DOI 10.12694/scpe.v19i4.1422
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 19, Number 4, pp. 351–360. http://www.scpe.org

ENHANCED DATA SECURITY FOR PUBLIC CLOUD ENVIRONMENT WITH SECURED HYBRID ENCRYPTION AUTHENTICATION MECHANISMS

PRABU S,* GOPINATH GANAPATHY,† AND RANJAN GOYAL‡

Abstract. Cloud computing is an evolving computing technology that provides many services such as software and storage. With the introduction of cloud storage, the security of outsourced data has become a major issue in cloud computing. Data storage in cloud computing environment needs to be secured in order to provide a safe and foolproof security for data outsourcing of the cloud service users. This paper presents a model for security of data in public cloud storage environment which successfully detects the unauthenticated access or any anomaly in the data. The proposed authentication model along with the data security model presented in this paper shows that this model is the best model suitable for securing the data in cloud computing environment.

Key words: Cloud Computing; Data Outsourcing; Data Security; Encryption model; Data Storage.

AMS subject classifications. 68M14, 68P25, 68P20

1. Inntroduction. Cloud Computing is an internet based computing technology that provides many services to the users including cloud storage. The cloud storage is a kind of cloud computing service that provides storage of data in logical pools, that is, the data is actually stored in some physical data centers present in some other location, but the user can access the data anywhere and on any device. The cloud computing is actually not a new technology, rather it is evolved from many existing technologies including grid computing, utility computing, parallel computing, distributed computing and virtualization. The cloud computing is a very powerful environment having pool of thousands of connected servers [1].

The cloud computing environment can be deployed as public, private, community or hybrid model. The public cloud deployment model is openly accessible to the public. The use of public deployment model can help in reducing computing costs making it economically inexpensive and efficient. The private cloud deployment model is generally used by private organizations. This model utilizes the VPN (Virtual Private Network) which makes it more secure from outside intrusion as compared to public cloud model. The community cloud deployment model is shared by several organizations that leads to formation of a community. This model is only suitable for the organizations working on the similar projects. The hybrid model can be a combination of public, private or community models. Here, it is a notable point that among all the deployment models, the public cloud model is most insecure and generic model. The public model can be used by anyone irrespective of the fact whether the use is a part of organization or community thus making it a generic cloud model. Thus, data security to the public cloud model is required to be provided in order to secure the outsourced data of the users.

This paper presents a model for enhanced data security for public cloud environment. The paper provides the description of model and its analysis which shows that the proposed model is suitable for enhanced security of data in public cloud environment. Rest of the paper is organized as follows: Section 2 provides the description of the cloud security with respect to attacks and security issues, fraud detection and different security mechanisms. Section 3 provides a discussion on related works based on the data security issues and reviews of cloud storage environment. Section 4 provides detailed discussion on the existing security mechanisms used for proposing the hybrid model. Section 5 provides the proposed model for enhanced security in (public) cloud environment. Section 6 provides an analysis on the proposed model followed by the conclusion in Section 7.

2. Cloud Security. Cloud Computing though being a powerful architecture, is vulnerable to many security issues and attacks. A discussion on the attacks, fraud detection and security mechanisms are provided below.

2.1. Attacks and Security Issues. There are several number of possible attacks to which the cloud storage is vulnerable. The attack can be a physical or a network based. The physical attack can be the attack from an unauthorized person, trying to access the data in cloud storage by breaking into the authentication

*School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, India
†School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, India
‡School of Computing Science and Engineering, Vellore Institute of Technology, Vellore, India

mechanisms. The network based attacks are the attacks from a system or a network of systems that are controlled by an attacker in order to break into the storage system or to disrupt the service. The most common among the network based attacks are Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM) attack. In DDoS attack, the attacker sends too many meaningless packets or requests which the system fails to handle and the service gets disrupted [2]. In case of MITM attack, the attacker sits between two parties and tries to acquire the information or data being exchanged [3]. This creates a major security issue for data outsourcing.

