A Novel Framework for Cloud Security against Data Breach

Arpit Gupta
Department of CSE
Medi-Caps Institute of Technology & Management,
Indore, India

Vaishali Chourey
Associate Prof., Department of CSE
Medi-Caps Institute of Technology & Management,
Indore, India

ABSTRACT
Cloud computing is the most emerging technology now-a-days. Every internet user accessing cloud services either directly or indirectly without knowing or aware of security aspects because of trust between the user and the cloud service provider. But, this trust is harmed by the malicious user or hacker by breaching the data, data theft & data loss by using various mechanisms. In this research paper we proposed a architecture which provide protection to the cloud environment and controls Data Breach and Data Loss. In this research paper we also explore the deficiencies in the current cloud threat control strategies. No single mechanism can solve the serious cloud security problem. So, use of many traditional and technical strategies provide the secure cloud computing environment.

Keywords- Cloud Computing, Cloud security threats

1. INTRODUCTION
According to NIST[1] (National Institute of Standard & Technology) Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources such as (networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing is a new computing model which comes from grid computing, parallel computing, distributed computing, utility computing, virtualization technology and other computing technologies.

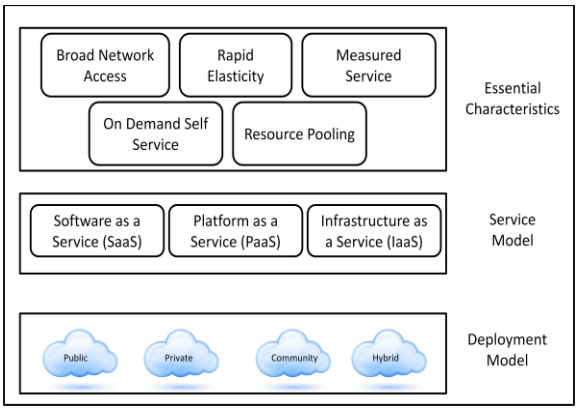

Figure 1. NIST Visual Model of Cloud Computing Definition

NIST [1], defines cloud computing by describing five essential characteristics, three cloud service model and four deployment model as shown in Figure 1.
Cloud service provider should ensure the security of client's data. A cloud service provider offers various services such as location independence, scalability, pay for use, data storage, backup and recovery, on demand services and protection against hackers. The extensive use of virtualization technology is implementing on the cloud may rise the security concern for the customers of a public cloud. Security and privacy of data is the key problem in the cloud environment.

2. CLOUD SECURITY THREATS
Cloud Security Alliance conducted a survey of industry experts to identify the greatest threat in the cloud computing environment. According to Notorious nine Cloud Computing Top Threats 2013 ,[2] the top cloud threats are ranked in order of severity as

- **Data Breach** A data breach is an intentional or unintentional release of secure information to an untrusted environment i.e. disclosure of information, data leak and data spill .

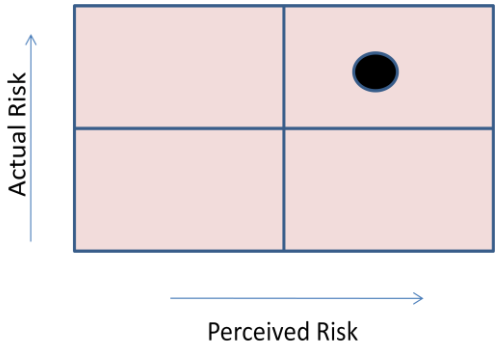

Figure 2.Risk Matrix by Cloud Security Alliance 2013

A risk matrix is shown in the figure 2 by the Cloud Security Alliance 2013.A survey by CSA in 2013 and observe the severity of Data Breach threat.

- **Data Loss** Compromised data may include. Data may be loss due to deleted or altered data without first making backup ,loss of encoding key and unauthorized access of sensitive data.
- **Account Hijacking** Account or Service Hijacking is usually carried out with stolen creditals. It includes phishing, fraud and exploitation of software vulnerabilities .

