Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Integrity and Security in Cloud Environment Using AES Algorithm

R G Suresh Kumar *
Associate Professor (Ph. D)
Department of Computer Science
India

Kamala kannan .R
M. Tech Final Year
Department of Computer Science
India

Abstract— Cloud computing is the recent emergent technology of IT industry. Almost every enterprise application is moved to cloud which raised the concern about the integrity and privacy of data of client as well as enterprise officials. The main goal of cloud compting is how to secure, protect the data and process. AES Algorithm is of the out sourced data in cloud enviroment the "effective automatic data reading protocol" and multi server data compression algorithm effecently check.

Keywords—AES,Cloud Computing, Data Integirity,, Error Handler

I. INTRODUCTION

Everything has cloud linked to it by one means or the other. Let it be a technical magazine or a blog, all talk about fresh new emergent technology so called cloud computing. Definition of Cloud computing varies from professionals to professionals and from individual to individual. Everyone has their own way of defining cloud computing. Basic working motto of cloud computing is to provide cheap and efficient service to the mass. This reduces infrastructure cost, data management cost, etc. cloud providers offers vast services such as software as a service, infrastructure as a service, platform as a service and also few hints of monitoring as a service. These are services faces a common problem of data integrity problem. In recent times, most of the enterprise application are deployed in cloud. Cloud are of three types, public cloud which is mostly maintained by third parties, private cloud which is used for specific application and hybrid cloud which is a combination of both the above mentioned clouds. Recent times, lot of hacking stuff are coming into report. This is due to poor security measures of corporation. In addition to the fault of corporation, there is a third party often at fault, the users.

II. CLOUD COMPUTING

Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications.In cloud computing, the word cloud is used as a metaphor for "*the Internet*," so the phrase *cloud computing* means "a type of Internet-based computing," where different services -- such as servers, storage andapplications -- are delivered to an organization's computers and devices through the Internet.The Architecture diagram for the cloud computing is shown in the below Figure 1.

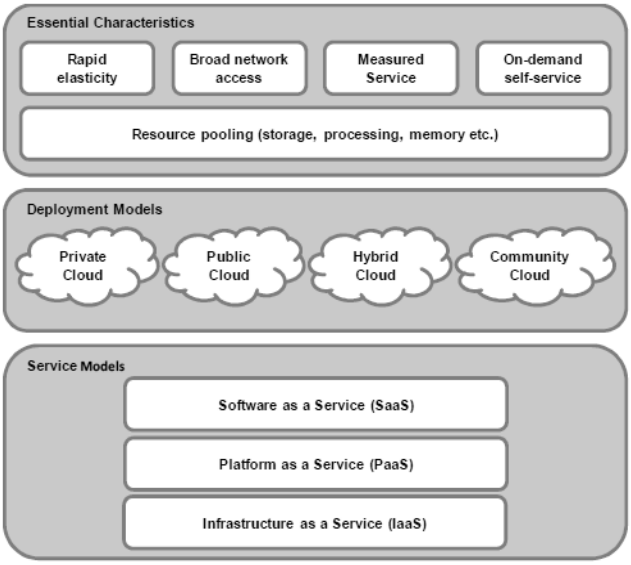


Figure 1. Overview Cloud Computing [3]

A.Cloud Computing Models

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet based on user demand.

