ISSN 2277-3061

A HYBRID APPROACH OF AES AND FILE ENCRYPTION TO ENHANCE THE CLOUD SECURITY

Nisha [1], Naseeb Singh [2]
[1] Research Scholar, Department of Computer Science Engineering, AIET, Faridkot
[2] Assistant Professor, Department of Computer Science Engineering, AIET, Faridkot

ABSTRACT

Cloud computing is a paradigm shift in the way we define software and hardware, and architect our IT solutions. The emerging cloud technologies, due to their various unique and attractive properties, are evolving with tremendous momentum and rapidly being adopted throughout the IT industry. In this dissertation, we identify security challenges that arise in integration of cloud-based services, and present a set of novel solutions to address them. We analyze the security of our solutions, demonstrate their usage and effectiveness, and evaluate their performance by extensive experimentation. To address the problem of security in untrusted cloud storage, we introduce a hybrid solution of AES and file encryption. The key used in AES algorithm is generated randomly from the file's data which is sent by the cloud provider. After implementing the proposed methodology, we have seen an improvement in the processing time and cost which will increase the overall efficiency of the system.

Keywords

Cloud Computing; Cloud Security; Confidentiality; AES; File Encryption; Ciphers; Cloud.

INTRODUCTION

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. There are some important points in the definition to be discussed regarding Cloud Computing[4]. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable.

There are many benefits stated of Cloud Computed by different researchers which make it more preferable to be adopted by enterprises. Cloud Computing infrastructure allows enterprises to achieve more efficient use of their IT hardware and software investments. This is achieved by breaking down the physical barrier inherent in isolated systems, automating the management of the group of the systems as a single entity. Cloud Computing can also be described as ultimately virtualized system and a natural evolution for data centers which offer automated systems management.

SECURITY ISSUES IN CLOUD COMPUTING

Security issues come under many guises both technical and socio-technical in origin. To cover all the security issues possible within the cloud, and in-depth. Existing efforts look to provide a taxonomy over the issues seen. The Cloud Security Alliance1 is a non-profit organisation that seeks to promote the best practises for providing security assurance within the cloud computing landscape. The Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classiffcation of security issues found within the cloud.

Although insecure APIs can lead to data loss or the unwanted exposure of information, consumers can also loose their information through other means.

Availability Issues: Availability issues are when users data is made inaccessible to the consumer. The data has been made unavailable. Such a lack of availability can be a result of access privilege revocation, data deletion or restricting physical access to the data itself. Availability issues can be attributed to an attacker. For example, Denial of Services attacks, attempt to the service with requests in an attempt to overwhelm the service and cease all of the services intended operations.

Data Leakage: Another form of data leakage stems from the disclosure of information that, though hidden, is deduced from freely available information. For example: say that Bob is a member of a rather masculine society i.e. rugby club. The ability to clearly identify, authenticate, authorize and monitor who or what is accessing the assets of an organization is essential to protecting an IS from threats and vulnerabilities. Separation is the key ingredient of any secure system, and is based on the ability to create boundaries between those entities that must be protected.

Security identification of threats: Essentially securing an Information System (IS), involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

Confidentiality and privacy: Confidentiality refers to only authorized parties or systems having the ability to access protected data. The threat of data compromise increases in the cloud, due to the increased number of parties, devices and applications involved, that leads to an increase in the number of points of access. Delegating data control to the cloud, inversely leads to an increase in the risk of data compromise, as the data becomes accessible to an augmented number of parties. A number of concerns emerge regarding the issues of multitenancy, data remanence, application security and privacy [19].

Integrity: A key aspect of Information Security is integrity. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware.Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication. Managing an entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated or stolen.

Account or Service Hijacking: When communicating with the CSP malicious entities may seek to reject the integrity and authenticity of the user's communication with the CSP and vice versa. There are several ways in which the integrity and authenticity of a users session can be impugned. The rise of `Web 2.0', has seen the web browser becoming increasingly used as a means to access remote services. Browser-based interfaces and authentication are used by consumers to establish a session with their service provider.