2.2. Fraud Detection. The detection of any fraud or attack is an important factor deciding the level of security in the system. The data outsourced should be kept into an environment equipped with a fraud detection mechanism. The detection can help in taking further actions to prevent any theft or loss of data. The mechanism of fraud detection may have several factors such as usual locations of login and possible places the user can login in a particular time duration. For example, one user logging in from New York cannot login just after 10 minutes from Hong Kong. Nonetheless, there can be a verification process initiated in that case. Further, the usual activities of a user activities can help in the prediction of fraud [4]. The work does not consider the fraud detection in terms of the example given above as the model proposed in the paper eliminated such scenario from getting executed.

2.3. Security Mechanisms. There are many possible mechanisms for security of data in public cloud. The cryptography algorithms can be used for encryption of the data and sensitive information. The cryptography is a technique which can be used to securely transfer the information between two parties. The data can be encrypted with the use of algorithms, so the attacker cannot read the actual data even in case the attacker acquires the data. There can be a private and public key which can be used to decrypt the data on successful transmission [5].

3. Related Works. Sugumar et al. [6] provided a detailed demonstration about the security issues, characteristics and its importance in public cloud storage environment. The two models proposed were based on the owners and users of the service. In case of any sensitive data stored, the owner and the users are treated as different, otherwise as same. The security issues and requirements addressed in the paper suggested that there is a need of new mechanism for ensuring of outsourced data. Singla et al. [7] explored the security of data and data at moving. The paper proposed an authentication protocol mechanism that was based on a 3-step process and a block cipher based encryption algorithm was proposed in the paper to prevent against known attacks. The first step in the 3-step in the authentication protocol mechanism is sending the message to the client on demand. The second step involves the client responding to the message with a value that is calculated using a one-way hash function. The third step involves authentication by verification of the response value against its own calculated hash value. In case of a match, the cloud service will be offered by to the client, otherwise the connection will be terminated

Masala et al. [8] presented a cloud platform that was designed to provide secure access to the data stored in the cloud. The cloud platform was built using open stack architecture and the authentication was done using biometric fingerprint and face recognition. Kaaniche et al. [9] provided a review of data security and privacy preservation in cloud storage environment using cryptographic mechanisms. The comparative analysis of different cryptography based defense mechanisms and the work done in the paper shows that the there are high security and privacy challenges that are required to be solved with evolving cloud infrastructure. A survey of security issues for cloud computing presented by Khan [10], analyzed and categorized the working mechanisms of possible security issues and its surveyed some of its possible solutions. The paper also provided a survey on intrusion detection and prevention systems and analyzed the effectiveness of the system. The literature suggested countermeasures to deal with the security issues discussed in the paper.

The literature survey of the related works showed that the public cloud environment is vulnerable to many network-based attacks and there is high need to solve this issue by providing a foolproof authentication protocol and encryption mechanism for proper authentication and authorization of users. Thus, this paper provides a hybrid authentication mechanism which on analysis shows that the mechanism is highly secured from severe network-based attacks. Further, the model proposed in this paper, secures the data in rest and data in transit by making it highly tough for the attacker to enter into the environment and remain into the environment.

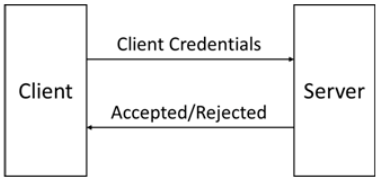

FIG. 4.1. *PAP 2-way handshake mechanism*

4. Existing Mechanisms. The existing mechanisms for authentication and encryption are discussed as follows:

4.1. Authentication Protocols. There are several existing authentication protocols proposed by researchers and scientists. The most common among them used to build the proposed mechanism includes Password Authentication Protocol (PAP), Secure Socket Layer (SSL) and Challenge Handshake Authentication Protocol (CHAP). This paper only focuses on these methods to provide a multi-layered hybrid authentication protocol.

