iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security Augmentation of Cloud

Geeta Deshwal[1], Vinod Saroha[2], Dr. Sanjeev Rana[3]
[1]PG student (BPSMV), [2]Assistant Professor (BPSMV) ,[3]Professor (MMU MULLANA)

Abstract: Cloud gives us many reasons for use. It is an integration of computation devices which includes hardware, software, integrated services which may used by more than one use in more reliable and effective way of computing data and access of data. Basically a third party which owns the infrastructure of cloud provides these data storage facilities. It carrying many advantages some of are: reliability, scalability, flexibility and efficiency, outsourcing non-core activities. With these a lots of services and advantages cloud offers an innovative business model. In this paper we have discuses about security issues related with cloud when we are using aloud services to store our meaningful information. What kind of security issues we may face we try to describe many security threats and solutions. This paper introduces a detailed security issues and their solutions with AES.

I. INTRODUCTION

Internet has been represented like cloud on network diagrams. Now variety of latest services started to emerge. We are using cloud computing all day long without realizing it, when we use Google and type a query Google is actually not playing much more than a messenger.

Cloud computing is recent development of internet. It is the latest technology in the world of information technology that shares various resources with the help of internet across the world. Major advantage of cloud computing is it can share resources without using any other storage medium of special purpose software. So that customer does not need to pay money on extra resources. And cloud is also not required any other installation process like customer's location, end to end users information etc. cloud computing is considered into fifth generation after main frame computer, personal computer, client server. We can also called cloud computing Adhoc service it means we can use a cloud when we need it.

A webmail is simple example of cloud computing in which you can share information dynamically. We can access cloud computing service at any place by using any kind of device like mobile phones, laptops, computers etc. today's very common example of usage of cloud computing is we can easily store and manage various Apps at one place i.e. cloud. Our data will be secure even if we lost our mobile.

Most of the well developed companies have promoted their own cloud computing platforms an8d infrastructures for their users and deploy their web application on this platform.

To get enter into this amazing virtual environment users/industries have transfer data on the cloud first. To make cloud more flexible extensible and reusable technology used by cloud computing is service oriented architecture. In this paper we have discuses about security issues related with cloud when we are using aloud services to store our meaningful information.

What kind of security issues we may face we try to describe many security threats and solutions. in every new technology to make that more reliable and easy to use their developer set some set of rules and restrictions similarly in cloud computing a set of rules which is called protocols and special purpose software named as middleware are also located at the central server administrator system.

II. BASIC OF CLOUD COMPUTING

Cloud computing is promising technology which is specially concentrate to provide these special services like dynamic storage, sharing of information, storage of huge amount of data without any special requirement at user end. According to a forester he define cloud computing as "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customers application and billed by consumption." The main advantage of cloud

Computing provide different way to access and manage the cloud resources etc. it is an internet based service so users can be access the resource through any kind of virtual machine like mobile, laptops, computer etc.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

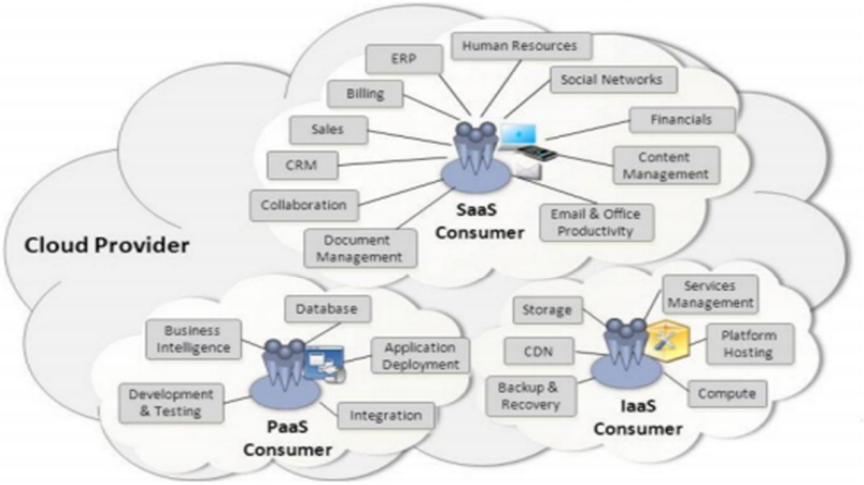


Fig1: services provide by cloud

A. Characteristics of cloud computing

1) *Elasticity*: cloud computing is allows to end users to enhance their resource at any time any place as well as they can scale their resources.

