SECURE AND ENERGY EFFICIENT IN CLOUD COMPUTING USING AES ALGORITHM

Mrs.V.Brindha*[1], Mrs.J.Gayathri [2], Dr.R. Umamaheswari [3]
[1]PG Scholar, Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, Tamilnadu, India
[2]Assistant Professor, Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, Tamilnadu, India
[3]Professor and Head, Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, Tamilnadu, India

*Corresponding Author: brindhav87@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. More and more vulnerabilities are discovered, and nearly every day, new security advisories are published. 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. In the proposed model an encryption and key exchanging mechanism has been described based oncombination of Advanced Encryption Standard (AES), Triple Data Encryption Standard (DES) encryption algorithm and Advanced Diffie-Hellman algorithm which helps to enhance security in mobile cloud computing. Moreover, this paper focuses on to resolve the wasteenergy in the network and for this purpose offloading algorithm has been used. Since offloading algorithm has been used, data splittingcan also be done in an efficient manner. Thus, it makes difficult for the intermediate person todecipher the code.

Keywords: Cloud Computing, Cloud Security, Cryptography, AES Algorithm.

1.INTRODUCTION

Cloud computing is emerging as a key computing platform for sharing resources that include infrastructure, software, applications, and business processes. Gartner predicts by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud, with focus on messaging, web security and remote vulnerability assessment. Other focus areas will include data-loss prevention, encryption, and authentication, as technologies aimed to support cloud computing mature. The notion behind cloud computing is that work done on the client side can be moved to some unseen cluster of resources over the internet. Cloud Service Provider (CSP) maintains database and applications for the users on a remote server and provide independence of accessing them from any place through a network. There are three major cloud service categories: software-as-a-ser

vice (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS).

SECURITY ISSUES

Cyber crime's effects are felt throughout the Internet, and cloud computing is an enticing target for many reasons. Providers such as Google, Microsoft, and Amazon have the existing infrastructure to deflect and survive cyber-attacks, but not every cloud has such capability. If a cyber-criminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cyber criminals. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous websites, and without proper security, hundreds of websites could be compromised through a single malicious activity.

Cloud computing security includes a number of issues like multi tenancy, data loss and leakage, easy accessibility of cloud, identity management, unsafe API's, service level agreement inconsistencies, patch management, internal threats etc. It is not easy to enforce all the security measures that meet the security needs of all the users, because different users may have different security demands based upon their objective of using the cloud services.

2 .RELATED WORKS

Cloud storage provides users with great benefits and advantages. It provides better accessibility, for instance itenables them to access data from any device connected to the internet. There is no need for users to bring theirphysical storage devices wherever they are and they can use any computer for saving and retrieving theirinformation. It enhances teamwork and collaborative efforts by allowing team members to access shared data. Inaddition to that, cloud storage is cost saving due to not having to buy or maintain expensive hardware. Also, it canbe used for backup, archival and disaster recovery purposes. Moreover, the data are stored on many servers toguarantee a sustainable service to the clients so that they are able to access their data at any time.

DEPSKY: dependable and secure storage in a cloud-of-clouds: Bessaniet al.3 proposed DEPSKY a secure andreliable system that takes a responsibility in improving the availability, integrity and confidentiality of the storedinformation by encrypting, encoding and replicating data on different clouds that form a cloud-of-clouds. Thesystem was implemented using four cloud storage service providers (Amazon S3, Windows Azure, Nirvanix andRackspace) and PlanetLab to run clients that access the service from numerous places around the world. The paperoutlines four drawbacks of the individual cloud 1) Loss of availability 2) Loss and corruption of data 3) Loss ofprivacy 4) Vendor lock-in. It describes how the DEPSKY system succeed in dealing with them by using aneffective set of Byzantine quorum system protocols, cryptography, secret sharing, erasure codes and the varietywhich comes from using more than a single cloud.CloudSafe: Storing Your Digital Asset in the Cloud-based Safe: Zhang et al.7 proposed CloudSafe to enhanceavailability and confidentiality of the stored information in the cloud through encrypting and encoding data intoseveral cloud storage providers.

In order to make a safe, dependable and quick data access repository possible,CloudSafe offers a cloud-based personal digital asset safe service which delivers the valuable assets betweenseveral cloud providers by using erasure coding and cryptography. The storage providers are: Dropbox, GoogleDrive, Microsoft SkyDrive and SugarSync. According to Zhang et al., the availability improves due to usingerasure coding to distribute the data on several cloud providers, in order to recover data access

when a providerfails. AES24 have been used for encrypting and decrypting data to keep data confidentiality.A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding: Lin et al.4 proposed athreshold proxy re-encryption scheme and combined it with a non-centralized erasure code to design a securedistributed storage system that offers secure and strong data storage and recovery. In addition, the formulatedstorage system allows users to forward their data to the server and to other users. The proposed system providesstrong confidentiality and secrecy of messages in storage servers. The re-encryption scheme boosts encodingoperations over encrypted messages and forwarding operations over encoded and encrypted messages. But each ofthese solutions has many limitations.