RESEARCH GAP

In this thesis work, we will try to enhance Security between the client and cloud accessing the cloud. No doubt, cloud has got multiple benefits but we should not forget that there is a high risk of data getting confidential information getting leaked It becomes necessary to find appropriate protection as the data may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. So in the recent world, security is a prime important issue. Cloud based systems saves data off multiple organizations on shared hardware systems. One important way to increase data protection, confidentiality and integrity is to ensure that the data is protected in transit and at rest within the cloud using file-level encryption. As the CSA Security Guidance points out, "encryption offers the benefits of minimum

reliance on the cloud service provider and lack of dependence on detection of operational failure." Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. No matter whether the data is in motion or at rest, it remains protected. The owner of the decryption keys maintains the security of that data and can decide who and what to allow access to the data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an admin could encrypt all backup data before sending into the storage cloud. An executive can protect corporate IP before putting it into the private cloud. And a sales representative could encrypt a private customer contract before sending it to a collaborative worksite, like Share point, in the public cloud. We will compare enhanced system against security, performance & ease of use.

- The current AES algorithm is very complex as it contains multiple rounds.
- AES consumes more CPU time and thereby consuming more power.

RESEARCH OBJECTIVES

Our main objective is to enhance the security between the client and the cloud provider by enhancing the AES algorithm using file based encryption methodology. The security has a primary role in the services of Cloud computing because the data being transferred between the client and cloud provider is of utmost importance and thereby neither the client nor the cloud provider will sacrifice on the security of the cloud.

- The data is enclosed in the encrypted format using AES by the client itself before sending it to the cloud. The cloud provider will never come to know about the original data of the client.
- Moreover, the data sent to the cloud provider is encrypted using AES encryption algorithm.
- The key used in AES is retrieved from the file sent by the Cloud provider.

These objectives are stated to ensure the privacy of the client's data when it is being transferred, processed or stored at the cloud provider.

METHODOLOGY

This thesis aims to provide an understanding of the different attack vectors created by multi-tenancy and virtualization in a public IaaS cloud. The vectors will be explored, focusing on the threats arisen from different tenants coexisting in the same physical host. A critical analysis of the different vectors will be provided along with guidance on how to approach them. This analysis will be performed using previous works from different entities and authors, along with personal knowledge obtained from experience. As part of the aim of this research, a strong foundation will be provided on the terms of cloud computing, multi-tenancy and virtualization. All these areas will be explored giving a strong definition. The different security issues will be also explored in order to provide an introduction to the main focus of the research.

- Client will enter the data that has to be sent to the Cloud Provider.
- We are going to use file based encryption through Enhanced AES algorithm in cloud computing.
- In the first step we will make a virtual cloud for saving the files and this virtual cloud is made with the help of development tool i.e. Cloud Sim.
- Inside the cloud DataCenter, we are having the Storage as a service (SAAS) for storing the files received from the client.
- The cloud server has number of files like a1.txt, a1.mp3, a1.mdf, a1.jpg.
- Client will make a request to the cloud server for sending the file. This file will be used by the client for encrypting the data before sending it to the cloud.
- The cloud server will send any file to the client. These files are stored inside the SAAS component of the cloud provider.
- Client will read the file's data and will randomly generate the row number and column number depending upon the length of the file.
- The client will further read the data stored at particular row and column number.
- This data will be used as a key for AES encryption and decryption.
- Client applies the Shift Row Operation of AES algorithm on the key data.
- Then again apply the XOR OPERATION on the key and the original data.
- This encrypted/encoded image is then transferred to the cloud provider.
- Cloud provider will receive the file sent by the client and will store it in the storage (SAAS).

So, Using this approach, we have achieved two purposes.

- If anyone tries to hack the data while transferring from client to the gateway, he/she will get only encoded data.

- If anyone tries to perform the mining on the files stored at the cloud provider, no results will be retrieved

During Downloading the file from cloud provider, the client will follow the following steps:

1. Client will ask the cloud provider to download his/her stored file at the SAAS.

2. Cloud provider will send the stored encrypted file of that client.

3. Client will receive the encrypted file and will try to decrypt it using the same key that has already been used for encryption.

ALGORITHM

1. client registers and logins with the cloud provider.
2. Client enters the data that he/she wants to send to the cloud provider.
3. For performing the AES algorithm, client needs the key.
4. for all the files in the SAAS, choose the random file say k.
5. send the file (k) to the client.
6. Compute the length of the file
7. Client generates a random no say d.
8. Fetch the data stored at d position.
9. the key (data) is stored in the variable named m.
10. Convert the client's data and key into binary format.
11. apply the XOR operations using key (m) and client's data.
12. Repeat the step 11 till the conditions are satisfied.
13. Convert the binary format data into the string format
14. Send the string message to the cloud provider for storage.

DECRYPTION ALGORITHM

1. Client logins with the cloud provider.
2. Client sends the name of the file to be downloaded to the cloud provider.
3. Cloud provider fetches the user's file/data and sends it back to the client.
4. Client receives the encrypted file.
5. Client decryptes the encrypted file using the same key which has been used before for encryption.

EXPERIMENTAL SET UP

This section gives the details of the experiments that we have conducted during the research period. Many files of different types with different sizes have ben taken like 3KB, 9KB, 35.6KB, 50KB, 115KB, 225KB, 560KB, 1786KB, 2.3MB. Data which has been entered by the user is of different length like 15 words, 20 words, 1000 words, 5000 words .

This experiments work on a machine with the following configuration:

IntelCore i5 CPU, 3.30 GHz, 16 GB RAM, Microsoft windows 7. We have the Java version 8 with the Netbeans IDE version 8. The working system calculate the processing time,cost ,number of files splitting, block size and image decryption time to enhance between the client and the cloud provider.

ISSN 2277-3061

S.NO	Message length	Start time	Finish time	Processing time
1	16	0.1	2560.1	2560
2	22	0.1	3840.1	3840
3	44	0.1	7040.1	7040
4	98	0.1	16000.1	16000
5	236	0.1	38400.1	38400

Table 1. Readings of the Proposed work when message of different lengths has been sent to the server

Evaluation of the System

After implementing the proposed methodology, we have reached up to a solution that the cloud security can be enhanced by applying the file based encryption algorithm along with the AES. The data sent/received by the client is of utmost importance and it needs to be handled carefully. We have been able to reduce the processing time, encryption time, processing cost which increases the overall efficiency of the system.

Accuracy of the System

Accuracy of the System can is enhance by measuring Processing time, total Cost, encryption and decryption times etc as shown in the graphs below.

- **Processing Time**

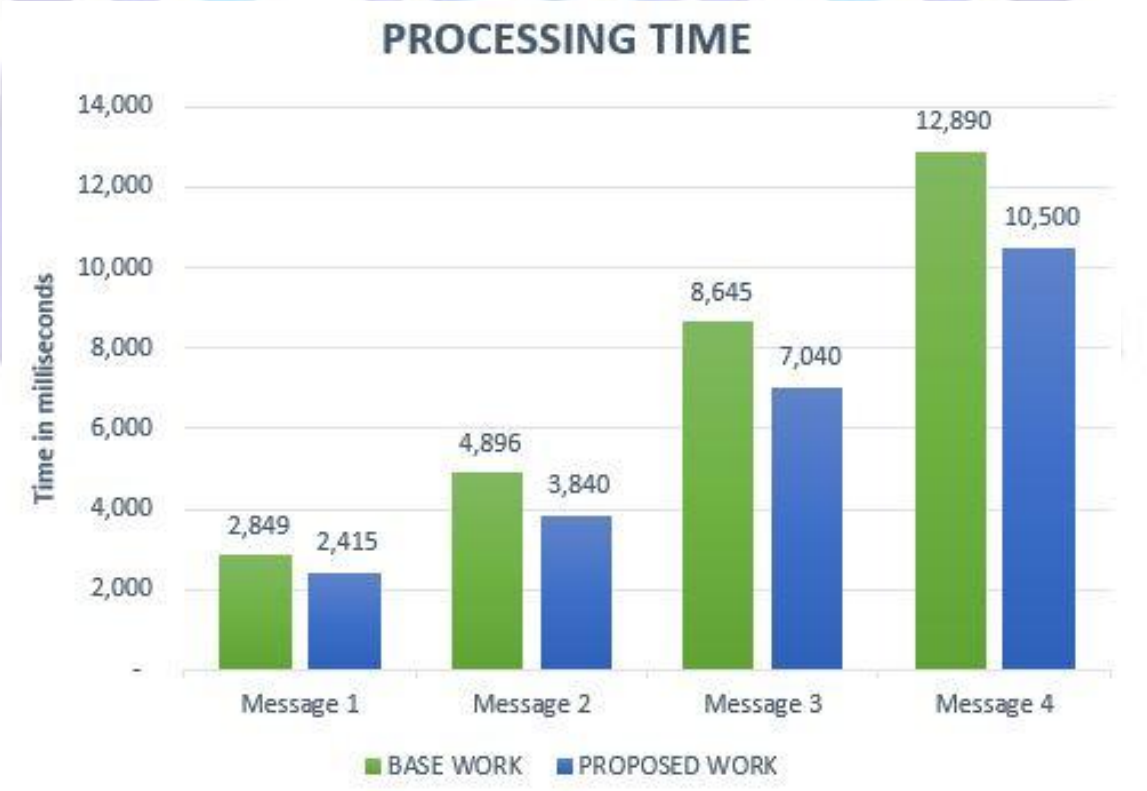

Figure 1. Processing time

It is clear from the figure 1 that the processing time of the overall proposed system has been reduced. The messages shown here are of different length as described in Table 1. Decreasing the processing time of the system was the

main objective of this research. The processing time depends upon the length of the message. As the message length increases, the processing time will also increase. But we have been able to reduce the processing time of the proposed work as it will finally increase the overall efficiency of the system.

- **Cost**

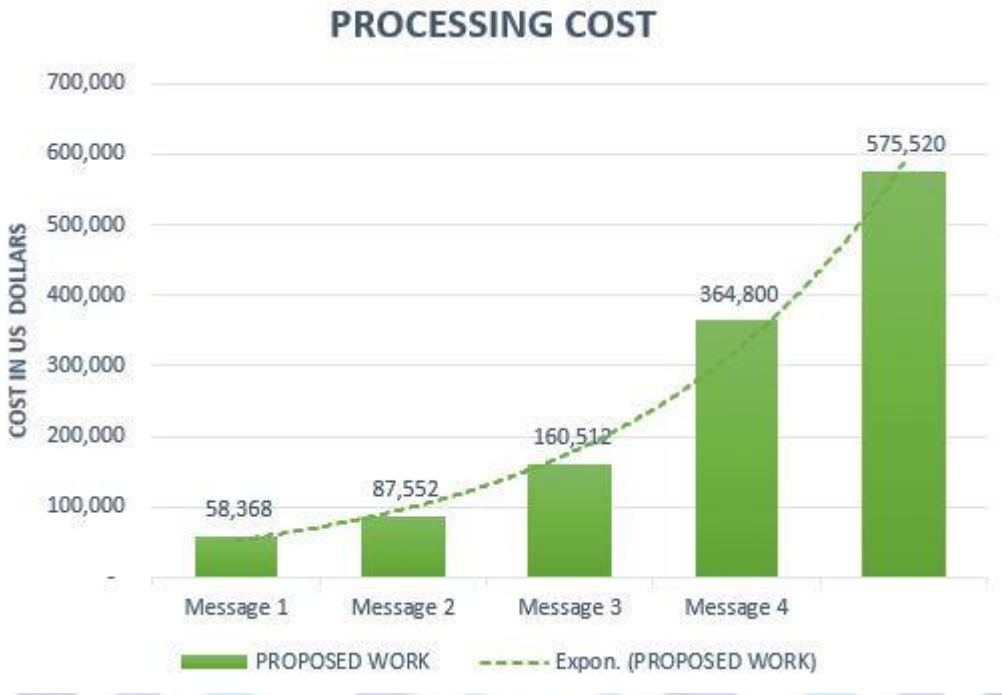

Figure 2. Message length v/s Cost

From the above bar chart (figure 2), it is clear that the cost has been reduced. Usually Cloud Computing providers have detailed costing models which are used to bill users on pay per use basis. The Cost depends upon the size of the file. As the size of the file increases, the Cost will also increase. But we have been able to reduce the Cost of the proposed work as it will finally increase the overall efficiency of the system.

Figure 3. Encryption Time

From the above bar chart (figure 3), it is clear that as the message length increases, the encryption time will also increase. The decrption time taken by the algorithm will also keep on increasing, if we increase the message length. The graph depicting the decrption times has been shown in Figure 4.

Figure 4. Decryption time of the Proposed work

CONCLUSION

Security problem is a big problem for the development of cloud computing, encryption is a central technology to ensure the cloud computing data security. Security infrastructure is required to safeguard web and cloud services. At the user level, one needs to perform trust negotiation and reputation aggregation over all users. At the application end, we need to establish security precautions in worm containment and intrusion detection against virus, worm, and distributed DoS (DDoS) attacks. We also need to deploy mechanisms to prevent online piracy and copyright violations of digital content. The primary conclusion of our research is that adoption of user-centric security models and shifting certain parts of communication and computation to the client side allows us to provide the cloud consumers with more visibility and control over their resources. Therefore, using this approach not only the security and privacy concerns of cloud consumers can be addressed more effectively, but also the burden of managing end-users' identities and access control will be reduced from cloud service providers.

This study collectively describes cloud computing security challenges in general and describes the mitigation practices that have been proposed to handle the identified challenges. We have successfully implemented the above proposed system and has reached to a solution that by using the file encryption method along with AES, we can achieve the better security in cloud computing. However, most important future work identifies here is that there are concrete standards for cloud computing security still missing. There are some open cloud manifesto standards and few efforts made by the cloud security alliance to standardize the process in the cloud. The cloud vendors and users do not encourage the usage of these standards as they are restrictive. In addition to this the cloud computing with such great offering such as storage, infrastructure and application designing capabilities on the go to the IT industry still fail to have proper standards for interoperability with other cloud service providers. This failure to provide concrete security standards, common underlying framework for data migration and global standards for cloud interoperability, make the leading technology the cloud computing" still a vulnerable option for aspiring users.

REFERENCES

[1] T. Lindeberg, Addressing cloud computing security issues , International Journal of Computer Vision, pages 117—154,1998.

[2] Buyya R, Murshed M. A review on cloud computing security issues & challenges.,Concurrency and Computation Practice and Experience 2002.

[3] L. Wang, Gregor Laszewski, Marcel Kunze, Jie Tao, “Cloud Computing: A Perspective Study”, New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008.

[4] R. Maggiani, Communication Consultant, Solari Communication, “Cloud Computing is Changing How we Communicate”, 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009.

[5] Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, Cloud Computing Types ,Architecture ,Application and Role in IT, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009.

[6] Kapil Bakshi ,Thunder in the Cloud: $6 Cloud-Based Denial-of-Service Attack, August 2009, Vol. 169, pp. 36-45, 2009.

[7]Torray Harries , Taking account of privacy when designing cloud computing services, CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE Computer Society Washington, DC, USA, May 2009.

[8] Randy Marchany, A survey of trust in computer science and the semantic web,Journal of Web Semantics: Science, Services and Agents on the World Wide Web ,2010.

[9] Yanpei Chen, Vern Paxson,Electrical Engineering and Computer Sciences University of California at Berkeleyhttp://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html January 20, 2010.

[10] Wojciech Mazurch, Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator , Future Generation Computer Systems ,2010.

[11] Dimitrious zissis , Dynamic trust enhanced security model for trusted platform based International Telecommunication Union, X-509 | ISO/IEC 9594-8, 2010.

[12] Paul Stryer, Establishing and managing trust within the public key infrastructure, Computer Communications ,2010.

[13] S.Sukashinin,V.Kavitha ,Security Issues in Cloud Computing and Countermeasures,International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[14] Alexa Huth,James Cebula, Security Attacks and Solutions in Clouds,2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2011.

[15] Lee Butlen and Richard, Understanding Data centers and Cloud Computing ,44th Hawaii International Conference on System Sciences, pp. 1–10, Koloa, Hawaii, January 2011.

[16] Peter Mell, Timothy Grance,The NIST Definition of Cloud Computing, http://docs.ismgcorp.com/files/external/Draft-SP-800- 145_cloud-definition.pdf, 2011.

[17] Thomas W. Shinder, “Security Issues in Cloud Deployment models”, TechNet Articles, Wiki,http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud deployment-models.aspx,September 2011.