2) *Virtualization:* one of the main advantage of cloud computing is virtualization it means we can access cloud services at any place through any platforms.

3) *Reliability*: cloud computing provides end to end reliability.

4) *Sharing of resources*: cloud computing provides various features in which sharing of resources is important.

III. CURRENT SECURITY ISSUES IN CLOUD

Throughout the internet cyber crime effects are felt and cloud computing is the main target for hackers because cloud contain huge amount of information and Apps. In cloud security is necessary at all levels for example security requirements in cloud at user level where user run application software and many of interactive services of cloud. Another level of security required at application level where highly programmed software run. And at the most important on database of the cloud where highly confidential user's data stored. On the basis of this knowledge we may classify the security requirement in cloud they are describing in this paper.

A. User level
B. Application level
C. Database level
D. Cloud networking
E. Transmission of files over cloud

As we all know cloud provide a lot of services more like multiple user may access the cloud security at the same time. Where more than one user interacts with cloud at the same instants of the time level of security must be high so that no user command may interrupts another one. Or it should be convenient to all users with minimum waiting time. A term may arise when we talk about multiple users' task at the same time.

F. Load balancing in cloud.
G. Energy efficiency.
H. Resource utilization.
I. User's demand.
J. Prevent deadlock condition.

Above points are also important enough to handle because cloud provide multiplexing of users so that is must be balance the load of user's commands at the same time. With this proper utilization of resource and energy is also important. User's demand may change time to time so that cloud must enhance their services on the basis of user's requirements.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. PROPOSED WORK

cloud computing is likely suffer from a number of different vulnerable things, enabling hackers to use cloud computing services without any charge or they may steal user's information without authentication. One of the major concerns of this computerized world is security, every user want proper privacy and secrecy of their information over public computing medium like cloud which gives us facility to store information like centralized. In this paper i tried to explain how to save our important data over cloud by using encryption technique i.e. AES. 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 [3]. 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-never send anything but encrypted data to cloud storage [4]. 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 [5].

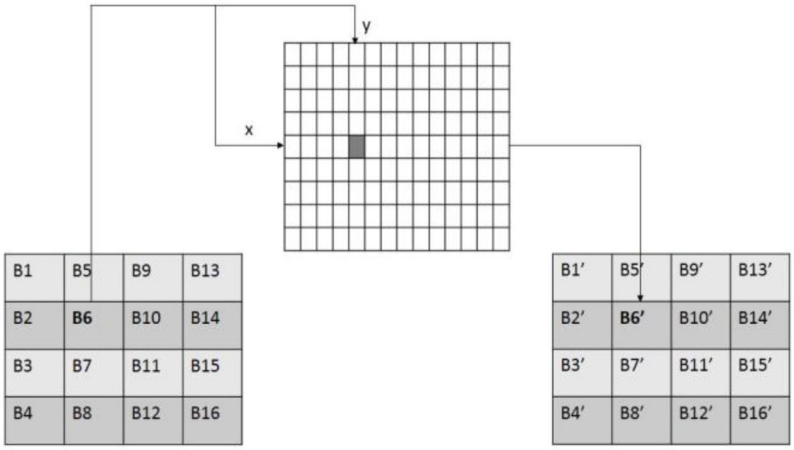
V. AES IMPLEMENTATION

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.

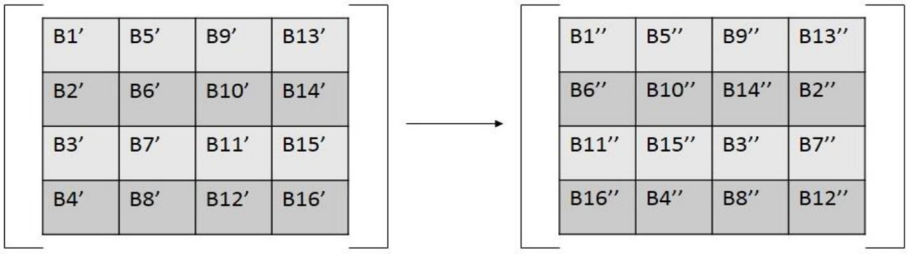
16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule.

