ISSN 2277-3061
Volume 17 Number 1
International journal of Computers and Technology

DESIGN AND IMPLEMENTATION OF AN OTP BASED DATA SECURITY MODEL INCOPERATING AES AND SHA2 IN CLOUD ENVIRONMENT

Jaspreet Kaur [(1)], Navdeep Kaler [(2)]
[(1)] Research Scholar, Department of Computer Science & Engineering, LLRIET, Moga
jaspreetcse.dtc@gmail.com
[(2)] Assistant Professor, Department of Computer Science & Engineering, LLRIET, Moga
navdeep.kaler@gmail.com

ABSTRACT

Cloud computing has revolutionized the way computing and software services are delivered to the clients on demand. It offers users the ability to connect to computing resources and access IT managed services with a previously unknown level of ease. Thus, security concerns among users of the cloud have become a major barrier to the widespread growth of cloud computing. In this research work, we have used the 3 step security mechanism for the keeping the data secure at the cloud. We have implemented the strong authentication mechanism using AES encrypted OTP and enhanced the security of data using Cloud Broker and AES. When you log on to your machine and then try to access a resource, say a file server or database, something needs to assure that your username and password are valid. With sensitive data stored in the cloud of the different users, we need a strong authentication mechanism along with OTP. Data breaches because of no/weak authentication. Afterwards we have verified the integrity of data stored at cloud provider using SHA2. Multiple parameters like processing time, processing cost, AES encryption time, OTP generation and encryption time have been calculated and analyzed. We have been able to enhance the security by optimizing the processing time as well as processing cost. After implementing the proposed methodology, it has been summarized that the cloud security can be enhanced by applying the proposed mechanism. The proposed system has reduced the complexity, processing cost which increases the overall efficiency of the system.

KEYWORDS

Cloud Computing, Cloud Security, Security issues, OTP, AES, and Hashing

INTRODUCTION

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because it is offering lots of opportunities. Enterprises have been determined to reduce ccomputing costs and for that reason most of them started using it in IT technology then adapted virtualization technology. For the good of the enterprises it is futuristic to help them in this i.e. Cloud Computing. Cloud Computing has taken the enterprise to new level and allows them to further reduce costs through improved utilization, reduced administration and infrastructure cost and faster deployment cycles. 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 virtual machine or physical machine. The cloud is a representation 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. 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. Different researchers have stated various benefits of cloud computing due to this reason they have been adopted by enterprises more preferable. 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 termed as virtualized system and a natural evolution for data centers which offer automated systems management. Security controls in cloud computing are similar to those in traditional IT environments. However, because of the cloud service and operational models employed with the implied organizational division of responsibilities and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions. As part of the transition to cloud computing, it is critical that consumers understand their level of risk tolerance and focus on mitigating the risks that the organization cannot afford to neglect.Often it is not understood that the type of service model being offered by the provider (i.e. IaaS, PaaS or SaaS) has significant impact on the assumed "split of responsibilities" between the consumer and the provider to manage security and associated risks. For IaaS, the provider is supplying (and responsible for securing) basic IT resources such as machines, disks and networks (Buvya et al., 2002). The consumer is responsible for the operating system and the entire software stack necessary to run applications, plus the data placed into the cloud computing environment. As a result, most of the responsibility for securing the applications themselves and the data they use falls onto the consumer. In contrast, for SaaS, the infrastructure, software and data are primarily the responsibility of the provider, since the consumer has little control over any of these features of the service.

RELATED WORK

In order to assess the trend and level of research work done till date, in the area of titled work, an exhaustive literature has been reviewed. A gist of some of the most relevant research work is presented in this chapter under various classified headings. Several books and entities have covered for the last years the concept of cloud computing. It is a hot topic nowadays in the technology and business world; thus there are multiple definitions. The National Institute of Standards and Technology (NIST), provides a well-recognized description for cloud computing (Harold et al., 2009), including its characteristics, service models and deployments models. T. Lindeberg (1998) portrays the different security issues of distributed computing because

of its administration conveyance models. In any case, the hidden innovation of cloud without anyone else gives a noteworthy security hazard. Buyya R, Murshed M (2002) talk about the security and protection concerns of cloud computing and some conceivable answers for improve the security. In light of the security arrangements proposed we have concocted a secured structure for distributed computing. In today's worldwide focused business, organizations must improve and take full advantage of its assets to succeed. This obliges empowering its representatives, business accomplices, and clients with the stages and coordinated effort devices that advance development. L.Wang, Gregor Laszewski present a novel technique to hide data in the edges of the image by extending the Least Significant Bit embedding algorithm. This algorithm hides data in the edge pixels and thus ensures better security against attackers. In the Least Significant Bit embedding algorithm (LSB) and Random Least Significant Bit embedding algorithm (RLSB) an attacker can easily detect the presence of hidden image. To overcome these problems a new algorithm is proposed based on least significant bit embedding algorithm (LSB) for hiding secret messages in the edges of the image. The algorithm ELSB hides data in edge pixel. The proposed algorithm is applicable to all kinds of images and can be used in covert communication, hiding secret information like copyrights, trade secrets and chemical formulae. R. Maggiani (2009) listing out the security issues and challenges in cloud environment, the security standards and management tools which are in place and recommended the best solutions which we can rely on. Cloud computing provides scalable and efficient means to manage IT resources in organizations. The flexibility the cloud brings in has some disadvantages over privacy and security. If the providers and consumers follow the security measures discussed above cloud computing will be more secure. As and when the issues around security and privacy are elucidated cloud computing will be accepted widely. Harold C. Lin (2009) proposes an image steganography technique based on the canny edge detection algorithm. It is designed to hide secret data into a digital image within the pixels that make up the boundaries of objects detected in the image. More specifically, bits of the secret data replace the three LSBs of every color channel of the pixels detected by the canny edge detection algorithm as part of the edges in the carrier image. Kapil Bakshi (2009) discuss the strategy, architecture, and solution details that Cisco brings to the industry and governments. For the purposes of this paper, we will focus on the data center aspects of cloud computing. The intended audience for this paper includes public managers, government executives, IT decision makers, and IT professionals who are evaluating cloud computing strategy and cloud data center solutions. Torry harries (2009) aims to provide a means of understanding the model and exploring options available for complementing your technology and infrastructure needs. . The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of “grid computing”, “distributed computing”, “utility computing”, or “autonomic computing” is to broaden horizons across organizational boundaries. Resource sharing in a pure plug and play model that dramatically simplifies infrastructure planning is the promise of „cloud computing“. The two key advantages of this model are ease-of-use and cost-effectiveness.

GAP ANALYSIS

In order to avail the benefits of cloud, the security of data being transferred between the client and user must be ensured. Security is the key for the Cloud success, security in the cloud is now the main challenge of cloud computing. Until a few years ago, all the business processes of organizations were on their private infrastructure and, though it was possible to outsource services, it was usually non-critical data/applications on private infrastructures. Now with cloud computing, the story has changed. The traditional network perimeter is broken, and organizations feel they have lost control over their data. New attack vectors have appeared, and the benefit of being accessible from anywhere becomes a big threat. After studying the existing papers, it is analyzed that the existing techniques are not capable of protecting data. There are various policies issues and threats in cloud computing technology which include privacy, storage, reliability, security, capacity and more. But most important among these to concern is security and how service provider assures it to maintain. Generally cloud computing has several customers such as ordinary users and enterprises who have different motivations to move to cloud.

Various concerns after analyzing the problems in cloud Computing are: security, integrity, loss of data and third party access.

i. After studying the existing paper [22], it is analyzed that the existing techniques are not capable of protecting data in an efficient way.

ii. For the data integrity, the data can be changed in way before reaching to the server/client. There is no data verification involved.

iii. Unauthorized person can come to know about methodology.

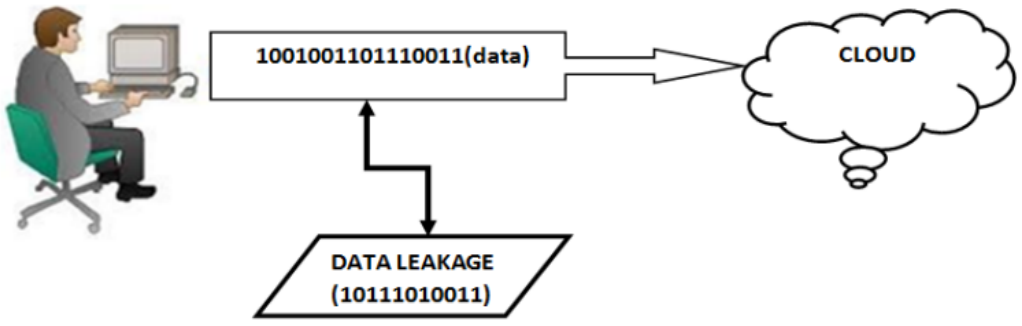

Figure 1. Man in the middle Attack.

PROBLEM FORMULATION

- **No secure authentication:** In the present work, there is no secure authentication procedure defined. When you log on to your machine and then try to access a resource, say a file server or database, something needs to assure that your username and password are valid. With sensitive data stored in the cloud of the different users, we need a strong authentication mechanism along with OTP. Data breaches because of no/weak authentication.
- **No Gateway is defined:** The user should not be directly connected to the cloud provider as there is high risk of data getting stolen or hacked by the third party intruder. There is a requirement of gateway/broker that acts as an intermediate between the cloud provider and the client.
- **Weak Encryption Mechanism:** In the present work, only one encryption algorithm is chosen i.e. AES for encryption of data at the client's end.

RESEARCH OBJECTIVES

- To implement and study the performance of existing security mechanisms in cloud environment.
- To implement the strong authentication mechanism using AES encrypted OTP (One-Time Password).
- To enhance the security of data using Cloud Broker and AES.
- To verify the integrity of data stored at cloud provider using SHA2.
- To develop the proposed algorithm and compare the performance of proposed algorithm with existing algorithm.

PROPOSED 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. The research work is divided into 3 phases:

- Phase 1: Secure Authentication.
- Phase 2: Encryption of File using AES.
- Phase 3: Decryption of file after verification.

STEPS INVOLVED IN PHASE 1

- Study of existing security mechanisms in cloud computing
- Choice of the cloud provider
- Registration of Client with the cloud provider
- Login of client into the cloud
- Generation of OTP
- Encryption of OTP using AES
- OTP verification

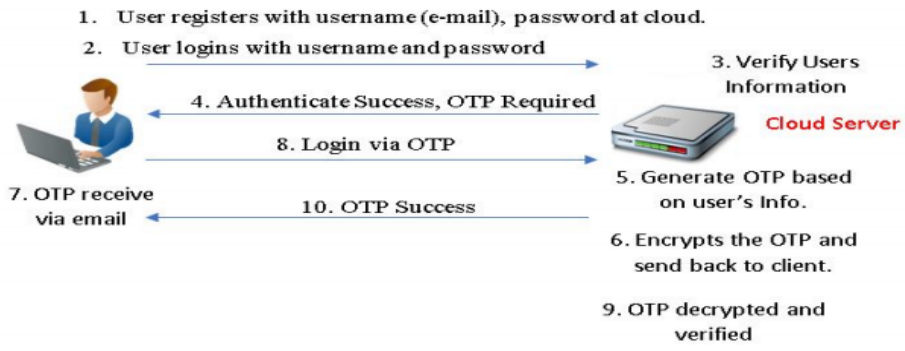

Figure 2. Secure Login using Encrypted OTP Authentication

STEPS INVOLVED IN PHASE 2

- Choice of file to be uploaded
- ii. Encryption of file using AES
- Establishing connection with the cloud gateway.
- Storage of encrypted file at the cloud provider end
- Hashing of the stored file using SHA2.
- Receiving hash key by client.

STEPS INVOLVED IN PHASE 3

- Request to be made for earlier uploaded file via cloud gateway.
- ii. Generation of new hash value of the requested file.
- Verification of the new key with the previously generated value.
- Conditional downloading of file
- Receiving of the downloaded file at the cloud gateway.
- Receipt of decrypted file by client
- AES decryption of gateway-sent encrypted file at the client end

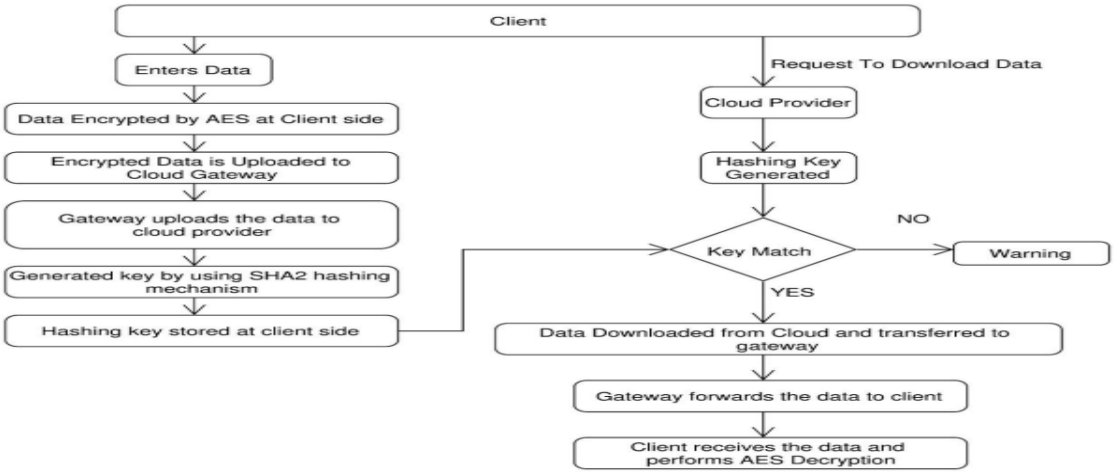

Figure 3. Flow of Work.

INTEGRATION CHECK

- Hash files will be generated in cloud server using SHA-2 algorithms.
- ii. Integrity of the data is checked using these hash values.
- If all the hash codes are matched then file is downloaded at the gateway or the broker, else file is accessed by someone.

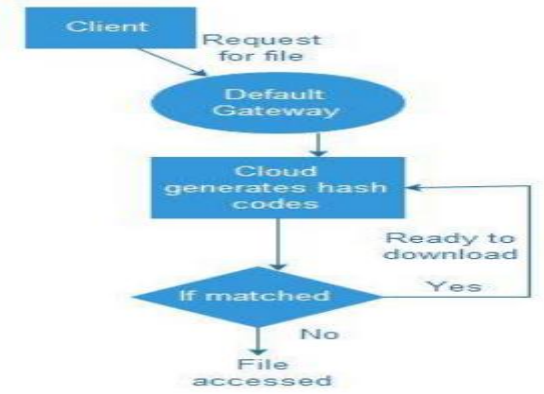

Figure 4. Integration Check

UPLOADING OF FILE AT THE CLOUD SERVER

- Client will enter the data that has to be sent to the Cloud Provider.
- The AES algorithm will be performed at the client side which will encrypt the data before sending the data to the gateway.
- This encrypted data is then transferred to the gateway.
- Gateway will receive the file sent by the client and will transfer it to the cloud provider for storage.
- Cloud provider will receive the data from the gateway
- Cloud provider will apply the SHA2 hashing algorithm on the received file and will send the generated hash key value back to the client.
- This model will prevent will the types of attacks like man in the middle attack/ data mining attack.

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 end, the client will follow the following steps:

- Client will ask the gateway to download his/her stored file.
- Gateway will forward the request to the cloud provider and cloud provider will generate the hash value of the stored file using SHA2. This generated value is compared with the client's original key value. If the values have been matched, then the encrypted file is sent back to the gateway, else the warnings will be displayed to the user that file has been accessed by someone.
- Gateway will receive all the encrypted file and will send the file to the client.
- Client will further perform the AES decryption to fetch the original data.

ALGORITHM

In the proposed work we will enhance the security of data using hybrid technique of AES and SHA2 in cloud computing, which protect the data from man in the middle attack .so that the private information can be sent from the client end to the cloud end and can be retrieved securely.

- Client registers and logins with the cloud provider.
- Cloud provider will generate the OTP and will encrypt it using AES.
- The encrypted OTP is sent to client's registered email address.
- After OTP verification, the client will choose the data to be sent to the cloud provider.
- For all the data in the dataset, apply the AES encryption technique at the client side.
- Client sends the encrypted data to the available gateway.
- Gateway receives the encrypted data and forwards it to the cloud provider.
- Cloud provider receives the file generates the hash value using SHA2 and sends it to the client.

ALGORITHMS USED

Security is the key for the Cloud success, security in the cloud is now the main challenge of cloud computing. There are techniques which are used to enhance the cloud computing security i.e. AES and SHA2.

AES

The Advanced Encryption Standard (AES), also known as Rijndael (Keiko et al., 2012) (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first publicly accessible and open vague cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The number of cycles of repetition is as follows:

10 cycles of repetition for 128-bit keys.

12 cycles of repetition for 192-bit keys.

14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

SHA2

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with. A key aspect of cryptographic hash functions is their collision resistance: nobody should be able to find two different input values that result in the same hash output. SHA-2 includes significant changes from its predecessor, SHA-1.

SIMULATION VIEW OF PROPOSED WORK

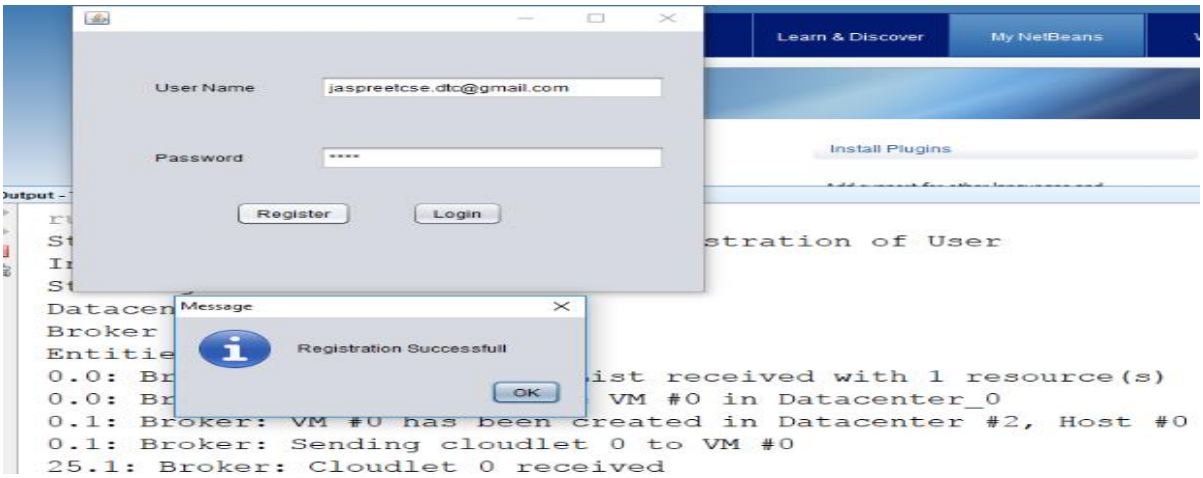

Figure 5. Registration at the cloud provider.

The above figure 5 demonstrates the registration of the user at the cloud provider. The user will enter his/her id and password and will get himself/herself registered at the cloud end. Once the user has been registration, the system will automatically navigation to the login section. On submitting the Login button, the request will go to the cloud provider that will check whether the user's entered data is valid or invalid. After the Login Section is completed, the system will generate the one time password by using the MD5 algorithm and will encrypt the OTP using AES encryption algorithm. The encrypted OTP is sent to the user's registered email ID at the cloud provider.

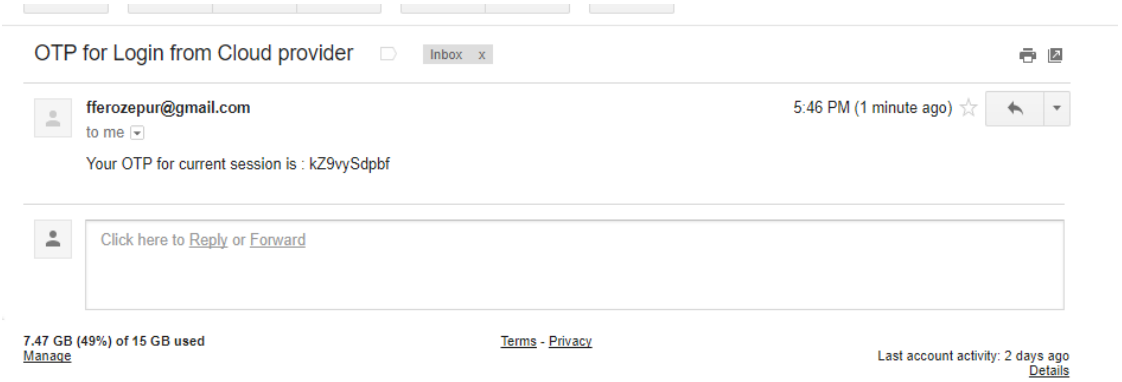

Figure 6. OTP received via e-mail

After OTP verification, the user will enter into the main page where he/she can upload the file to the cloud provider or can download the previously uploaded files from the cloud server. This section will only open when the user's credentials are properly verified by the cloud provider.

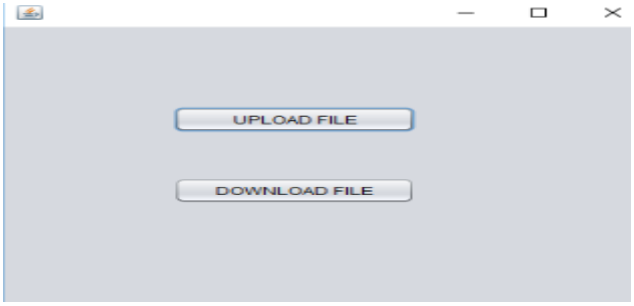

Figure 7. Main Sections after Login Process

User will choose the file from his/her laptop when he/she clicks on the file upload button. This file will be encrypted at the client side using AES. After encryption process is completed, the encrypted data is sent to the gateway.

EXPERIMENTAL RESULTS

After analyzing the loophole of base security of the data between the client and the cloud provider is enhanced by using the AES and verification mechanism at the cloud provider. This experiments work on a machine with the following configuration: Intel Core 2 CPU, 980 MHz, 1.99 GB RAM, Microsoft windows 7. We have the Java version 8 with the Net beans IDE version 8.

Table 1. Readings of the Base work

S.NO.	FILE TYPE	FILE SIZE	PROCESSING TIME (MILLISECONDS)	PROCESSING COST (RUPEES)	AES ENCRYPTION TIME (MILLISECOND)
1	PHP	26bytes	44.1	134.244	1.01236
2	VB	74bytes	110.1	335.6	1.034521
3	HTML	116bytes	176.1	536.976	1.067
4	MP3	162bytes	242.1	738.342	1.12734
5	CDR	221bytes	306.1	933.6	1.138023
6	JS	328bytes	458.1	1397.358	1.339389
7	PSL	383bytes	524.1	1598.724	1.537704
8	JAVA	495bytes	680.1	2074.68	1.638387
9	FLV	533bytes	746.1	2276.046	1.73907
10	PDF	635bytes	878.1	2678.778	2.172312
11	HTML	722bytes	1008	3075.408	2.571993
12	TXT	777bytes	1074.1	3276.774	2.7031855
13	JSP	828bytes	1140	3478.14	3.2432125
14	ASPX	1.00KB	1424	4344.624	5.04635
15	VLC	1.18KB	1686	5143.986	8.014975
16	JAR	1.25KB	1772	5406.372	11.722665
17	MSI	1.50KB	2126	6486.42	12.02995
18	XML	2.34KB	3308.1	10092.7	12.640743
19	MP4	3.74KB	5254.1	16029.95	13.166055
20	MKV	5.93KB	8340	25445.33	13.978255
21	ASD	7.49KB	10508	32059.9079	14.036395
22	HIB	10.01KB	14186	43281.486	15.12856
23	CLASS	15.04KB	21610	65932.11	15.36586
24	ISD	20.00KB	26010	79356.51	16
25	DOCS	23.3KB	32800	100072.79	16

Table 2. Readings of the proposed work

S.NO	FILE NAME	FILE SIZE	PROCESSING TIME	PROCESSING COST	OTP GENERATION AND ENCRYPTION TIME	AES ENCRYPTION TIME	SHA2 GENERATION TIME
1	PHP	26bytes	22.05	67.122	725	1.01	14
2	VB	74bytes	55.05	167.8	922	1.03	16
3	HTML	116bytes	88.05	268.485	750	1.07	15
4	MP3	162bytes	121	369.171	853	1.13	16
5	CDR	221bytes	153	466.8025	781	1.14	16
6	JS	328bytes	229	698.679	735	1.34	14
7	PSL	383bytes	127.05	799.362	781	1.54	15
8	JAVA	495bytes	340	1037.34	719	1.64	16
9	FLV	533bytes	373.05	1138.023	930	1.74	15
10	PDF	635bytes	439	1339.389	734	2.17	15
11	HTML	722bytes	504	1537.704	828	2.57	16
12	TXT	777bytes	537	1638.387	781	2.70	15
13	JSP	828bytes	570	1739.07	922	3.24	16
14	ASPX	1.00KB	712	2172.312	766	5.05	16
15	VLC	1.18KB	843	2571.993	750	8.01	15
16	JAR	1.25KB	886	2703.1855	812	11.72	16
17	MSI	1.50KB	1063	3243.2125	750	12.03	16
18	XML	2.34KB	1654	5046.35	731	12.64	16
19	MP4	3.74KB	2627	8014.975	766	13.17	16
20	MKV	5.93KB	4170	12722.665	734	13.98	15
21	ASD	7.49KB	5254	16029.95	813	14.04	14
22	HIB	10.01KB	7093	21640.743	766	15.13	15
23	CLASS	15.04KB	10805	32966.055	828	15.37	15
24	ISD	20.00KB	13005	39678.255	781	16.00	15
25	DOCS	23.3KB	16400	50036.395	797	16	15

PERFORMANCE METRICS

After implementing the proposed methodology, we have reached up to a solution that the cloud security can be enhanced by applying the model of AES, secure authentication with OTP and data verification using SHA2. 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 and cost as shown in the graphs below, which increases the overall efficiency of the system.

- **Processing Time**

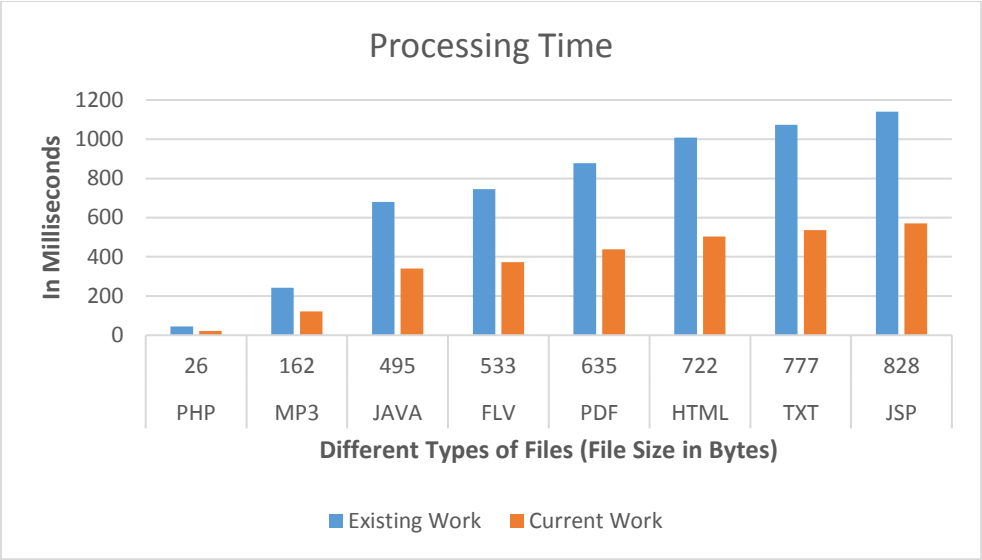

Figure 8. Processing time.

From the above bar chart, it is clear that the processing time has been reduced. The processing time depends upon the size of the file. As the size of the file 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**

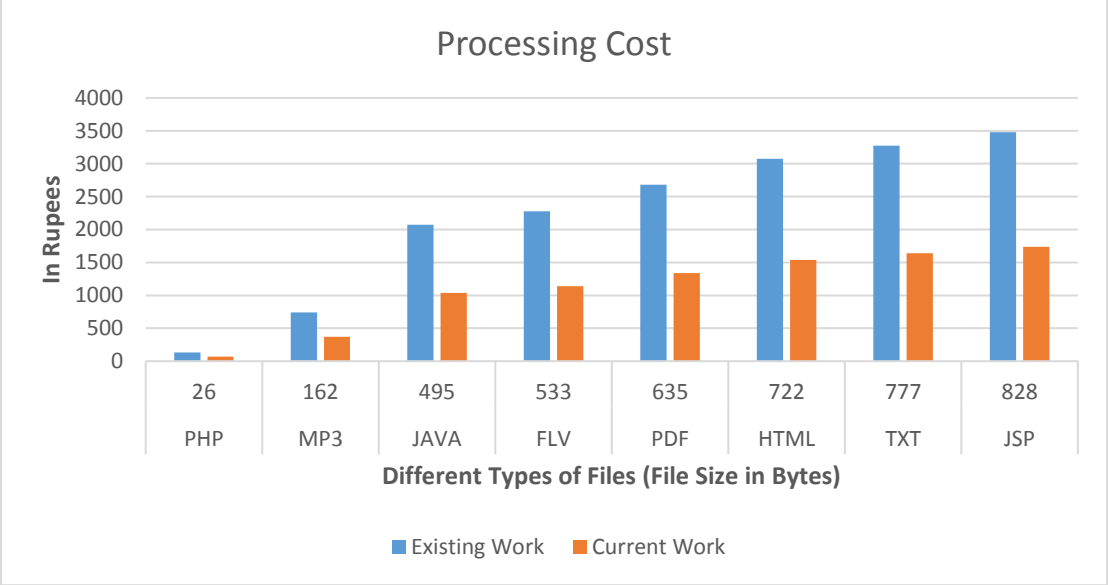

Figure 9. File Size v/s Cost.

From the above bar chart, 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 increase.

OTP GENERATION AND ENCRYPTION USING AES

For the secure authentication, we have generated the one time password via MD5 algorithm and is encrypted using AES and is sent to the client's registered email id. From the below graph, it is clear that by implementing the OTP mechanism, there is no effect on the system. From the number of experiments it is clear that OTP generation and encryption is taking lesser than 1 second

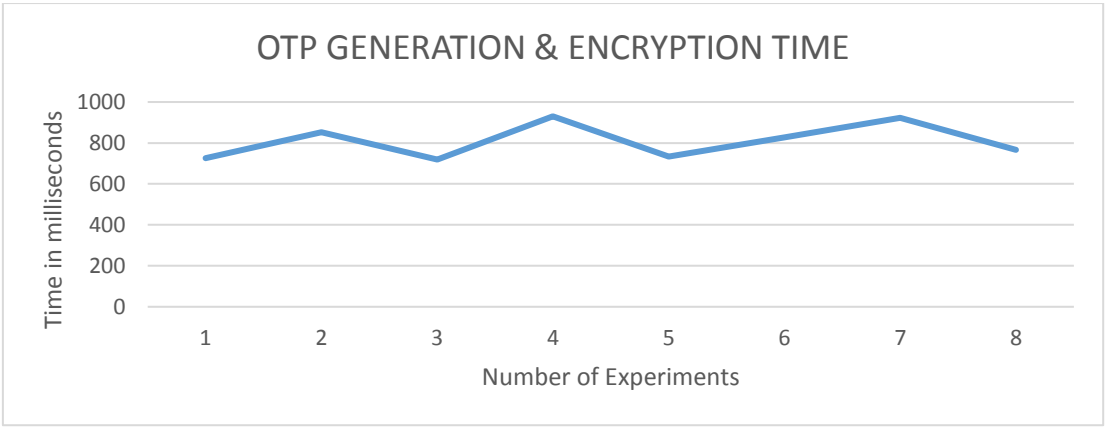

Figure 10. OTP generation and encryption time.

From the below line chart, it is clear that as the size of the file keeps on increasing, the encryption time will keep on increasing. We have taken different types of files of different sizes for testing purposes.

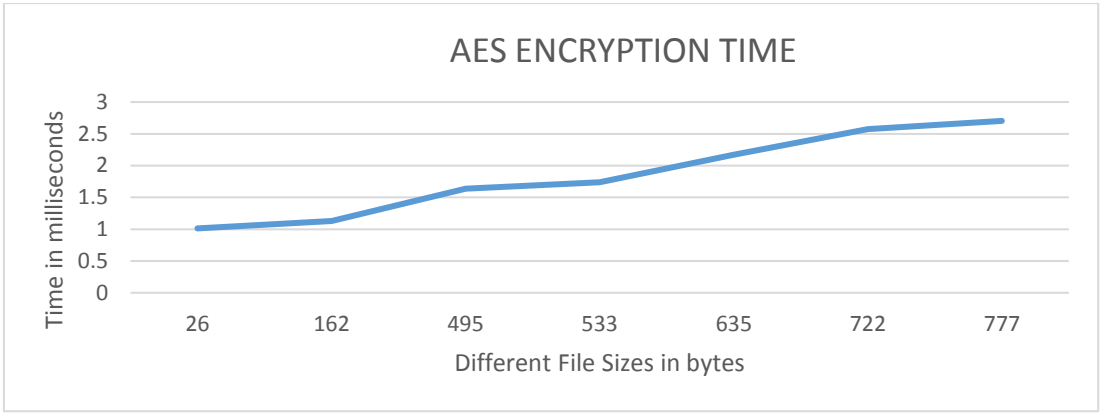

Figure 11. AES Encryption Time.

