Indian J.Sci.Res. 17(2): 666-672, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

TITLE: "ENHANCED EFFICIENT KEY MANAGEMENT FOR ONLINE ACADEMIC SYSTEM (OAS) IN ORDER TO PROTECT DATA IN THE PRIVATE CLOUD"

Sri G Sudhakar, Dr. S.Durgabhavani
Research Scholar & Lecturer, School of IT, JNTUH.
Professor & Director, School of IT, JNTUH.

Abstract - Now-a-days issues related to the security of data in cloud computing has become the most important topic in the IT Market. In Cloud only administrators can help decision-makers look beyond the three (software, platform and infrastructure) top cloud providers to specialized services that offer easy-to-use platforms and low cost relative to the value they provide. These specialty cloud providers can more suitably fit a company's cloud strategy, saving the company time and money. Developing a private or internal or corporate cloud for an organization is now become very important so as to keep the sensitive data safe..Online Academic system (OAS) a Cloud based application for the institution or organizations that can be accessed throughout the institution or a specific department in the institution or organization. This system (OAS) is being developed to maintain and facilitate easy access to information. For this the clients need to be signed up with the system after that they can login to the system and perform tasks per the privileges provided for them. The Cloud processing is the figuring innovation which gives assets like programming, equipment, and Cloud based information capacity frameworks have numerous complexities with respect to basic, private, delicate information of customer. The trust required on distributed storage is so far had been restricted by clients. The information stockpiling in the cloud has been a promising issue in these days. The major part of security is needed on area of data security and integrity of the academic data.

Key Words: cloud, security, online academic system, academic data, administrators, cloud strategy.

I. Introduction

To provide strong protection on data integrity, cryptographic methods can be applied. Intuitively, one may want to use message authentication codes (MAC) for data integrity. Initially, data owners (cloud users) locally generate a small amount MACs for the data files to be outsourced and maintain a local copy of these MACs. Whenever the data owner needs to retrieve the file, he can verify the data integrity by re-calculating the MAC of the received data file and comparing it to the locally pre-computed value. In case the size of data file is large, a hash tree [10] can be employed, where the leaves are hashes of data blocks and internal nodes are hashes of their children of the tree. The data owner only needs to store the root nodes of the hash tree to authenticate his received data. Whenever the data owner needs to retrieve a block or blocks of data, the server sends the data bock(s) as well as the necessary internal hash nodes, which can be either computed on the y or pre-computed by the cloud servers, to the data owner. The data owner calculates the hash value(s) of the received data block(s), with which he can compute the root hash given other internal hash nodes sent by the server. Data integrity is verified against the stored root hash. Given the second pre-image resistance property of the hash function, security of the data integrity

Verification mechanism can be achieved. While this method allows data owners to verify the correctness of the received data from cloud, it does not give any assurance about the correctness of other outsourced data. In other words, it does not give any guarantee that the data in the cloud are all actually intact, unless the data are all downloaded by the owner. Because the amount of cloud data can be huge, it would be quite impractical for data owner to retrieve all of his data just in order to verify the data is still correct. In case that the data auditing task is delegated to TPA, this method inevitably violates our suggested requirements, including: large auditing cost for cloud server (for accessing and transferring the whole data), and data privacy exposure to TPA (for retrieving local copy of data). OAS is creating basic Web based application links with database applications. The service uses Microsoft SQL Server as the back end, but users do not have to interact directly with the relational database management system. Instead, they use a point-and-click interface to create custom applications. The app builder allows users to create forms, publish data, create reports and generate graphs. There is also support for password authentication, styles, localizations and multiple languages.

II. Security Issues in cloud

Data Security

Storing the sensitive data using on-premises application deployment models allows the control of physical, logical and personnel security, as well as the application of access control policies. Because enterprise data is stored outside the enterprise when using the cloud, the provider must prevent vulnerabilities and malicious users to avoid breaches and guarantee data security.