For encryption, each round consists of the following four steps:

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



B. Shift Rows: A transposition step where each row of the state is shifted cyclically a certain number of times



Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Mix Columns: A mixing operation which operates on the columns of the state, combining the four bytes in each 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'''

D. AddRoundKey: Each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

E. Advantage of AES

1) AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's.
2) Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
3) This algorithm has speedy key setup time and good key agility.
4) It requires less memory for implementation, making it suitable for restricted-space environments.
5) The structure has good potential for benefiting from instruction-level parallelism.
6) There are no serious weak keys in AES.
7) It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
8) Statistical analysis of the cipher text has not been possible even after using huge number of test cases.
9) No differential and linear cryptanalysis attacks have been yet proved on AES.

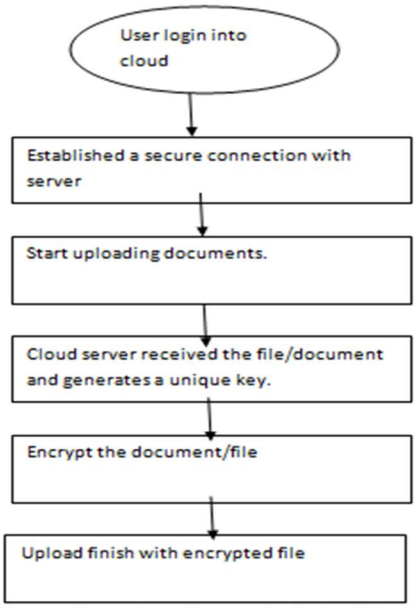


Fig2. Process of encrypting a file over cloud using AES

F. Steps to generate AddRound key

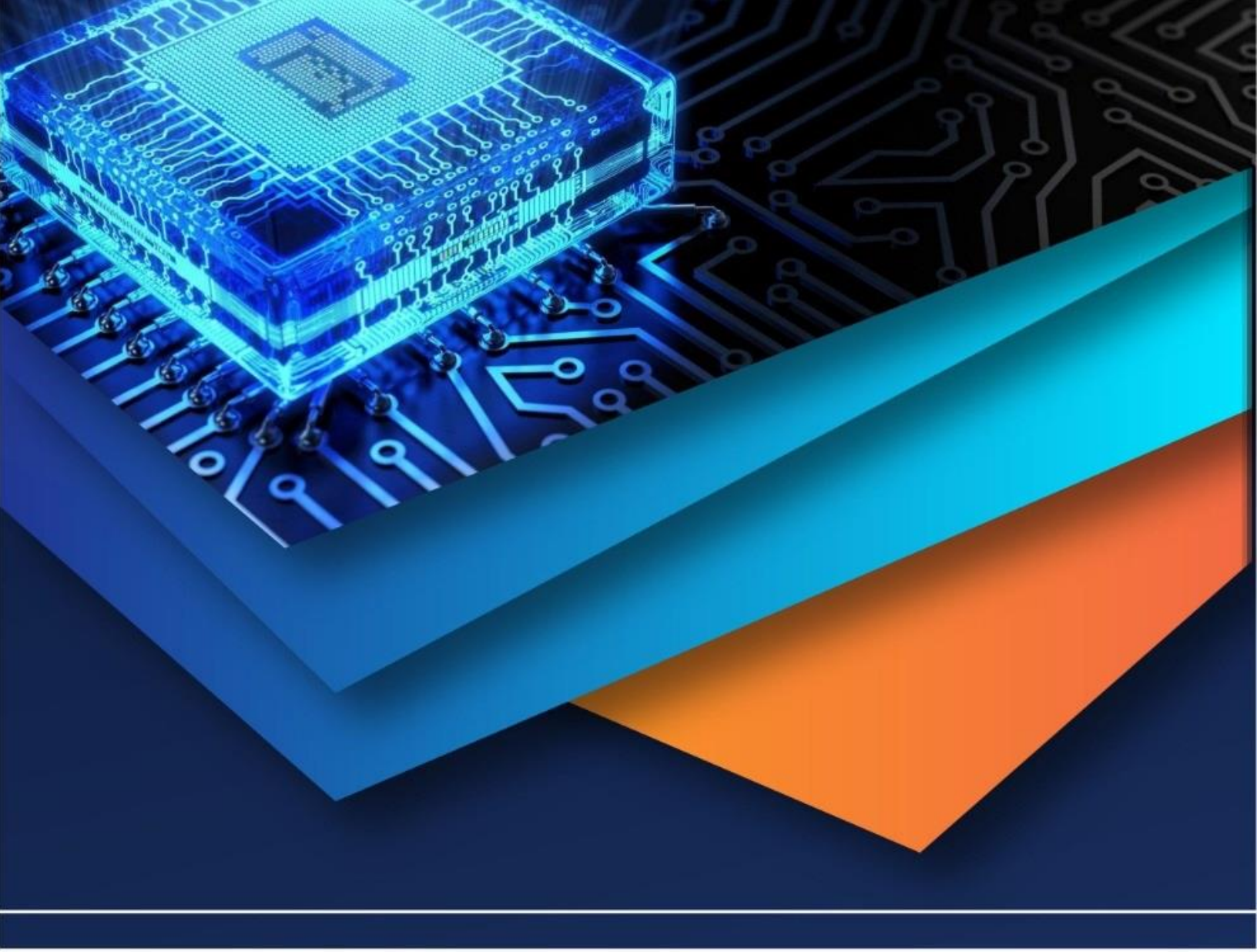
```
for (i=4; i<44; i++)
{
T = W[i-1];
if (i mod 4 = = 0)
T = Substitute (Rotate (T)) XOR RConstant [i/4];
W[i] = W[i-4] XOR T;
}
```