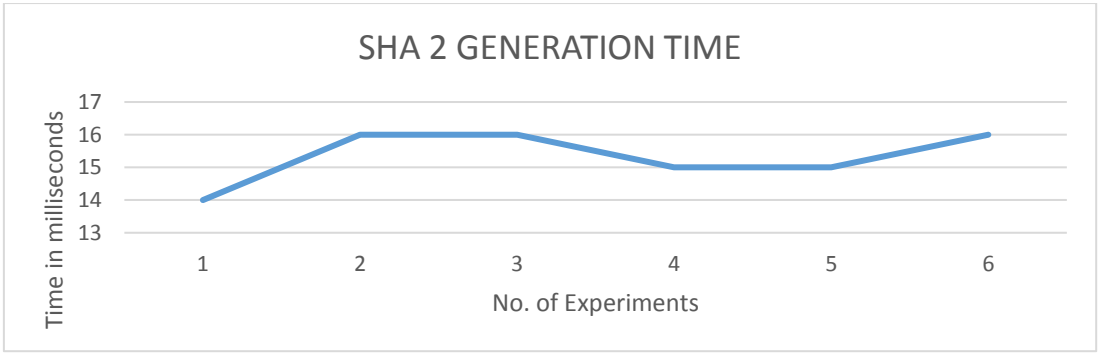

Figure 12. SHA2 Generation Time.

For the secure verification before downloading, we have included the SH2 verification mechanism that will match the newly generated key with the previously stored key. The above figure shows the key generation time using SHA2. From the graph it is clear that the SHA 2 generation is not taking much time and is not having any extra overhead on the entire performance of the system.

CONCLUSION

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 have reached to a solution that by using this proposed mechanism, we can achieve the better security in cloud computing more efficiently.

REFERENCES

[1] Mohis M and Devipriya V S, "An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique," IEEE, pp. 1-5, 2016.

[2] Kunal V. Raipurkar and Anil V. Deorankar , "Improve Data Security in Cloud Environment by using LDAP and Two Way Encryption Algorithm," IEEE, pp. 1-4, 2016.

[3] V.Swath, K.Sudha, R.Aruna, C.Sangeetha and R.Janani, "Providing Advanced Security Mechanism for Scalable Data Sharing In Cloud Storage," IEEE, pp. 1-6, 2016.

[4] Shivangi Sengar and Rajesh Kumar Chakrawarti, "Implementation of PDS System with Improved Security and Transparency under Cloud Environment," IEEE, pp. 1-6, 2016.

[5] Mohis M and Devipriya V S, "An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique," IEEE, 2016.

[6] S. Pandey , A. Dwivedi , J. Pant and M. Lohani , "Security Enforcement using TRBAC in Cloud Computing," IEEE, pp. 1232-1238, 2016.

[7] R.K.Shyamasundar, N.V.Narendra Kumar and Muttukrishnan Rajarajan, "Information-Flow Control for Building Security and Privacy Preserving Hybrid Clouds," IEEE, pp. 1410-1417, 2016.

[8] P. More and D G Harkut, "Cloud Data Security using Attribute-based Key Aggregate Cryptosystem," *IEEE,* pp. 855-861, 2016.

[9] D. Singh and Harsh K Verma, "A New Framework for Cloud Storage Confidentiality to Ensure Information Security," *IEEE,* 2016.

[10] Kunal V. Raipurkar and Anil V. Deorankar , "Improve Data Security in Cloud Environment by using LDAP and Two Way Encryption Algorithm," *IEEE,* 2016.

[11] S. Sengar and . R. K. Chakrawarti , "Implementation of PDS System with Improved Security and Transparency under Cloud Environment," *IEEE,* 2016.

[12] A. Albugmi, M. O. Alassafi , . R. Walters and Gary Wills, "Data Security in Cloud Computing," *IEEE,* pp. 55-59, 2016.

[13] A. Singh and M. Malhotra , "Hybrid Two-Tier Framework for Improved Security in Cloud Environment," *IEEE,* pp. 955-960, 2016.

[14] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu and Tie Qiu, "An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing," *IEEE,* pp. 1-13, 2016.

[15] Mrinal Kanti Sarkar and S. Kumar, "A Framework to Ensure Data Storage Security in Cloud Computing," *IEEE,* 2016.

[16] N.Thillaiarasu and ChenthurPandian.S, "Enforcing Security and Privacy over Multi – Cloud Framework Using Assessment Techniques," *IEEE,* 2016.

[17] R. R. Gupta, G. Mishra, S. Katara, A. Agarwal, M. K. Sarkar, R. Das and S. Kumar, "Data Storage Security in Cloud Computing Using Container Clustering," *IEEE,* 2016.

[18] S.Petcy Carolin and M.Somasundaram, "Data Loss Protection And Data Security Using Agents For Cloud Environment," *IEEE,* pp. 1-5, 2016.

[19] T. Mavroeidakos, A. Michalas and Dimitrios D. Vergados , "Security Architecture based on Defense in Depth for Cloud Computing Environment," *IEEE,* 2016.

[20] Deepak H. Sharma, C A. Dhote and Manish M. Potey, "Intelligent Transparent Encryption-Decryption as Security-as-a-Service from Clouds," *IEEE,* pp. 359-362, 2016.

[21] Deepak H. Sharma, C A. Dhote and Manish M. Potey, "Implementing Intrusion Management as Securityas-a-Service from Cloud," *IEEE,* pp. 363-366, 2016.

[22] K. V. Raipurkar and A. V. Deorankar, "Improve Data Security in Cloud Environment by using LDAP and Two Way Encryption Algorithm," Symposium on Colossal Data Analysis and Networking (CDAN), IEEE, 2016.