascertains that securing outsourced data and computation against mistrusted clouds is indeed costlier than the associated savings, with outsourcing mechanisms up to several orders of magnitudes costlier than their non-outsourced locally run alternatives [11]. From the view of a broad class of potential users, using cloud is much like trusting the telephone company–or Gmail, or even the post office–to keep communications private. People frequently place confidential information into the hands of common carriers and other commercial enterprises. There is another class of users who would not use the telephone without taking security precautions beyond trusting the common carrier. For procuring storage from the cloud, same thing applies-neversend anything but encrypted data to cloud storage [12]. Affirming this notion we provide a mechanism for achieving maximum security by leveraging the capabilities of cryptography. We provide architecture and guidelines to increase the security as well as the privacy of the data owner by transferring the process of encryption and decryption from the cloud to self. For maximizing the security of data, user segments and encrypts the data using a secured co-processor.

It may be argued that such encryption on user's end raises issues as user controlled keys may be inconsistent with portions of CSP's business model. Also this architecture can limit a cloud provider's ability to data mine or otherwise exploit the users' data [13]. So, to fully exploit potential of cloud computing there should be limited restrictions on processing and computation. This is possible when CSP can enable search on encrypted data. A model for this exists where CSP's can partially access the data without having to decrypt it.

Implementing AES algorithm

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128 bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical.
16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4- words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule.
For encryption, each round consists of the following four steps:

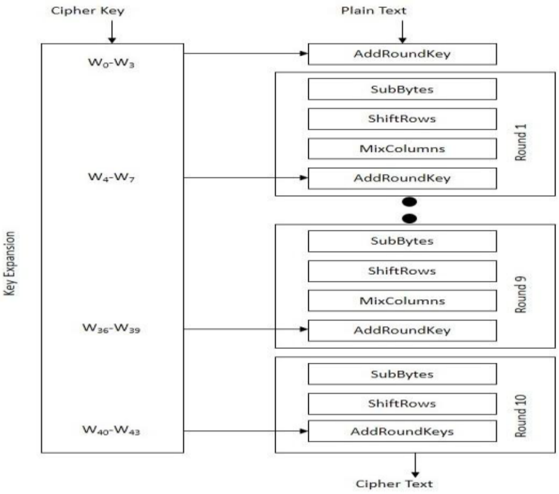


Fig. AES Encryption

SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (box).

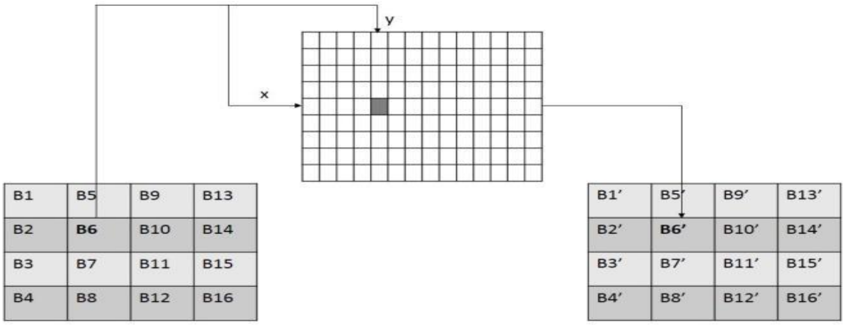
ShiftRows – a transposition step where each row of the state is shifted cyclically a certain number of times

MixColumns – a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher

1. SubBytes-

The purpose of this step is to give ample resistance from differential and linear cryptanalysis attacks. This is byte-by-byte substitution where each byte is substituted independently using Substitution table (S-box). Each input byte is divided into 24-bit patterns, representing an integer value between 0 and 15 which can then be interpreted as hexadecimal values. Left digit defines the row index and right digit defines the column index of S-box. At the intersection of row and column, value given is substituted. There are sixteen distinct byte-by-byte substitutions. S-box is constructed by a combination of GF (28) arithmetic and bit mangling.



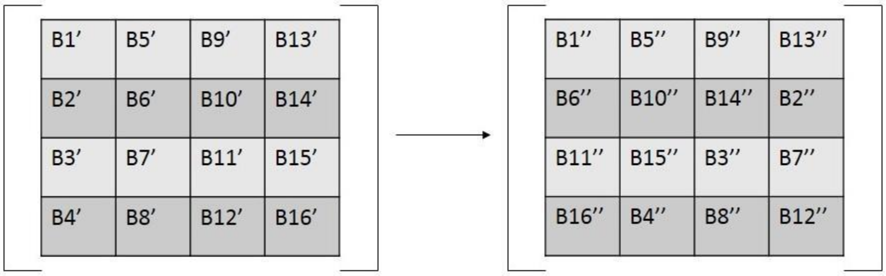
B1	B5	B9	B13
B2	**B6**	B10	B14
B3	B7	B11	B15
B4	B8	B12	B16