3. MAJOR CLOUD INCIDENTS IN RECENT YEARS

- In 2009,the major cloud computing service provider Amazon's Simple Storage Service was interrupted twice in February and July 2009.This accident resulted some networks sites relying on a single storage services were forced to a standstill.
- In March 2009,Google docs even led to serious leakage of user private information.
- Google Gmail also appeared a global failure up to 4 hours.
- Microsoft's Azure cloud computing platform also took place a serious accident for 21 hours.
- In April 2011, Sony experienced a data breach within their PlayStation Network. It is estimated that the information of 77 million users was compromised.
- In October 2013, Adobe Systems revealed that their corporate data base was hacked and some 130 million user records were stolen.
- In October 2013,US Federal Bureau Investigate new threat i.e. Crypto-Locker which encrypt victim's document and demands payment in return of decryption key.

4. PROBLEM STATEMENT

Many of the organizations and enterprises store their data at any physical location outside their own control in cloud environment. This storage of data at unknown physical location get face the question of privacy, confidentiality, integrity & authenticity of the data. It also demands a trusted computing system where data confidentiality is maintained. This lead to several research based on privacy & security**.**

5. RELATED WORK

The data stored in the cloud system can meet the problem of stolen and modified unauthentic ally. The data is encrypted before stored in the cloud system but if the size of the data is large then its time complexity for the encryption degrades the performance. Many authors proposes symmetric and asymmetric key encryption model in order to achieve confidentiality, authentication, validation, integration & non-repudiation such as-

As per Xufei Zheng, Yonghui Fang [3],In this research paper the author proposes a cloud security model for malware detection as in the cloud service instead of local based antivirus software. They proposed a model called "Artificial Immune System or AIS model". In this model they combine local-host based detector in the host agent and multiple detection engines in the cloud. They can monitor the whole cloud system from the incoming threats from the outside world.

V.Nirmala et.al [4],Cloud system consists two kinds of data i.e. stagnant data and the vibrant data. Stagnant data is static in nature while vibrant is dynamic which is changed periodically. The stagnant data can be stored securely using encryption techniques but the problem with the vibrant data .The author proposed a model combines the encryption mechanisms along with the data integrity check mechanisms which provide the data confidentiality, integrity and verification using the authenticator scheme in the cloud environment.

Arjun Kumar et.al [5],The author proposed a model in order to control data breach, data loss and account hijacking threats by using the ECC model i.e. Elliptic Curve Cryptography which is more efficient mechanisms as compare to RSA Algorithm .Using ECC all the data is in encrypted form by using the ECC public key & ECC private key through which they provide high level of security of data stored in the cloud system and it uses smaller key size.

Chandramohan.D. et.al [6],In order to provide the high security in cloud environment the author proposes a new framework which prevents the confidential information by multiple encryption of onion and garlic privacy preserving layered approach i.e. OPPA & GPPA .An Onion privacy preserving approach performed the multiple encryption using public key cryptography in order to achieve the data privacy, data breach & data loss.

Uma Somani et.al [7],The authors proposed a framework for the data security. They make use of digital signature with RSA Algorithm to encrypt the data while transferring to the network through which authentication and data security is achieved.

Rashmi M.Jogdand et.al [8], The use of cloud computing has increased rapidly in many organizations. Cloud computing has been envisioned as the next generation architecture of IT Industries. Security is the major issues in the cloud environment. The author focus on the data integrity with public verifiability and availability. The author proposed an elegant verification with access right scheme for seamless integration. In this model the author tries to achieve public verifiability by manipulating the classic Merkle Hash Tree and moving towards multi cloud and for data availability author adopting Depsky system model for multi cloud environment.

Pachipala Yellamma et.al [9]The authors proposed a method for providing data storage and security in the cloud system by using public key cryptosystem RSA. But, this method is not fruitful to provide all-round protection in the cloud environment.

Nandita Sengupta et.al[10],To secure the cloud environment the author proposed a hybrid cryptography system i.e. HVCCE (Hybrid Vigenere Caesar Cipher) which prevents the cloud environment in three places i.e. client end, network & server. It consists three phases of encryption .In the first phase Caesar cipher is applied on the plain text .In the second phase according to vigenere square value, vigenere cipher is applied along with the keyword on the encrypted text achieved from the first phase. In the third phase according to vigenere square value, vigenere cipher is applied with the reverse word of keyword considered in the second phase. This encryption is applied on the encrypted text achieved from second phase.

Mehdi Hojabri et.al [11], The author focuses on the security of cloud server. Author makes use of Kerberos authentication service in order to provide trusted ,on demand quality of service and high security. In this model each user for gain the cloud server must be register and authenticated by third party. After added the requirements information in to the database it can get some qualification. After getting the qualification it should refer to Kerberos authentication service. Each client register in the third party it should send the request access for a ticket granting ticket on behalf of it's user ID to the authentication server and ticket granting server. Ticket granting server gives response a block encryption using

encryption key. Then, the client request for a source granting ticket .TGS decrypts the incoming ticket and verifies the success of decryption by presence of its ID's then user access the services.