[1] **Corresponding Author**

Subashini & Kavitha urged the use of strong encryption techniques and fine-grained authorization to control data access. Subashini & Kavitha suggested administrators to eliminate access to customer instances and deleting the OS Guest user, as Amazon does with its EC2. However, Subashini & Kavitha added that individual cryptographically strong Secure Shell (SSH) keys are required by EC2 administrators to access a host. Logging and auditing for such access is routine. Users should encrypt their data before uploading. To test and validate the security of enterprise data stored in the cloud, Subashini & Kavitha suggested implementing the following assessments [1]:

Cross-site scripting (XSS): checking if the site is vulnerable to injection of code into the site content from outside sources.

Access control weaknesses: checking for allowance of unauthorized access to data or applications.

OS and SQL injection flaws, allowing injection of code or queries from invaders if left unidentified.

Cross-site request forgery (CSRF) by the user's browser poses a threat. Logging the IP can aid forensics.

Cookie manipulation, adding content to cookies that will be accepted by future users

can be prevented by using secure cookie storage.

Hidden field manipulation: using hidden fields put there by lazy programmers to obtain confidential information or breach databases creates great vulnerability.

Sometimes the programmers actually place confidential information within hidden fields making that information easily available to anyone who looks. Hidden fields should never be used.

Insecure storage: both physical and digital storage insecurity can result in data breach or loss.

Insecure configuration: which has security holes easily exploited should be carefully checked every time any change is made in the code .On the other hand, to ensure cloud data storage security, Wang et al. considered the task of authorizing a third party auditor (TPA), on behalf of the cloud client, to confirm the integrity of the dynamic data stored in the cloud and to evaluate the service quality from an objective and

independent perspective [2].

Insider Attacks

Cloud authorized users may be considered an insider threat if the users attempt to gain access to unauthorized privileges or to misuse authorized privileges in order to commit fraud, reveal information to others, or alter or destroy information. As a matter of fact, Modi et al. Illustrated that this can pose a serious trust issue between cloud providers and users [3].

Flooding Attacks

Zombies (innocent compromised hosts) are used to flood victims by sending huge number of packets of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) or a mix through the network. Illegal network connections and bots facilitate these attacks. This makes Bring your Own Device (BYOD) a serious security concern for enterprises using cloud [4][5][6][7][8]. Modi et al. urged that since the

application of VMs are available to anyone through the Internet, cloud computing is thus vulnerable to DoS or Distributed Denial-of-Service (DDoS) attacks via zombies [3]. Therefore, service's availability to authorized users can be affected by flooding attacks. This, in fact, can lead to loss of availability of the proposed service if the attacks target certain services provided on a single server. Direct DoS attacks are involved in this case. Moreover, indirect DoS attacks are meant for other service instances deployed on the same hardware machine that is completely exhausted by processing the flood requests. Differentiating between normal and fake usage in these attacks is a daunting task, and leads to a spiked increase in cloud usage bills. However, some solutions to detect and filter attack traffic exist in research such as Cloud TraceBack (CTB)

which Chonka et al. introduced [9].

User to Root Attacks

Password sniffing is used in User to Root Attacks to gain access to legitimate user's accounts. As a result, the attacker can exploit weaknesses in order to achieve root level access to the system, either physical or virtual. Root shells, as Modi et al. described, can be generated from buffer overflows using processes running as root [35]. This can happen when the static buffer is overfilled with application program code. Thus, a frequent target to attackers is the authentication process and the mechanisms used to secure it. Besides, keyloggers, phishing attacks, weak password recovery workflows, etc. do not have universal standards. Dual user authentication and biometrics may make this less of an issue as this technology matures. Thus in cloud gaining root level access to VMs or host can be acquired by attackers who can obtain access to valid user instances.

Port Scanning

Open ports, filtered ports, and closed ports lists can be extracted from port scanning. Attackers find open ports and attack the running services. Firewall rules, gateway filtering, router, IP address, Media Access Control (MAC) address, and other network related details can be

obtained. Modi et al. concluded that services can be attacked in the cloud using a port scanner where these services are provided [3]. However, if the provider runs in stealth mode, and users must type their desired access instead of selecting it, most of these problems disappear, though customers who hate to type may follow them..