B1′	B5′	B9′	B13′
B2′	**B6′**	B10′	B14′
B3′	B7′	B11′	B15′
B4′	B8′	B12′	B16′

Fig. Sub Bytes Step

2. ShiftRows

The purpose of this step is to provide diffusion of the bits over multiple rounds. The row 0 in the matrix is not shifted, row 1 is circular left shifted by one byte, row 2 is circular left shifted by two bytes, and row 3 is circular left shifted by three bytes



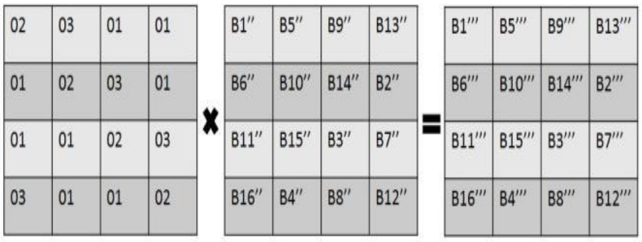
B1′	B5′	B9′	B13′
B2′	B6′	B10′	B14′
B3′	B7′	B11′	B15′
B4′	B8′	B12′	B16′

B1″	B5″	B9″	B13″
B6″	B10″	B14″	B2″
B11″	B15″	B3″	B7″
B16″	B4″	B8″	B12″

Fig. shift row transformation step

3. MixColumns

Like previous step, the purpose of this step is to provide diffusion of the bits over multiple rounds. This is achieved by performing multiplication one column at a time. Each value in the column is multiplied against every row value of a standard matrix. The results of these multiplication are XO Red together. For e.g. value of first byte B1'' is multiplied with 02, 03, 01 and 01 and XO Red to produce new B1''' of resulting matrix. The multiplication continues against one matrix row at a time against each value of a state column.



02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

B1″	B5″	B9″	B13″
B6″	B10″	B14″	B2″
B11″	B15″	B3″	B7″
B16″	B4″	B8″	B12″

B1‴	B5‴	B9‴	B13‴
B6‴	B10‴	B14‴	B2‴
B11‴	B15‴	B3‴	B7‴
B16‴	B4‴	B8‴	B12‴

Fig. Mix Columns Step

4. AddRoundKey-

In this step, the matrix is XO Red with the round key. The original key consists of 128 bits/16 bytes which are represented as a 4x4 matrix. This 4 words key where each word is of 4 bytes, is converted to a 43 words key. The first four words represent W[0], W[1], W[2], and W[3]

IV. CONCLUSION

Implementing AES for security over data provides benefits of less memory consumption and less computation time as compared to other algorithms. Though each cloud infrastructure has its own security strengths; the user can choose infrastructure according to his security. Each of the cloud providers has their own set of rules, pricing, flexibility, support and other important parameters. The key consideration dealt in this proposal is the encryption schema to secure data by making it unintelligible for all.

REFERENCES

[1] V. Sathana and J. Shanthini,"Automated Security Providence For Dynamic Group In Clode"In International Journal Of Innovative Research In CE",Vol.2,Special Issue 3,July 2014.

[2] B Bhavani Bai,"Ensuring Security At Data Level In Cloud Using Multi Cloud Architecture",In International Journal Of Science And Technology,(ISSN 2321-919X) June 2014.

[3] Anurag Singth Tomar,Gaurav Kumar Tak"Secure Group Key Agreement with Node Authentication"In International Journal Of Advancee Research In Computer Engineering and Technology(IJARCET),Vol.3,Issue 4,April 2014.

[4] Anu Kumari , Krishna Bansal"Secure resource location with the help of phonic coordinate system and host authentication in cloud environment", Vol. 3(2).

[5] K.Sriprasadh,Saicharansrinivasan,and O. Pandithurai" A Novel Method To Secure Cloud Computing Through Multicast Key Management", In International Conference Of Information Communication,2013.

[6] Rabi Prasad Padhy,Manas Rajan Patra and Suresh Chandra Satapathy"Cloud Computing Security Issues And Research Challenges",International Journal Of Computer Seience and IT ,Vol. 1,No.2,2011.

[7] Navai Jose,Chara Knmani A"Data Security Model Enhancement In Cloud Environment", In Journal Of Computer Science And Engineering"(IOSR-JCE),Vol.10,Issue 2,2013.

[8] Gansen Zhao, Chunming Rongy, Jin Liz, Feng Zhangx and Yong Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers," 2nd IEEE International Conference on Cloud Computing Technology and Science.

[9] (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high ground - cloud computing," The Big Switch:Rewining the World,from Edison to Google, , ITIC Publishing House, October 2008 1-1

[10] Ya-Qin Zhang, of computing in the "cloud - Client", The Economic Observer reported, the future http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri 14:30