Prashant Rewagad et.al [12],The author concentrates the major security threats i.e. data breach, privacy ,confidentiality. In order to achieve these they use a "three way mechanisms" in which the author uses digital signature and Diffie Hellmann key to protect the confidentiality in the cloud system and for the encryption/decryption purpose author used Advanced Encryption System. So, the data security, confidentiality and authentication is achieved.

6. PROPOSED FRAMEWORK

We proposed a new architecture in which we are using a Tri-Mechanism where authentication, data security & validation is achieved at the same time. Firstly we use Elliptic curve Diffie Hellman model to generate keys for the key exchange step. Then, the digital signature is used for the authentication of client. Thereafter Secure Hash Algorithm-I is used in order to encrypt or decrypt user's data file. This tri-mechanism provide all-round protection to the cloud environment and consists all characteristics of a trusted computing system. In order to avoid data modification, data breach, data loss at the server end ,we are using two separate server, one for encryption process known as trusted computing platform and another known as storage server for storing the user data file.

7. IMPLEMENTATION

For the analysis and implementation of proposed framework we deploy our project on CloudBees.

7.1 Base Approach 1: ECDH – Elliptic Curve Diffie-Hellman

Fei Sun et.al[14],ECDH is a relatively new key agreement algorithm based on Diffie-Hellman but using the elliptic-curve cryptography. Elliptic key operates on smaller key size. A 160-bit key in ECC is considered to be as secured as a 1024 bit key in Diffie-Hellman.

For generating a shared secret between A and B using ECDH, both have to agree up on Elliptic Curve domain parameters - certain public constants that are shared between parties involved in secured and trusted ECC communication. This includes curve parameter a, b, a generator point G in the chosen curve, the modulus p, order of the curve n and the cofactor h. There are several standard domain parameters defined by SEC, Standards for Efficient Cryptography [30] .

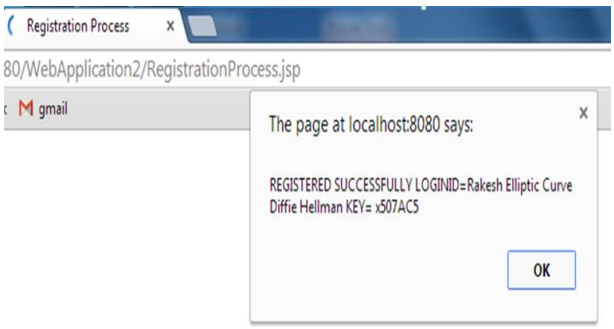

Figure 3.Elliptic Curve Diffie Hellman Key Generated & sent to the user email & mobile number

In the Figure 3 Elliptic Curve Diffie Hellman key generate by the model in order to secure the login password for the user and secure key exchange between user and server.

7.2 Base Approach 2: Digital Signature Algorithm

Sung-Ming Yen et.al[15], A digital signature scheme is a method by which the signer can sign an electronic document for the receiver (or the verifier) to keep as an evidence that the document was indeed sent originally from the signer. The National Institute of Standards and Technology (NIST) has proposed the Digital Signature Algorithm (DSA) as the public standard for digital signature.

Figure 4. Digital Signature generation

Figure 5. Digital Signature verification.

In figure 4 Digital signature is generated by the server after the valid signature input by the user then the authentication takes place and decrypt the required file and download at the client end. In figure 5. After the verification of digital signature clients file decrypted and downloaded to the client end.

7.3 Base Approach 3:Secure Hash Algorithm I

Dai Zibin et.al[16],The Secure Hash Algonthm (SHA) was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard PIPS PUB 180) in 1993, a revised version was issued as FTPS PUB 180-1 in 1995 and is generally referred to as SHA-1 .The algorithm takes as input a message

with a maximum length of less than 264 hits and produces as output a 160-hits message digest. . The input is processed in 512-bits blocks. The algorithm processing includes the following steps:

1) The algorithm starts off by initializing the five sub-registers of the first 160-bit register X labeled H_0, H_1, H_2, H_3, H_4 as follows:

H_0=67452301; H_1=EFCDAB89; H_2=98BADCFE; H_3=10325476; H_4=C3D2E1F0;

2) From here onwards, SHA-1 iterates through each of the 512-bit message blocks viz. m_0, m_1, m_2, … , m_{n-1}. For each of the message block, do the following:

a. Write m_j as a sequence of sixteen 32-bit words,

$m_j = W_0 \| W_1 \| W_2 \| \dots \| W_{15}$

b. Compute the remaining sixty four 2-bit words as follows:

- $W_t = (W_{t-3}$ xor W_{t-8} xor W_{t-14} xor $W_{t-16})$
- Cyclic shift of W_t by 1 i.e. $S^1(W_t)$

c. Copy the first 160 bit register into the second register as follows:

A= H_0; B= H_1; C=H_2; D=H_3;

E= H_4;

d. This step involves a sequence of four rounds, corresponding to four intervals 0<=t<=19, 20<=t<=39, 40<=t<=59, 60<=t<=79. Each round takes as input the current value of register X and the blocks W_t for that interval and operates upon them for 20 iterations as follows:

- For t = 0 to 79,
  - $T=S^5(A)+f_t(B,C,D)+E+W_t+K_t$
  - E=D;D=C; C= S^{30}(B);
  - B=A; A=T

e. Once all four rounds of operations are completed, the second 160-bit register (A, B, C, D, E) is added to the first 160-bit register (H_0, H_1, H_2, H_3, H_4) as follows:

- $H_0 = H_0 + A$;
- $H_1 = H_1 + B$;
- $H_2 = H_2 + C$;
- $H_3 = H_3 + D$;
- $H_4 = H_4 + E$;

3) Once the algorithm has processed all of the 512-bit blocks, the final output of X becomes the 160-bit message digest.

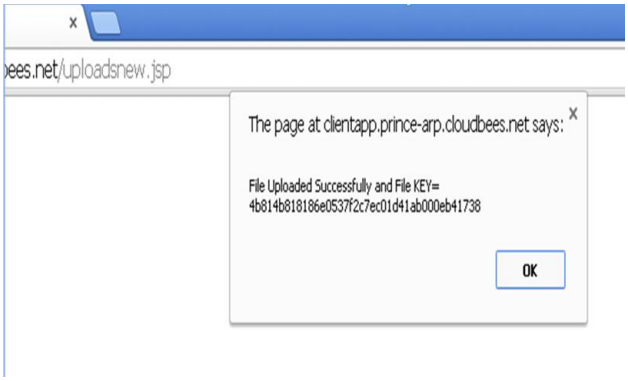

Figure 6.File Encrypted using the Secure Hash Key

In Figure 6 The file which is uploaded by the client is encrypted using Secure Hash Algorithm and the hash code generated as shown in above figure.

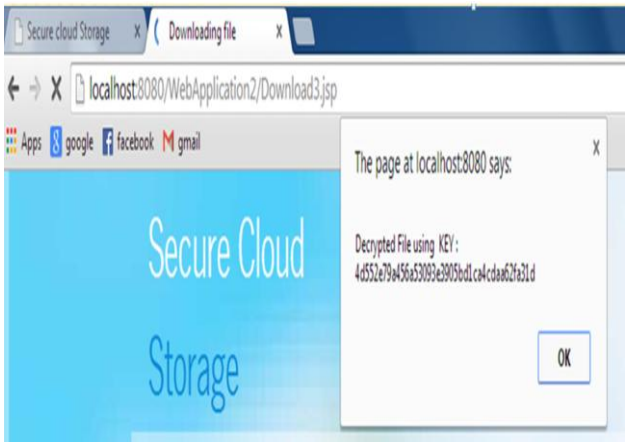

Figure 7.File Decrypted using the Secure Hash Key

After the verification of Digital signature the required file is decrypted using the key and algorithm as shown in Figure 7

8. EXPERIMENTED RESULT

8.1 Mathematical Analysis

For the analysis of performance and amount of time consumed by the proposed and the existing algorithms for the cryptographic operations perform to secure the data on the cloud server. For the mathematical analysis we compare the both existing methods to secure the cloud content with our proposed model i.e. the amount of encryption time, decryption time, key size, key storage memory size, key for encryption and decryption and finally a graph is plotted between existing and proposed architecture.

It consists the following steps as

Step 1: Select a file to analyze the existing and proposed model

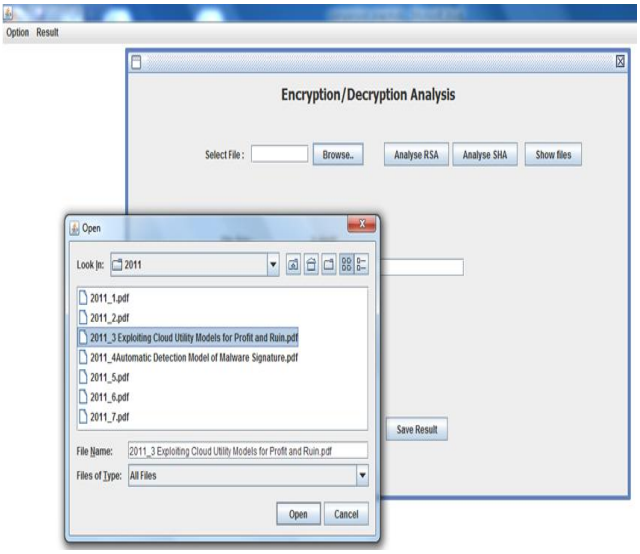

Figure 8 File selections for performing operations

Step 2: Analyze the existing algorithms Encryption/Decryption Time

Figure 9 Cryptographic operations perform on existing model

Step 3: Analyze the proposed algorithm Encryption/Decryption Time

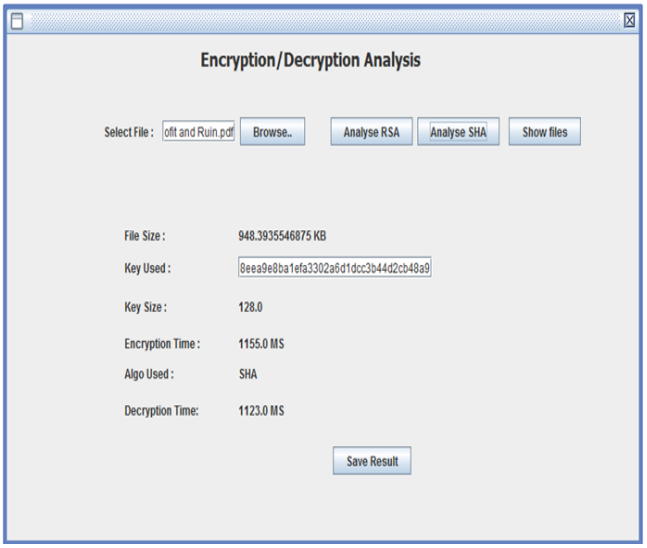

Figure 10 Cryptographic operations perform on proposed model

Step 4 : Save the result after Analysis

Step 5: Comparison between Existing and Proposed algorithms

File Size	Encryption Time (in ms)		Decryption Time (in ms)	
	Existing Approach	Proposed Approach	Existing Approach	Proposed Approach
20	1032	885	485	290
40	1385	957	780	570
60	1496	1092	862	613
80	1876	1300	995	718

Table 1. Comparison between existing and proposed model

In the Table 1. it is clearly identified that the key size of existing model is large, encryption and decryption time is also high as compare to our proposed model.

8.2 Graphical Analysis

For Graphical analysis, Graphs plot between parameter for existing and proposed model as

1. Encryption Time in (ms) for both existing and proposed model.
2. Decryption Time in (ms) for both existing and proposed model.
3. Key size for both existing and proposed model.