III. Security issues in a private cloud

A private cloud model enables the customer to have total control over the network and provides the flexibility to the customer to implement any traditional network perimeter security practice. Although the security architecture is more reliable in a private cloud, yet there are issues/risks that need to be considered:

1) Virtualization techniques are quite popular in private clouds. In such a scenario, risks to the hypervisor should be carefully analyzed. There have been instances when a guest operating system has been able to run processes on other guest VMs or host. In a virtual environment it may happen that virtual machines are able to communicate with all the VMs including the ones who they are not supposed to. To ensure that they only communicate with the ones which they are supposed to, proper authentication and encryption techniques such as IPSec [IP level Security] etc. should be implemented. [11]

2) The host operating system should be free from any sort of malware threat and monitored to avoid any such

risk [12]. In addition, guest virtual machines should not be able to communicate with the host operating system directly. There should be dedicated physical interfaces for communicating with the host.

3) In a private cloud, users are facilitated with an option to be able to manage portions of the cloud, and access to the infrastructure is provided through a web interface or an HTTP end point.

There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to develop the web interface using common languages such as Java, PHP, wand Python etc. As part of screening process, Eucalyptus web interface has been found to have a bug, allowing any user to perform internal port scanning or HTTP requests through the management node which he should not be allowed to do. In the nutshell, interfaces need to be properly developed and standard web application security techniques need to be deployed to protect the diverse HTTP requests being performed [13].

4) While we talk of standard internet security, we also need to have a security policy in place to safeguard the system from the attacks originating within the organization. This vital point is missed out on most of the occasions, stress being mostly upon the internet security. Proper security guidelines across the various departments should exist and control should be implemented as per the requirements [12].

Thus we see that although private clouds are considered safer in comparison to public clouds, still they have multiple issues which if unattended may lead to major security loopholes as discussed earlier. The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud. A trust model of cloud security in terms of social security has been discussed in [14].

Social insecurity has been classified as multiple stakeholder problem, open space security problem and mission critical data handling problem. All these issues have been considered while proposing a cloud trust model also known as "Security Aware Cloud".

Pros and cons of private cloud

When an organization properly architects and implements a private cloud, it can provide most of the same benefits found in public clouds, such as user self-service and scalability, as well as the ability to provision and configure virtual machines (VMs) and change or optimize computing resources on demand. An organization can also implement chargeback tools to track computing usage and ensure business units pay only for the resources or services they use.

Private clouds are often deployed when public clouds are deemed inappropriate or inadequate for the needs of a business. For example, a public cloud might not provide the level of service availability or uptime that an organization needs. In other cases, the risk of hosting a mission-critical workload in the public cloud might exceed an organization's risk tolerance, or there might be security or regulatory concerns related to the use of a multi-tenant environment. In these cases, an enterprise might opt to invest in a private cloud to realize the benefits of cloud computing, while maintaining total control and ownership of its environment.

However, private clouds also have some disadvantages. First, private cloud technologies, such as increased automation and user self-service, can bring some complexity into an enterprise. These technologies typically require an IT team to rearchitect some of its data center infrastructure, as well as adopt additional management tools. As a result, an organization might have to adjust or even increase its IT staff to successfully implement a private cloud. This is different than public cloud, where most of the underlying complexity is handled by the cloud provider.

Another potential disadvantage of private clouds is cost. A benefit of public cloud is cost mitigation through the use of computing as a "utility" -- customers only pay for the resources they use. When a business owns its private cloud, however, it bears all of the acquisition, deployment, support and maintenance costs involved. [14]

IV. Application Delivery Issues:

Application delivery

Applications have evolved significantly over the years. The term delivery is now generally accepted as the means of bringing an application to the user in this new era of mobility and cloud. In the enterprise, business applications have moved away from desktop-bound software installed on a local server accessed by users across the LAN. Modern applications need to work across all types of networks, and at locations beyond the confines of the physical workplace.

ADCs, which are widely deployed as a key fixture in the enterprise, help applications adapt to the networks and protocols that are in place today. They also ensure that applications perform optimally, are always available and don't present any security risks either to the user or business.

Application availability

The average consumer expects the devices and applications they interact with on a daily basis to always work, and for information to be instantly available on demand. These expectations have carried over to the types of devices and applications that they use. To satisfy today's workers, business applications need to be as intuitive and easy to use as the ones they rely on for personal tasks and entertainment.

Many employees are no longer restricted to using locked-down, company-owned equipment, and can use personal devices to work whenever they choose. With people working at any time of the day or night, IT must make certain that workplace servers and applications are available around the clock. Enterprises invest heavily in IT infrastructure to ensure that employees always have access to applications and information when they are needed.[16]

Application and user security

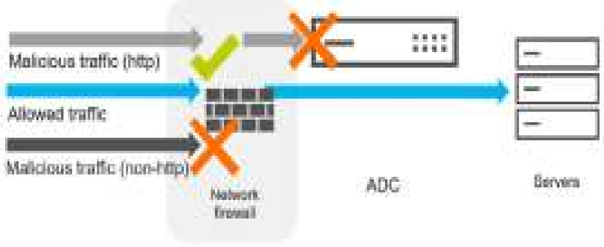
Delivery over the web has introduced new threats and vulnerabilities that traditional LAN-bound applications never had to contend with. As workers become more mobile and require remote access to applications and data, IT must devise more-stringent safeguards against external attacks and data leakage.

ADCs serve as the natural entry point or gateway to the network. They authenticate each user attempting to access an application. If the application is SaaS based, the ADC can validate a user's identity using an on-premises Active Directory data store that eliminates the need to store credentials in the cloud. Not only is this process more secure, it also enhances the user experience by providing single sign-on capabilities across multiple applications.

SAML, the XML-based protocol, is now widely used to simplify the application login process. The ADC can act as a SAML agent, authorizing users via any data stores where their identity can be confirmed. Some applications allow the use of credentials from sites such as Facebook or Google+ to validate identity before granting access. ADCs can act as a SAML identity or service provider in this respect.

Distributed Denial-of-Service (DDoS) attacks have become rampant.1 Enterprise web properties, specifically, are being targeted with the intent of overwhelming their servers and disrupting their ability to conduct business. The ADC can implement rate-limiting measures to protect internal server resources from being targeted by these specially designed attacks. When an unusually massive surge of inbound requests occurs, the ADC can throttle these requests and minimize the amount of available bandwidth they consume, or reject the request entirely.

ADCs have converged load balancing and advanced Layer 7 protection, which traditionally were only available as standalone solutions. Application firewalls can inspect data packet headers for suspicious content or malicious scripts that may not be detected by network firewall (See Figure).

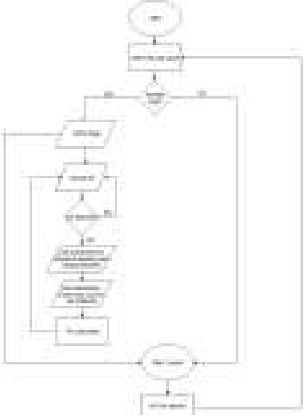


Protection beyond network firewall capabilities (Layer7) [16]

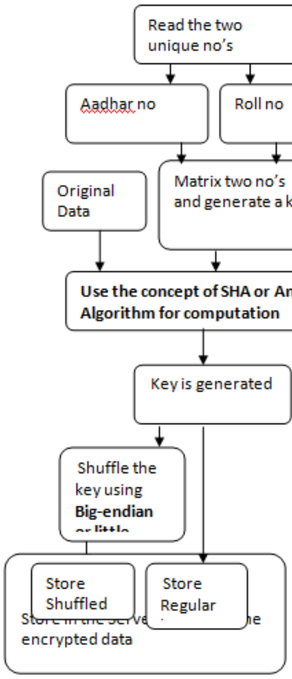
V. Implementation

Proposed Online Academic System (OAS)

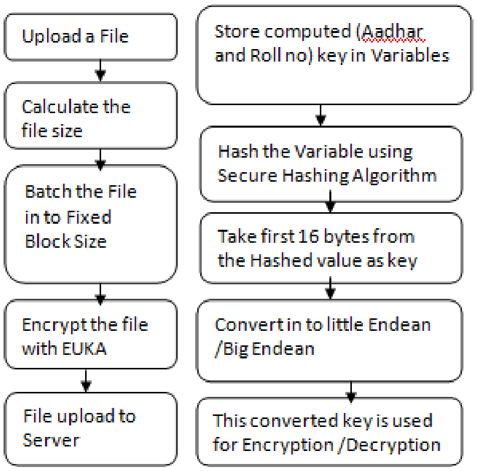
5.1 Cloud Architecture of Online Academic System



5.2 Files Upload – Encryption & Hash Value


Read the two unique no's
Aadhar no
Roll no
Original Data
Matrix two no's and generate a key
Use the concept of SHA or Any Algorithm for computation
Key is generated
Shuffle the key using Big-endian or little
Store Shuffled
Store Regular
Store in the serve
encrypted data

5.3 Proposed Enhanced Unique key Algorithm (EUKA) Flow Chart


Upload a File
Calculate the file size
Batch the File in to Fixed Block Size
Encrypt the file with EUKA
File upload to Server
Store computed (Aadhar and Roll no) key in Variables
Hash the Variable using Secure Hashing Algorithm
Take first 16 bytes from the Hashed value as key
Convert in to little Endean /Big Endean
This converted key is used for Encryption /Decryption

5.4 Steps in Uploading a File & Key Management

VI. Result Analysis:

We had executed every one of the calculations utilizing EUKA encryption systems which were already executed as AES and RSA based encryption techniques the advantages of utilizing EUKA are as decrepit Some factors that are broke down by considering bundle estimate while utilizing EUKA , by which we expect that our system will give effective outcome then past created framework. Thus, EUKA encryption and unscrambling speed is a great deal more less and in this manner said to be more effective than

AES and RSA. What's more, numerous more advantages of utilizing EUKA are said in [13].

S.No	Factors Analyzed	AES	RSA	EUKA Proposed
1	Key used	Random	Random	Unique
	Key length	128	1024	variable
	Key computed	No	No	Yes
2	Simulation Speed	moderate	low	High
3	Power consumption	moderate	high	low
4	Hardware & Software Implementation	Not efficient	Efficient	Highly Efficient
5	Security	secure	Min Attack	Highly Secure

After usage of EUKA instead of AES and RSA alongside secured hash work we got more proficient outcome. With the best encryption system calculation i.e. EUKA , system should demonstrate the proficient execution in its execution, the security safeguarding ought to be accomplished along these lines, that TPA ought to not request the duplicate of entire information and won't any learning from the information or putting more weight on the end client. The performance of

the system is improved by using tomcat server which is easy to handle and has higher processing capabilities.

Attacking module used should be able to find Found that compared to individual auditing, batch auditing indeed helps reducing the TPA computation cost by 20 the altered data in the cloud when the data is stored or updated dynamically.

As there is less number of expensive operation required for batching such as modular exponentions and multi

applications. In the wake of directing group inspecting test with expanded no of undertaking from 1 to 2000, with interims of 8.

Total File Size(kb)	No. of blocks of the file(4kb)	Total uploading time using EUKA (ms)	Total uploading time using AES(ms)	Total uploading time using RSA(ms)
6.49	2	31211	35181	37586
160	41	17802	18838	33802
628	158	101112	101179	156283
1024	308	179211	201771	358745

We had additionally attempted to bolster information flow alongside protection preserving. Some factors that are examined by considering parcel measure while utilizing EUKA, by which we expect that our framework will give proficient outcome then past created framework. Consequently, AES encryption and decoding speed is a great deal more less also, consequently said to be more proficient then AES and RSA. What's more, numerous more advantages of utilizing AES are said in [10] The graphical representation of the outcome are appeared in the following graph in which transferring time is spoken to on y-axis, the blue line (Series1) represent the qualities for AES while red (series2) shoes an incentive for RSA, while information measure is spoken to on x-axis, it demonstrates that chart of RSA goes high which demonstrates the required more opportunity for uploading the record then AES. Results are gone up against the framework which has the accompanying setup Intel centre i3 processor,1.66 GHz spped,32 bit working system,2gb Slam ,500gb hard plate. Result may change on various setups. In the organization or in an academic system it is very important that

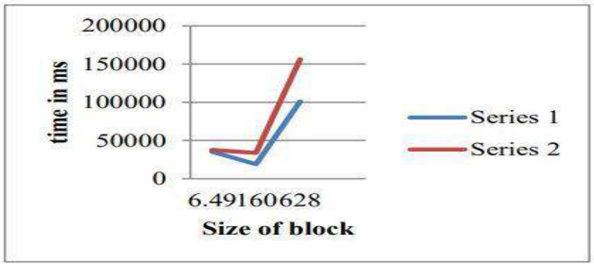


Figure 5: Graph Size of block vs Time(ms) for AES and EUKA

VII. Conclusion

In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud computing. Although the computational time is increased but the privacy is preserved the data is stored in the cloud by using the most a Unique Algorithm and compared with prominent algorithm AES. We use the homomorphism straight authenticator and arbitrary veiling to ensure that the TPA (if any) would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the load of cloud user from the tedious and possibly expensive auditing task, but also reduces the users fear of their outsourced data leakage. Considering TPA may simultaneously deal with different review sessions from various clients for their outsourced information records, we additionally expand our privacy-preserving public auditing protocol into a multi-client setting, where the TPA can play out different inspecting assignments in a bunch way for better effectiveness. We had beaten the greater part of disadvantages of the current framework by securing information flow and execution change. General examination demonstrates that our plans are provably secure and profoundly effective. Our preparatory analysis led case further shows the quick execution of our plan on both the cloud and the examiner side. We leave the undeniable usage of the system on business open cloud as a vital future degree.

Future Work

The above mentioned algorithm is vulnerable if the unique values are known to the other near and dear ones so the additional security can be achieved if the algorithm can use an oyher algorithm which can defect the facial features and convert into the variable value used to use as a key for encryption and decryption.

References

[1] S. Subashini, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1 – 11, 2011.

[2] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, May 2011.

[3] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, Jan. 2013.

[4] P. Gupta, A. Seetharaman, and J. R. Raj, "The usage and adoption of cloud computing by small and medium businesses," *International Journal of Information Management*, vol. 33, no. 5, pp. 861 – 874, 2013.

[5] X. Wei, L. Gomez, I. Neamtiu, "Malicious Android Applications in the Enterprise: What Do They Do and How Do We Fix It?," in *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on*, 2012, pp. 251–254.

[6] R. G. Lennon, "Bring Your Own Device (BYOD) with Cloud 4 Education," in *Proceedings of the 3rd Annual Conference on Systems, Programming, and Applications: Software for Humanity*, New York, NY, USA, 2012, pp. 171

[7] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," *IT Professional*, vol. 14, no. 5, pp. 53–55, Sep. 2012.

[8] R. Oppliger, "Security and Privacy in an Online World," *Computer*, vol. 44, no. 9, pp. 21– 22, Sep. 2011.

[9] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1097 – 1107, 2011.

[10] " International journal of science and research india online" ISSN:2319-7064

[15]- http://searchcloudcomputing.techtarget.com/ definition /private-cloud.

[16] www.citrix.com/netscaler.