Seiger et al.5 has a few limitations like that it needs more management andresources, keys are managed by the provider and data is exposed to hacking attacks when a user sends it to theservers of the service provider or in case the hacker breaks the transmission security protocol. Bessaniet al.9requires a lot of physical resources thus increases costs. Another limitation of the paper is that keys could bemanaged by many servers which will increase risk. Somani et al. 6 also has a few limitations for example it usesthe RSA encryption technique that is less secure and slow in encrypting and decrypting large amount of data. RSAcontains a public and a private key therefore the solution needs key management from a third party, which willincrease risk.

3 .PROPOSED SYSTEM

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.

Our target is to handle two issues the user encounter when using cloud computing services. Thefirst one is users concerns about hacking threats whether internally or externally. The other one is the infeasibilityof encrypting all data without taking into consideration its confidentiality degree. Therefore, we propose aframework that allows the users to encrypt own data using a key that is not available for the provider. In additionwe encrypt data bases on the degree of confidentiality.

4.ADVANTAGES

- The user decides to use cloud services and migrate his data on the cloud.
- User submits his service requirements with CSP's and chooses provider offering best specified services.
- When migration of data to the chosen CSP happens and in future whenever an application uploads any data on the cloud, the data is encrypted and then sent.
- The encryption process is done using AES algorithm.
- Once encrypted, data is uploaded on the cloud.

5 .SYSTEM MODEL

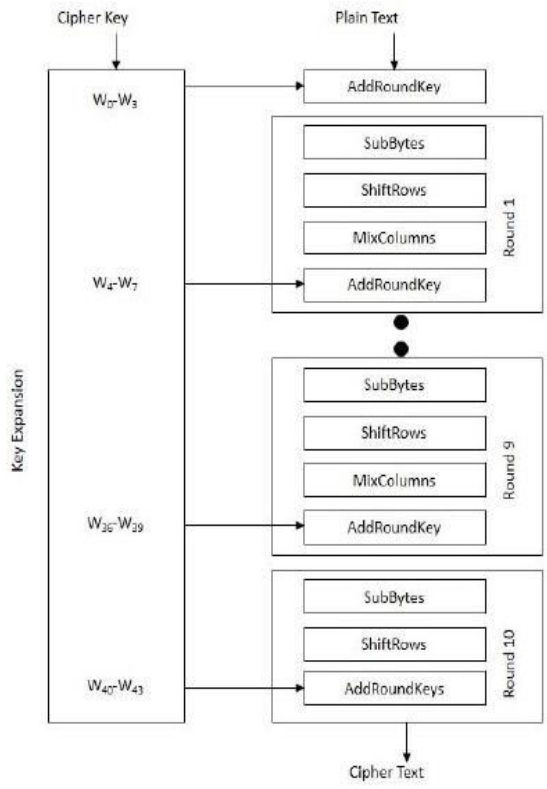

Fig 1 System Model

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-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:

- SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-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 key using a key schedule.

COMPARING AES WITH OTHER ALGORITHMS

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, nonlinearity of the key expansion practically eliminates the possibility of equivalent keys in AES. A performance comparison amongst AES, DES and Triple DES for different microcontrollers shows that AES has a computer cost of the same order as required for Triple DES [9]. Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blowfish in terms of time consumption [8].

PERFORMANCE EVALUATION

We have built a simulator to evaluate the proposed framework. The simulator was developed using Microsoft.Net C# with the support of library System Security which is implemented within C# and using the default settingsin Microsoft .NET Framework 4.5. We have done all necessary validations and verifications. All simulationexperiments were conducted using the same platform: Intel(R) Core(TM) i7-2600K CPU, processor speed3.40GHz, and RAM of 3 GB. The operating system is Microsoft Windows NT 6.1.7601 SP1. We used theprovided classes in Microsoft .Net environment to simulate 3DES, AES128 and AES256. Security library thatprovides the functionality of a cryptographic cipher used for encryption and decryption.

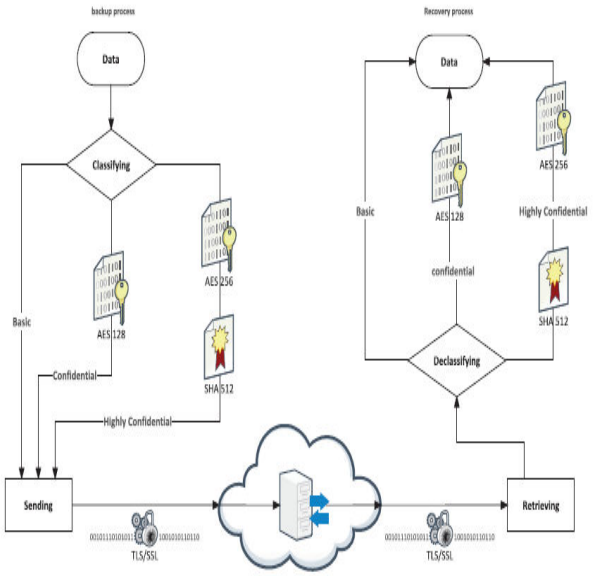

Fig 2 secure cloud framework

We have tested the performance of symmetric algorithms including AES128, AES256 and 3DES. Theperformance evaluation is based on the time needed to encrypt data blocks with different sizes varied between 2GB and 10 GB. The results showed that AES128 has outperformed the other algorithms in terms of speed inencrypting data blocks as it has the lowest processing time compared to other algorithms.

CLOUDLETS

With the emerging cloud computing and theexplosive growth of mobile applications, mobile cloudcomputing (MCC) has become a promising technology formobile services. In MCC, mobile devices, such as smartphones and tablets, can offload data storage andcomputational task on to the cloud through wirelesscommunications, thereby overcoming their limitedcapabilities regarding processing power, storage capacity,and battery lifetime.

The remote cloud provides data storage and computingservice while mobile devices are clients to access the servicethrough wireless networks, mainly cellular and WLAN(Wireless Local Area Network). When accessing a remotecloud is costly due to long WAN (Wide Area Network)latencies, a mobile user can exploit nearbyComputers that are well-connected to the Internet and usescloud service over a high-bandwidth WLAN. The vastcomputation resources on remote cloud servers can enablecomputation intensive applications, such as imageprocessing for video games, optical character recognition(OCR), and augmented reality, run on mobile devices.WiFi or Bluetooth to form a mobile cloudlet, in which mobiledevices (referred to as cloudlet nodes) can be computingservice providers as well as clients of the service. Bydividing the task among cloudlet nodes, the initiator mobiledevice could speedup computing and conserve energy.Users can get direct cloud computing access instantlythrough interactions among one another, eliminating thecommunication latencyand data roaming charges introduced by the cellularnetworks. Mobile cloudlet is appealing to users pursuing acommon goal in group activities,

such as multimediasharing for audience at an event and language translationfor a group of tourists in aforeign country. The major concern of using mobile cloudletresides in the limited computing power of mobile devicesand the unstable connections between cloudlet nodes dueto node mobility.

6. PROBLEM STATEMENT

Organizations can use services and data stored asand when required at any physical location outside theirown control. This facility raised the various security issueslike privacy, confidentiality, integrity etc., and demanded atrusted computing environment wherein dataconfidentiality can be maintained. To get rid of the sameand to induce trust in the computing, there is need of asystem which provides authentication, verification andencrypted data transfer, hence maintaining dataconfidentiality.

7. CONCLUSIONS

In this paper, we have proposed an efficient confidentiality-based cloud storage framework that enhances theprocessing time and assures confidentiality and integrity through data classification and applying TLS, AES andSHA based on the type of classified data. The efficiency of our proposed framework has been shown throughconducting simulations. The simulation results show that our framework achieves better processing time whileassuring data confidentiality and integrity. As part of our future work, we plan to enhance our framework byconsidering other aspects. This includes automatic data classification and the use of different cryptographicalgorithms such as asymmetric public key, RSA, and Elliptic curve cryptography that could provide higher degreeof confidentiality and security.A strong user authenticationframework for cloud computing with Advanced Diffie-Hellman algorithm, AES ,3DES and Digital Signature. Inthe proposed work a offloading algorithm, we incorporatethe data caching mechanism and improve taskmanagement strategies with dynamic energy schedulingalgorithm which shows that the high efficiency of ouralgorithm allows the mobile device to calculate the optimaloffloading decision at the local end with much lower timecomplexity and energy consumption.

REFERENCES

[1] B.Karthikeyan, Dr.T.Sasikala and K.Nithya, "Secure AndEnergy Efficient Model With ModifiedOffloading Algorithm In Mobile CloudComputing," Asian Journal of Research in Social Sciencesand Humanities Volume 6, Special Issue, Sept 2016 (BASEPAPER)

[2] Ragini, ParulMehrotra, S.Venkatesan, "An EfficientModel For Privacy And Security In MobileCloud Computing," International Conference on RecentTrends in Information Technology, 2014.

[3] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos,"Security In Cloud Computing: OppurtunitiesAnd Challenges"http://dx.doi.org/10.1016/j.ins.2015.01.025.

[4] SaurabhDey, SrinivasSampalli, Qiang Ye, "A LightweightAuthentication Scheme Based OnMessage Digest And Location For MobileCloud Computing," IEEE 2014.

[5] Xu Yang, Xinyi Huang, Joseph K. Liu.http://dx.doi.org/10.1016/j.future.2015.09.028.

[6] HuiSuo, Zhuohua Liu, Jiafu Wan, Keliang Zhou,"Security And Privacy In Mobile CloudComputing," IEEE 2015.

[7] "Cloud Security and Privacy", Tim Mather, SubraKumaraswamy, and ShahedLatif – O'Reilly Book.

[8] Elminaam, DiaaSalama 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.

[9] 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.

[10] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[11] Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available: http://www.redorbit.com/news/technology/1112692915/cloud-computing-growth-paas-saas-091212/

[12] Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast [Online]. Available:

http://www.idc.com/getdoc.jsp?containerId=236552

[13] 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.

[14] Jensen, Meiko, et al. "On technical security issues in cloud computing." Cloud Computing, 2009.CLOUD'09.IEEE International Conference on.IEEE, 2009.