VI. CONCLUSION

The investigation on confidentiality preservation and data classification, started with a literature review. The literature view has been conducted in order to search all relevant information of top quality. According to these encryption techniques we may assure that an AES technique is quite good to use in order to secure our important file over cloud. 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 key consideration dealt in this proposal is the encryption schema to secure data by making it unintelligible for all. 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;

REFERNCES

[1] Ellen Messmer (2012). Gartner: Growth in Cloud Computing to shape 2013 security trends, Network World [Online] Available: http://www.networkworld.com/news/2012/120612- gartner-cloud-security-264873.html
[2] Sachdev Abha Thakral, and Mohit Bhansali. "Addressing the Cloud Computing Security Menace." IJRET, Volume 2, Issue 2, pp. 126-130, Feb 2013.
[3] Chen, Yao, and Radu Sion. "On securing untrusted clouds with cryptography. “Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. ACM, 2010. [4] Talbot, David (2009). “How Secure Is Cloud Computing?” Technology Review [Online]. Available: http://www.technologyreview.com/computing/23951/
[4] Agudo, Isaac and Nuez, David and Giammatteo, Gabriele and Rizomiliotis, Panagiotis and Lambrinoudakis, Costas. Cryptography Goes to the Cloud. In Lee, Changhoon and Seigneur, Jean-Marc and Park, James J. and Wagner, Roland R., editors, Secure and Trust Computing, Data Management, and Applications, pages 190–197, Springer Berlin Heidelberg, 2011.
[5] Op-ed: Encryption, not restriction, is the key to safe cloud computing. Available Online: http://www.nextgov.com/cloud-computing/2012/10/oped-encryption-not-restriction-key-safe-cloudcomputing/58608/
[6] “Cloud Security and Privacy”, Tim Mather, Subra Kumaraswamy, and Shahed Latif – O’Reilly Book.
[7] Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance Evaluation of Symmetric Encryption Algorithms." IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.
[8] Sanchez-Avila, C., and R. Sanchez-Reillol. "The Rijndael block cipher (AES proposal): a comparison with DES." Security Technology, 2001 IEEE 35th International Carnahan Conference on. IEEE, 2001.
[9] NIST, FIPS PUB 197, “Advanced Encryption Standard (AES),” November 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[10] Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available: http://www.redorbit.com/news/technology/1112692915/c loud-computing-growth-paas-saas-091212/
[11] Worldwide and Regional Public IT Cloud Services 2012- 2016 Forecast [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=236552
[12] John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―, 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY