Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021)
IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2

2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1272-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICCS51141.2021.9432070

Enhancing the Reliability of Cloud Data by Implementing AES Algorithm

N.Suganya[1],R.Sathiya[2], G.Ilamurugan[3], M.Pavithra[4], C.Karthikeyan[5]

[1]*Department of Computer Science and Engineering, Karpagam Institute of Technology, Coimbatore*

[2]*Department of Information Technology, Karpagam Institute of Technology, Coimbatore*

[3]*Department of Computer Science and Engineering, Sri Sairam Institute of Technology, Chennai*

[4]*Department of Computer Science and Engineering, J.K.K Nattraja college of engineering and technology, Komarapalayam*

[5]*Department of Computer Science and Engineering, Karpagam Institute of Technology, Coimbatore*

nrsuganya@gmail.com[1],sathiyait@gmail.com[2],
ilamurugan.cse@sairamit.edu.in[3],pavithra.m79@gmail.com[4],
karthikeyan.rdp@gmail.com [5]

Abstract: Cloud computing can be said as a technology which is based on the networks. Cloud computing has it origin from distributed computing, grid computing, utility computing. In cloud the users may pay for what they are using. To reduce the infrastructure the data can be moved from their environment to the cloud environment by the users. The users can loss the control over the data. The data moving on infrastructure will face several attacks. There is a possibility that the attacker will spoof the data from an authenticated user with ease. This paper concentrates on improving cloud computing data protection through Tclouds and trusted computing.

Keywords: cloud computing, threats, attacks

INTRODUCTION

As the technology is growing rapidly, the access to software and data storing also changes accordingly. Cloud is anywhere and everywhere. The resources are provided to the customer as a service like Software, Platform and Infrastructure as services which can be called as SAAS, PAAS, and IAAS respectively. The cloud providers provide cargo deck in the shape of information centres, where the datum is stored in a very centralized location. In cloud there is a Service Level Agreement between the service provider and user. The SLA can identify the wants of the end-user, eliminate expectations and reduce complex issues.

CHARACTERISTICS:

Improved Availability

If there exists a fault in one machine it does not affect other virtual machine. Single point of failure is avoided in cloud.

Network Access

Online services are only available through the internet. Cloud computing uses internet as a networking channel[10].

Increased Storage

The cloud can change dynamically and can handle large volume of data. With dynamic workloads it can work effectively.

SERVICE MODELS:

SAAS:

In this service, the application software is provided in the cloud. Multiple users can access it by running the single instance of the service.

PAAS:

Development environment is provided as a service from which highest layers are developed. The end-user can develop their own platform depending on the need.

Infrastructure-as-a-service:

The physical end of a data center infrastructure is maintained by IAAS provider, thereby enabling clients to completely configure the virtualized services to suit their needs.

DEPLOYMENT MODELS:

The different cloud models are as follows:

Private cloud:

Private clouds are owned and maintained by one organization. Only the members of the organization can access or control the cloud which results in secure information access. The private cloud is secured than the general public cloud.

Public cloud:

Services offered by the provider are made publicly available over the web. If the customer wants to access the cloud the customer pays for the employment.

Hybrid cloud:

This is a cloud environment which is formed by combining 2 cloud platforms namely personal and public. Private cloud is the place used for storing user information safely and for processing great deal of knowledge private cloud is employed.

Community cloud:

The infrastructure is shared among the organization in community clouds. Clouds of the environment may be located on and off the premises.

PROBLEM STATEMENT

As all the platforms now- a- days becoming digital, there comes the popularity and need to store all the data in cloud. But, with the rise of usage of Cloud computing, cloud infrastructure needs up-to-date insights into the requisite security requirements, and as an emerging technology, cloud computing solutions have specific problems and challenges.

The objective of this paper is to produce a close overview of the kinds of security issues investigated within the area of cloud computing and also the proposed solutions to accommodate the problems. It also helps cloud developers quickly identify and fix holes in cloud security concerns with a close overview.

When storing data on cloud, one might want to form sure if the info is correctly stored and might be retrieved later. The data stored on the cloud is usually considered

valuable to malicious intentioned individuals. The loss of control outside the protected company perimeter increases data security uncertainty and increases the risk of compromises. Cryptographic algorithms were implemented to enhance the security of the user's data.

RELATED WORK

The paper also relates to research on user data protection. Below are some of the plays.

Mechanisms for auditing and third party auditing are introduced in [4]. To enforce the security policies, a master checklist for internal and external auditors are used during auditing. Checklist of Iaas includes data location awareness, data ownership awareness, data protection plan. SAAS model checklist consists of data surrender activity, data format check and performance.

In the paper [8] concepts about integrity are discussed. Here, only the users who have permission or in other word the users who have authorization are able to edit the information and here confidentiality is the concept that only person who has authorization are permitted to read the information. Storage in the cloud platform also give good data protection and licensing control over user access. The data which is stored in the cloud could be compromised so that encryption of the respective information is possible in the cloud [7] before storing. The encryption methodologies such as asymmetric and symmetric key encryption were used. For decryption and encryption, public and private keys are used in Asymmetric encryption method. One key is used by Symmetric key encryption uses only single key for the same purpose. Here, when information is encrypted using the asymmetric key, it causes an encryption which is highly secured but at the same time the process is very slow. Here the way in which encryption is performed can be done on the basis of the based on the difficulty of decryption being accurate.

Moreover, information can be saved, and it can be reserved using operational and maintenance of cloud computing. Since the information is not stored in client region, security measures cannot be enforced directly. When there exists a situation in which the data is not available, the backup data are used. Cloud computing storage security enforces data isolation, data location, data long term survivability. Customers [8] will have the rights to supervise and audit cloud computing services to ensure customer data is safe. Cloud provider takes the responsibility of security, but their monitoring and auditing is an issue. The disaster recovery management includes system backup and data disaster recovery. The network transparent security is protected by the virtual private network technology.

The security problems in the cloud and strategies are discussed to solve them are given in [1]. Multi-tenancy occurs as a result of sharing the service of cloud that multiple people can use. Due to sharing, confidentiality issues are created. To avoid this issue isolation among the tenant data is preserved. Isolation will occur in VM's, data, API's and operating systems. Users calculate risk based on the non-availability of the data. In SLA the average time the services are not available for, and the chance penalty cost.

In [2] the service models and security issues are discussed. In IAAS the virtual server is used instead of the dedicated server because of the server capacity problems. In PAAS, the IDE is provided as a service where the developer can develop, deploy and complete the application life cycle. In SAAS, instead of installing the software in the desktop system it is

provided as a service and the customer can pay for what they can use.

Providing authentication and access control is important to prevent from unauthorized users accessing the data. If a company is not satisfied with any of the service provider, then the company can change the provider. Encryption is used while customer transfers data from his environment to the cloud. This is done to protect data. For more security, VPN or SSH tunneling can be implemented. The hardware components may be attacked by the people. Due to the availability, the data should be available at all the time. The backup plan of the user's data is provided either to the customers or to the provider.

PROPOSED FRAMEWORK

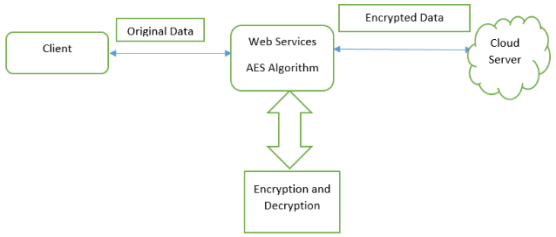


Figure 1.1 Cloud Framework

Here, an algorithm is proposed, where blocks are symmetrically ciphered in in hardware as well as software. As a result it can be named as Advanced Encryption Standard (AES). It performs all the computations on bytes and not bits. In AES four rounds are carried out to encrypt the data. Once the data is encrypted it is sent to the cloud environment. To reach the information, which is present in the cloud, the encryption of data is performed in the cloud and customer end is the place where the information will be decrypted.

AES has a series of linked operations, and it is basically a substitution-permutation network. Operations like replacing inputs with specific outputs and others processes like shuffling bits around them occurs.

ENCRYPTION PROCESS:

Each round of AES involves four sub-processes.

i)Byte Substitution

ii)Shift rows

iii)Mix Columns

iv)Add round key

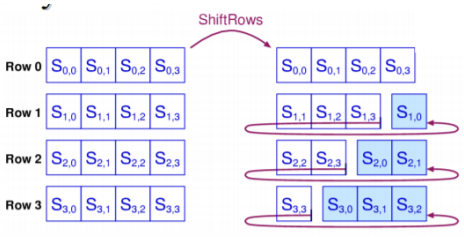
BYTE SUBSTITUTION:

A 16 x 16 table is used where replacement of each data which is in byte takes place by the byte which is having an index of the bits which are in 4th left position of the row and also 4 bits of the right column.

SHIFT-ROWS:

In shift-rows,

- I row stays the same.
- II row will circularly shift one byte to left
- III row will circularly shift two byte to left
- IV will circularly shift three byte to left



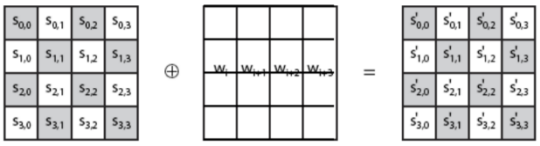
MIX-COLUMNS:

Here, a mixed approached is followed. A math function can be used to replace the data in each column. 4 bytes of a column is taken as input as well as outputs. It will lead to an output

of 16 bits. Moreover, in the final iteration this move is not performed.

ADD ROUND KEY:

The figure below shows the process. Here the 128 bits are formed using the 16 bytes which are present. This data is combined with the round key's 128 bits using XOR. Finally, the result is found, if by calculating we receive the last line. Or else, we again start to extract the 128 bits from the 16 bytes of the information present and begin another process. This process is repeatedly performed till we get the expected output.