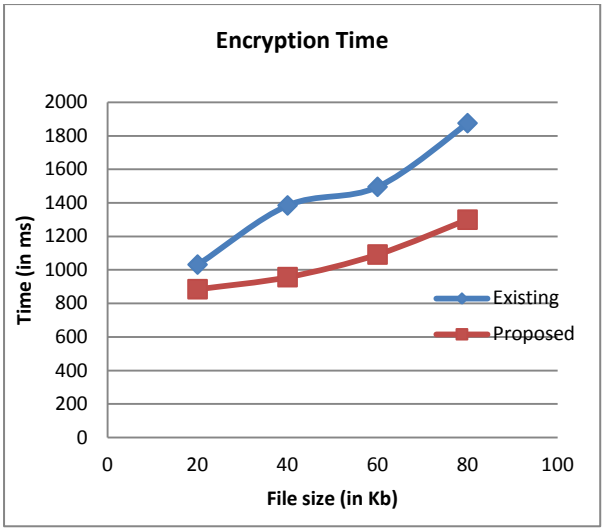

Figure 11 Encryption Time in (ms) for both existing and proposed model

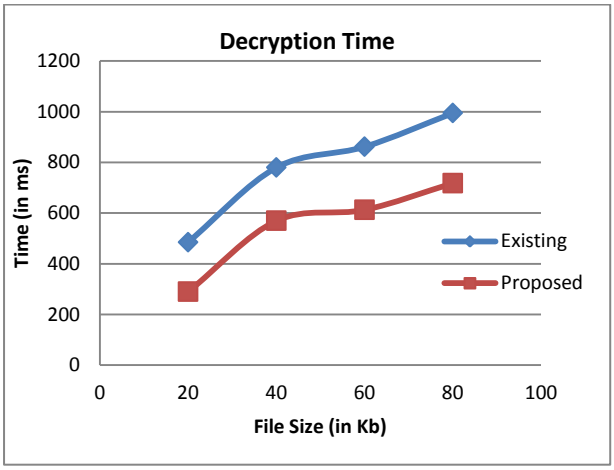

Figure 12 Decryption Time in (ms) for both existing and proposed model

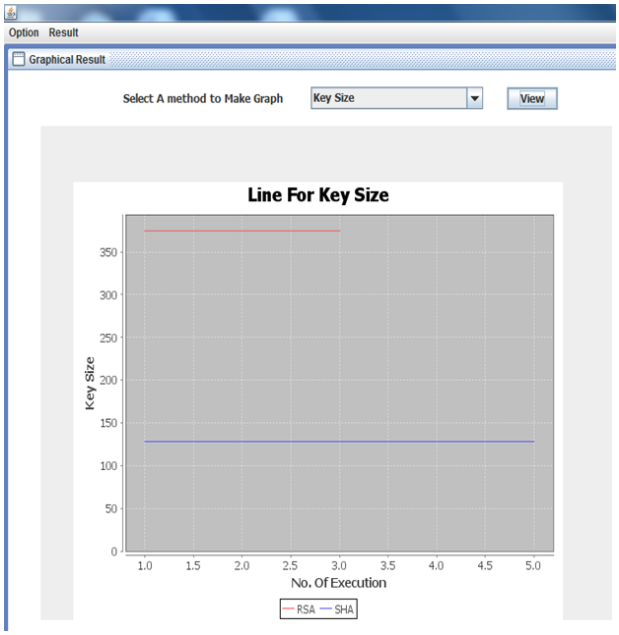

Figure 13 Key size for both existing and proposed model

Figure 11,12 and 13 concludes that the encryption,decryption time and key size of existing approaches are high while the proposed farmework required less amount of time. In this way our proposed architecture provides all round protection to the cloud environment with high performance and efficiency ratio.

For the analysis of project we perform man in the middle attack using the WebScarab tool on the virtual cloud server and client end. WebScarab , It is a web security application testing tool. It serves as a proxy that intercepts and allows people to alter web browser web requests (both HTTP and HTTPS) and web server replies. WebScarab also may record traffic for further review.WebScarab in an open source tool developed by The Open Web Application Security Project (OWASP), and was implemented in Java so it could run across multiple operating systems. In 2013 official development of WebScarab slowed, and it appears that OWASP's Zed Attack Proxy ("ZAP") Project (another Java-based, open source proxy tool but with more features and active development) is WebScarab's official successor,although ZAP itself was forked from the Paros Proxy, not WebScarab. The following analysis are:

By performing Man-in-the middle attack and sniffing attack we observe the result as : URL are monitor by the attacker only HTML view is visible to the attacker . Encryption key is not visible . The client download their required file from the cloud server the client need to verify using digital signature for the authentication then user enter valid digital signature which is used as (One Time Password)OTP So, the replay attack is not possible because same signature is not valid for second time download. Every time new signature is generated and verifying by the server and after verifying digital signature the required file is downloaded and decrypted using SHA-I Algorithm blended with AES Encryption Algorithm.

In figure 14 and 15 illustrates that if any content change by the attacker then the session gets expired and alert message is shown the clients machine that some malicious activities are performed on the network and user again login for further process.

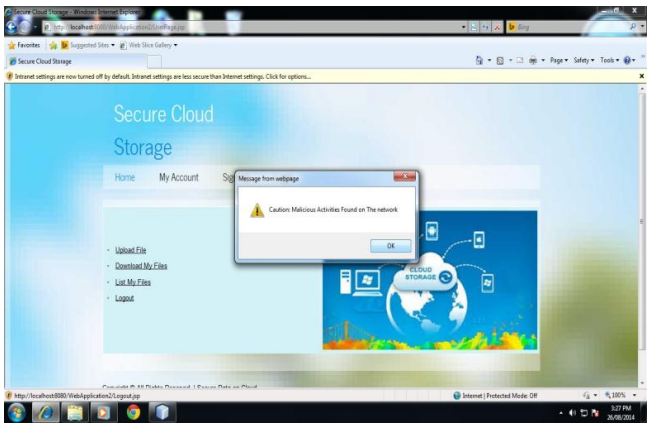

Figure 14. Alert message on the client window

Properties	Use of RSA + Digital Signature	Use of Elliptic Curve Cryptography	Use of Digital Signature + AES Algorithm	Proposed Model
Man-in Middle attack	Possible	Not possible	Possible	Not possible
Replay attack	Possible	Possible	Not possible	Not possible
Data Tampering	Possible	Not possible	Not possible	Not possible
Secure Key Exchange	Not Possible	Not Possible	Not Possible	Possible
Data Breach	Possible	Possible	Possible	Not possible
Data Loss	Possible	Possible	Possible	Not Possible
Non Repudiation	Achieve	Not Achieve	Achieve	Achieve
Authentication	Achieve	Not Achieve	Achieve	Achieve
Account Hijack then Data Breach	Possible	Possible	Possible	Not Possible
Security Level	Low	Moderate	Moderate	High
Efficiency	Moderate	High	Low	Moderate

Table 2 Comparison with Other Model

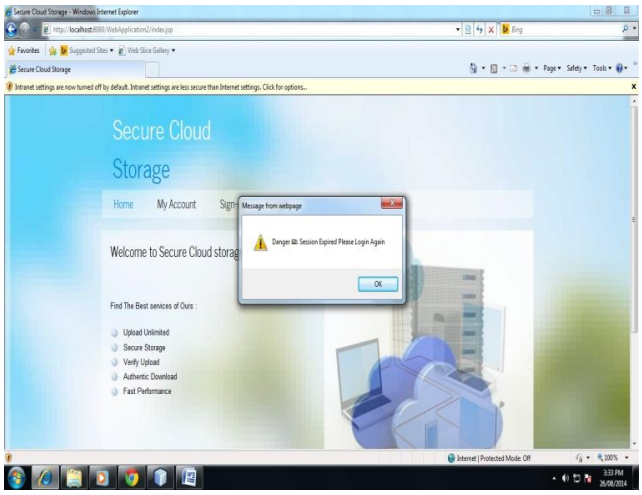

Figure 15 . Session expire and redirect to Homepage

The proposed model also supports the non-repudiation of the client because only valid digital signature is entertained by the server for the downloading of the file. In this way client never repudiate that the particular file was not downloaded by the user because digital signature was sent to the client for particular file download after valid signature enter file downloaded. In this way our proposed model provide all round protection to the cloud environment that is verification, authentication & data security at the same time. In this way our proposed architecture can be used as Backup server for IT Industries. Secure Data Center , Keeping confidential information of security agencies and this model can be beneficial to the ordinary user who puts their confidential data on cloud securely.

8.3 Theoretical Analysis

In the above Table 2 concludes that the proposed model provides all round protection to the cloud environment. It also concludes that the proposed model efficiency and security parameters are also reliable for the large infrastructure like cloud.

9. ACKNOWLEGMENTS

I express my professional gratitude with a great pleasure to Mrs. Vaishali Chourey, Associate Professor, Computer Science & Engineering Department of Medi-Caps Institute of Technology and Management, Indore whose constant encouragement enabled me to work enthusiastically, working under her guidance, has been a fruitful and an unforgettable experience & special thanks to IJCA Organization who provokes me to write quality of research paper.

10. CONCLUSION & FUTURE WORK

Although cloud computing has many advantages there are still many actual problems that needs to be solved. According to service delivery models, deployment models & essential characteristics of cloud computing, data security & privacy protection issues are the primary problems that need to be solved as soon as possible. In this research paper we proposed a security architecture for cloud system which provides all-round protection to the cloud i.e. authentication, data security & verifiability at the same time..

Finally, we conclude that i.e. "A Novel Framework for Cloud Security against Data Breach" can protect Data Breach, Data Loss from Cloud. Even clients account gets hijack no Data Breach and Data Loss possible.

For data security and privacy protection issues the fundamental challenges are separation of sensitive data and access control. Our proposed architecture is highly efficient and secure for private, community cloud & for the stagnant data and our future work is to make efficient system for public cloud & vibrant data. Our future work is to make a mobile application for secure data uploading/downloading from the cloud environment using this mechanism

11. REFERENCES

[1] Paul Simmonds, Chris Rezek , *" Security Guidance for Critical Areas of Focus in Cloud Computing"*, 2011 Cloud Security Alliance.

[2] The Notorious Nine Cloud Computing Top Threats in 2013,Cloud Security Alliance.

[3] Xufei Zheng, Yonghui Fang, *" An AIS-based Cloud Security Model"*, in IEEE International Conference on Intelligent Control and Information Processing , in August 13-15, 2010 , pp. 153 - 158 .

[4] V.Nirmala, *"Data confidentiality and Integrity Verification using user Authenticator scheme in Cloud"*, in Proceedings of 2013 IEEE International Conference on Green High Performance Computing, March 14-15,2013, pp. 1-5.

[5] Arjun Kumar, *" Secure Storage and Access of Data in Cloud Computing"*, in 2012 IEEE International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012, pp. 336 – 339.

[6] Chandramohan.D, " *A Novel Framework to Prevent Privacy Breach in Cloud Data Storage Area Service",* in Proceedings of 2013 IEEE International Conference on Green High Performance Computing, 14-15 March 2013, pp. 1-4

[7] Uma Somani,Kanika Lakhani, Manish Mundra, "*Implementing Digital Signature with RSA Encryption Algorithm to enhance the Data Security of cloud in cloud computing*" in 2010 IEEE 1st International conference Parallel ,Distributed & Grid computing (PDGC-2010), 28-30 Oct. 2010 , pp.211 – 216.

[8] Rashmi M.Jogdand, R.H.Goudar, Gazal Begum Sayed, Pratik B.Dhamanekar, *"Enabling public verifiability & availability for secure data storage in cloud computing"*, Springer Berlin Heidelberg, DOI-10.1007/S12530-013-9095-4.

[9] Pachipala Yellamma,Challa Narsimham, Velagapudi sreeivas, "*Data security in Cloud Using RSA*" in 2012 CSI Sixth International Conference on Software Engineering (CONSEG), 13 July 4-6, 2013 , pp. 1-8.

[10] Nandita Sengupta, Jeffrey Holmer, "*Designing of Cryptography Based Security System For Cloud Computing*" , in 2013 IEEE International conference on cloud & ubiquitous computing & emerging technologies, Pune 15-16 Nov. 2013, pp. 52-57.

[11] Mehdi Hojabri, K.Venkatrao, "*Innovation in Cloud Computing: Implementation of Kerbores version5 in Cloud Computing in order to enhance the security issues* ", in 2013 IEEE International Conference on Computing Technologies, 21-22 Feb. 2013, pp. 452 – 456.

[12] Prashant Rewagad, Yogita Pawar," *Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing"*, in 2013 IEEE International Conference on Communication Systems and Network Technologies, 6-8 April 2013, pp. 437 – 439.

[13] Arpit Gupta, Vaishali Chourey, "*Cloud Computing: Security Threats & Control Strategy using Tri-Mechanism*", Proceedings in 2014 IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies , 10-11 July, 2014, pp. 324-331.

[14] Fei Sun, Shi-ping Yang , "*Based on the agent of elliptic curve Diffie-Hellman Key Establishment Protocol* " in 2010 IEEE 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE) , pp. 134-136.

[15] Sung-Ming Yen and Chi-Sung Laih, "*Improved Digital Signature Algorithm* ",in 2010 IEEE Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), pp. 236 - 240 .

[16] Dai Zibin, Zhou Ning , "*FPGA Implementation of SHA-1 Algorithm* ", in IEEE 5th International Conference on ASIC, 21-24 Oct, 2003 , vol-2, pp. 1321 – 1324.

[17] Haoyu Wang, Junjun Kong, Yao Guo and Xiangqun Chen, "*Mobile Web Browser Optimizations in the Cloud Era: A Survey* ", in 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering , pp. 527 – 536.