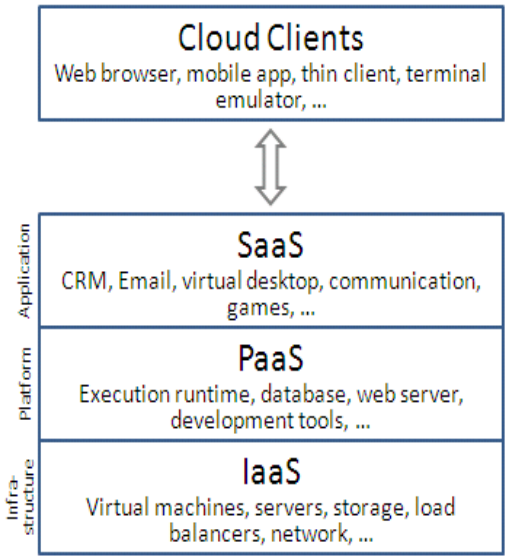


Figure2:Cloud Computing Models

1. Software as a Service (SaaS)

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet

2. Platform as a Service (Paas)

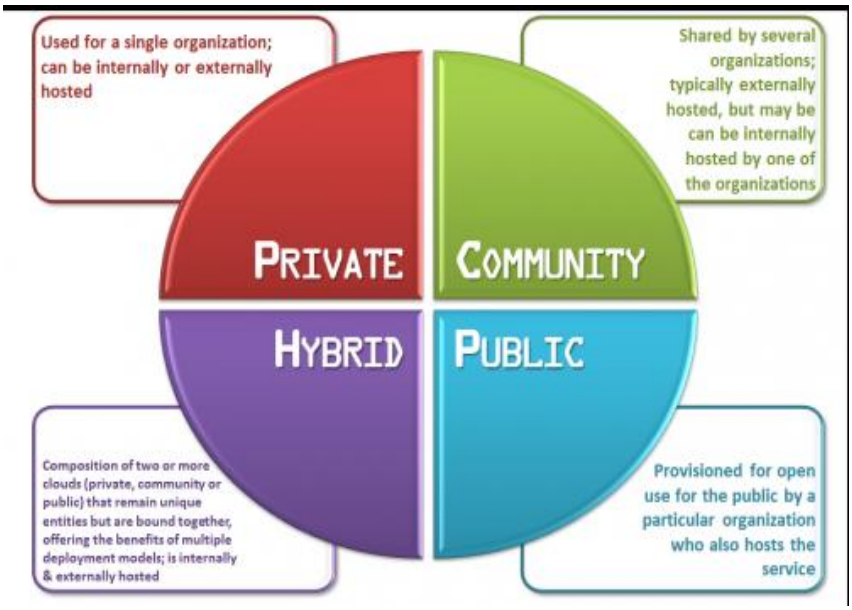
Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

3 Infrastructure as a Service (Iaas)

Infrastructure as a Service(IaaS) is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis

B.Types Of Clouds

With cloud computing technology, large pools of resources can be connected through private or public networks. This technology simplifies infrastructure planning and provides dynamically scalable infrastructure for cloud based applications, data, and file storage. Businesses can choose to deploy applications on Public, Private, Hybrid clouds or the newer Community Cloud.



A. Public Cloud

in public cloud storage, it can access by any subscriber with an internet connection and access to the cloud space.

B. Private Cloud

In private cloud storage, it is established for a specific organizations and limits to access to those organizations.

C. Hybrid Cloud

In hybrid cloud storage, it is combination of the public and private cloud storage. It means where critical cloud data located in private cloud while other data is stored and accessed from public cloud.

D.Community Cloud

In community cloud is a is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider.

III. RELATED WORK

The importance of ensuring the remote data integrity has been highlighted by the following research. Works under different security models. and these can be useful to ensure the storage correctness without having users possessing local data are all focusing on single server scenario. Jules et al.[5] defined a formal "proof of retrivabilty"(POR) model for ensuring the remote data integrity, their scheme combines spot-checking as well as error correcting code to ensure both possession and getting of files on archive service systems.

IV. PROPOSED SYSTEM

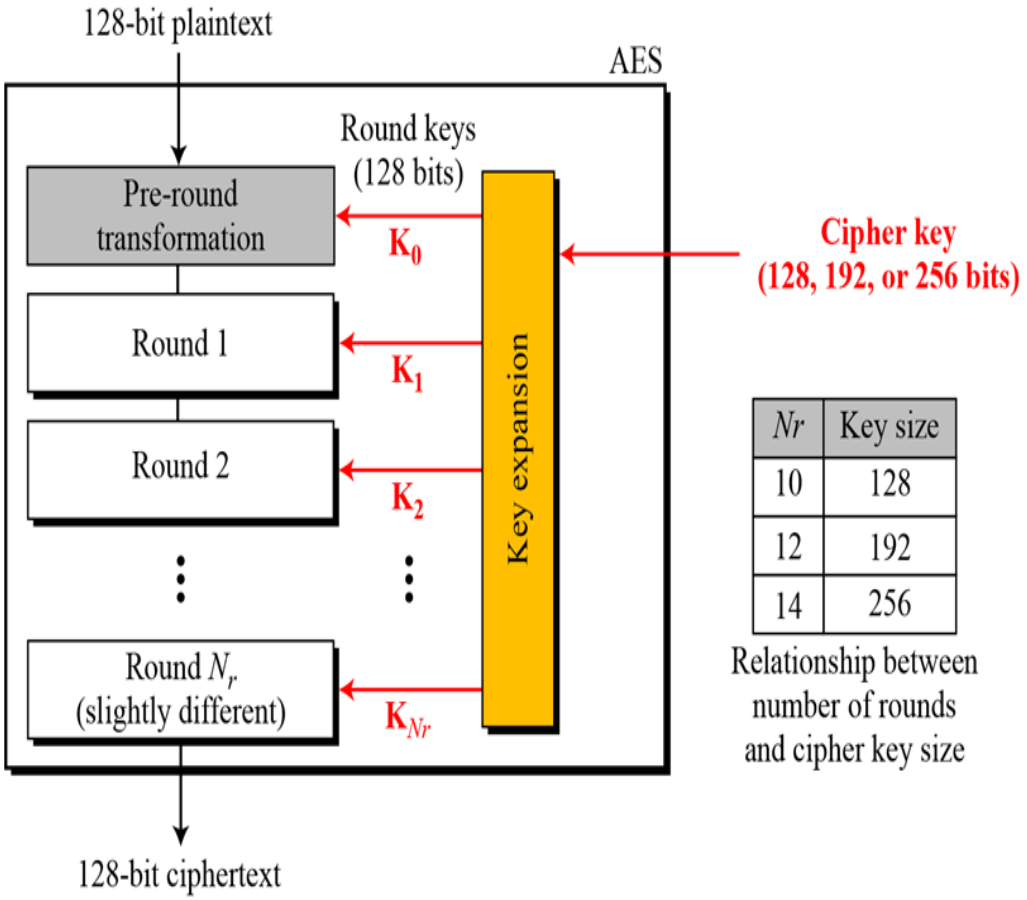
In this section, we propose a framework which involves securing of files through file encryption. The file present on the device will be encrypted using password based AES algorithm The user can also download any of the uploaded encrypted files and read it on the system.

A. AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) . The criteria defined by NIST for selecting AES fall into three areas:

1. Security
2. Cost
3. Implementation.

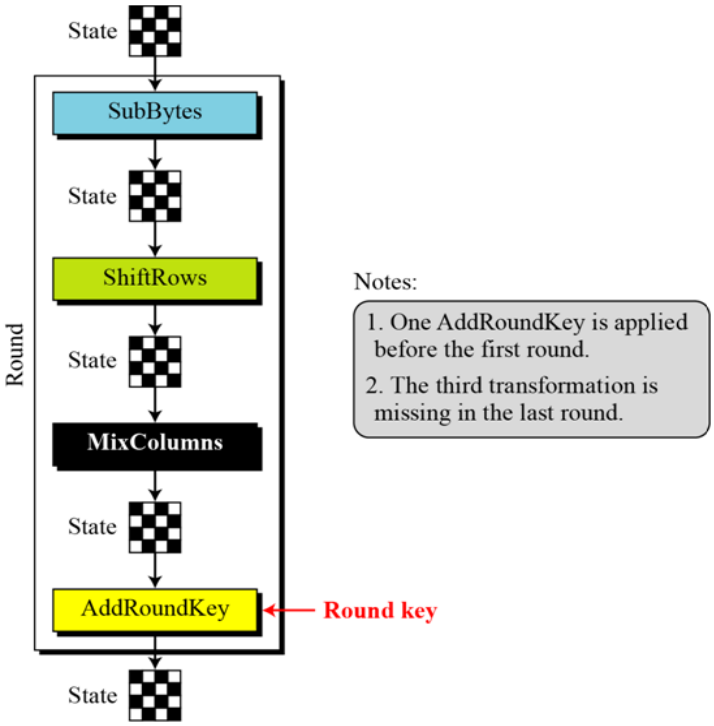
AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

The structure of the Each Round in AES Algorithm



To provide security, AES uses four types of transformations: substitution, permutation, mixing, and key-adding.

Substitution

a non-linear substitution step where each byte is replaced with another according to a lookup table.

Permutation

a transposition step where each row of the state is shifted cyclically a certain number of steps.

Mixing

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

Key-Adding

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

AES Encryption & Decryption Algorithm

AES is an algorithm for performing encryption (and the reverse, decryption) which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt or decrypt

AES Encryption Algorithm

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
        byte state[4,Nb]
        state = in
        AddRoundKey(state, w[0, Nb-1])
        for round = 1 step 1 to Nr–1
                SubBytes(state)
                ShiftRows(state)
                MixColumns(state)
                AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
        end for
        SubBytes(state)
        ShiftRows(state)
        AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
        out = state
```



```
end
```

AES Decryption Algorithm

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
        byte state[4,Nb]
        state = in
        AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
        for round = Nr-1 step -1 downto 1
                InvShiftRows(state)
                InvSubBytes(state)
                AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
                InvMixColumns(state)
        end for
        InvShiftRows(state)
        InvSubBytes(state)
        AddRoundKey(state, w[0, Nb-1])
        out = state
end
```

Comparison Of DES & AES Algorithm

The below table3 shows the comparison of DES & AES Algorithm.

	DES	**AES**
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers

V. CONCLUSION

In my work, I have used AES and provided the file level security to end users of Cloud. To open secure file, user must need securely their confidential file in storage in secure manner or user can securely transfer their confidential files across the network. By this key, all data will be in encrypted manner. This approach is quite useful because it enables user to keep away the unauthorized person such that he cannot be able to read user files.

REFERENCES

[1] Balachandra Reddy Kandukuri, Ramkrishna Paturi V, DR. Atanu Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing

[2] "Cloud computing Benefits, risks, recommendations for information security cloud computing" November 2009, http://www.enisa.europa.eu

[3] Huiming Yu, Nakia Powell, Dexter Stembridge and Xiaohong Yuan, "Cloud Computing and Security Challenges", 2012 ACM Publication

[4] Kamal Dahbur, Bassil Mohammad and Ahmad Bisher Tarakji, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing"
[5] La'Quata Sumter, "Cloud Computing: Security Risk", 2010 ACM Publication
[6] Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms to Enhance The data Security of Cloud in Cloud Computing", 2012 VSRD International Journal of Computer Science & Information Technology
[7] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", 2010 International Journal of Computer Applications
[8] Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth, "A Layered Security Approach for Cloud Computing infrastructure", 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009 IEEE.
[9] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing
[10] Mark Townsend, "Managing a Security Program in a Cloud Computing Environment", 2009 ACM Publication 978- 1- 60558-661-8/09/09