DECRYPTION by AES:

In AES, decryption is similar as reversing the encryption. Every round is composed of the 4 processes carried out in reverse fashion.

i) Add round key

ii) Mix-Columns

iii) Shift-rows

iv) Byte Substitution

METHODOLOGY:

The following are the contributions of our work:

In the first phase, the client login into the cloud server with the authorized username and password. The client requests the server for the data. Once the request is reaches server, it verifies the request followed by sending the data to the client.

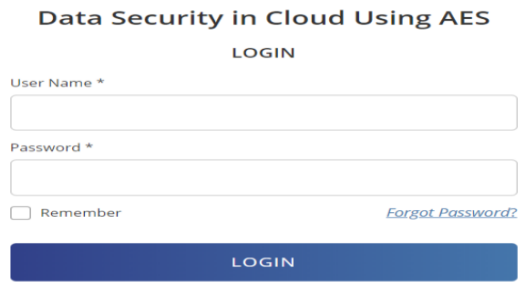


Figure1.2 Client Login into Cloud Server

Configuration of the virtual setup is the Second phase of our work. Virtual machines can be paused and restarted easily to return to previous instances, quickly since they are dynamic in nature. Virtualization is used which is a technology the helps the customer to perform function using operating systems at the same time, sharing the underlying resources on a single computer system. The programs licensed to the customer are stored in the data centers which is a server set.

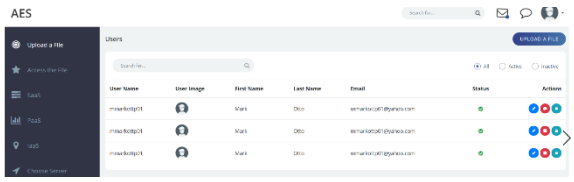


Figure1.3 Client Page

An encryption engine which was installed at the client's end will incorporate encryption strategy.

CONCLUSION AND FUTURE WORK:

We believe that data security in cloud computing, a section stuffed with challenges is in infancy now, and a lot of research problems are yet to be identified. If the users have strict security policies, their data will be confidential. To protect the confidentiality of the data, a client side strategy must be incorporated in the cloud. Encryption and decryption processes have a vital

role in preventing threats to data. There are a lot of security problems even when the encryption is implemented.

REFERENCES

[1] AkhilBhel and KanikaBhel (2012) "An Analysis of Cloud Computing security issues" World Congress on Information and Communication Technologies.

[2] Mathisen E. Security challenges and solutions in cloud computing. In5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011) 2011 May 31 (pp. 208-212). IEEE.

[3] Mohit E, Prem A. To enhance the data security of cloud in cloud computing using RSA algorithm. International Journal of Software Engineering. 2012;1(1).

[4] Gul I, ur Rehman A, Islam MH. Cloud computing security auditing. InThe 2nd International Conference on Next Generation Information Technology 2011 Jun 21 (pp. 143-148). IEEE.

[5] Deng M, Petkovic M, Nalin M, Baroni I. A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges. In2011 IEEE 4th International Conference on Cloud Computing 2011 Jul 4 (pp. 549-556). IEEE.

[6] Zhang X, Wuwong N, Li H, Zhang X. Information security risk management framework for the cloud computing environments. In2010 10th IEEE international conference on computer and information technology 2010 Jun 29 (pp. 1328-1334). IEEE.

[7] Mewada S, Singh UK, Sharma P. Security Based Model for Cloud Computing. IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC). 2011;1(1):13-9.

[8] Liu W. Research on cloud computing security problem and strategy. In2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) 2012 Apr 21 (pp. 1216-1219). IEEE.

[9] Malik A, Nazir MM. Security framework for cloud computing environment: A review. Journal of Emerging Trends in Computing and Information Sciences. 2012 Mar;3(3):390-4.

[10] Saveetha P, Arumugam S. Study on Improvement in RSA Algorithm and its Implementation. International Journal of Computer & Communication Technology. 2012 Aug 7;3(6):78.

[11] Mewada S, Singh UK, Sharma P. Security Based Model for Cloud Computing. IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC). 2011;1(1):13-9.

[12] Wang C, Wang Q, Ren K, Cao N, Lou W. Toward secure and dependable storage services in cloud computing. IEEE transactions on Services Computing. 2011 May 12;5(2):220-32.

[13] Liu W. Research on cloud computing security problem and strategy. In2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) 2012 Apr 21 (pp. 1216-1219). IEEE.

[14] Ojha N, Padhye S. Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key. IJ Network Security. 2014 Jan 1;16(1):53-7.

[15]Gurudatt Kulkarni & Jayant Gambhir, TejswiniPatil, AmrutaDongare (2012) "A security aspect in cloud computing" 3rd IEEE International Conference on Software Engineering and Service Science (ICSESS).

[16]AES Encryption: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[17]AES Encryption: https://www.comparitech.com/blog/information-security/what-is-aes-encryption/.