The PAP is a password based authentication protocol that provides two-way handshake mechanism. In this protocol, the client sends the details such as username and password to the server which gets verified on the server side. In case the credentials match with the data present on the server-side database, the server sends an acceptance acknowledgement to the client and a connection is established. In case of no match, the client request is rejected and the connection request is terminated. Fig. 4.1 visualizes the PAP mechanism.

The issue in this protocol is that this protocol is highly vulnerable to network attacks such as Man-In-The-Middle Attack (MITM) which can lead to account hijacking and unauthorized access. This issue occurs in the case of PAP as the credentials sent by the client are in clear or plain text, i.e. not encrypted. This issue is fixed up to some extent by encrypting the credentials with some cryptographic algorithm. Nonetheless, there is still a chance that the attacker can decrypt the credentials making it still vulnerable to the MITM attacks.

The Secure Socket Layer (SSL) is a protocol used to establish a secure connection between the server and the browser of the client by the use of encrypted links to make the transactions private. The SSL uses a public and private key. The public key is used for asymmetric encryption and private key is used for symmetric encryption. The use of asymmetric key provides better authentication and the use of symmetric key provides faster authentication. A SSL certificate is required to establish a SSL connection for which the submission of Certificate Signing Request (CSR) is required to be done to the Certification Authority (CA). The CSR contains the details and identity of the website along with the private key. The CA then validates the data and issues a SSL certificate which matches with the private key. Thus, the SSL is based on mutual authentication i.e. the digital certificates verify the web servers and client identity before the establishment of the connection. If the web page is SSL secured, then the web address will begin with HTTPS instead of HTTP and a lock icon with appear which contains the details of the website certificate. Also, if the SSL is having Extended Validation (EV) certification then a green address bar will appear instead of the usual address bar. The use of SSL can prevent fraud and hijacking as it relies on encryption and the originality of the website is also verified up to some extent but it may cause a slowdown in the performance. Thus, the SSL can be used along with the proposed model but the model did not consider the use of SSL. Another protocol is Extensible Authentication Protocol (EAP). EAP is an authentication framework. The EAS was originally an extension for Point-to-Point (PPP) authentication. EAP framework supports multiple authentication mechanisms. This framework can also be used but the proposed model did not consider the complete use of this framework.

Another method of authentication is Challenge Handshake Authentication Protocol (CHAP). It is an internet standard that uses one-way MD5 hash function. The CHAP is based on a 3-way handshake mechanism [11]. In this type of authentication, instead of the actual password, the transmission of the hash result is performed over the network. As the password in this case, does not get transferred over the network, it cannot be captured during the transmission. Also, the hash function generates the random string in such a manner that the operation cannot be reverse engineered to obtain the original password. Nonetheless, this method is vulnerable to remote server impersonation. This vulnerability can be prevented by using a two-way authentication

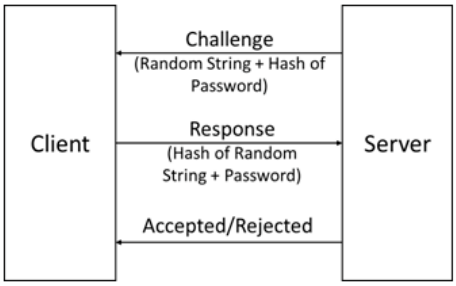

FIG. 4.2. *CHAP 3-way handshake mechanism*

using separate keys for transmitted and received data to identity server as well as client. This concept is used in MS-CHAP in which the challenge is sent repeatedly during the connection. Fig. 4.2 visualizes the CHAP mechanism.

4.2. Data Security. There are several existing algorithms proposed by researchers and scientists. The most suitable is discussed in this paper that is used in proposing the encryption model, i.e. Advanced Encryption Standard (AES). The AES is an encryption standard that is actually the 128-bit based symmetric block cipher algorithm known as Rijndael algorithm [13-15]. The AES is being used worldwide and is the most secure standard at present. The AES is the successor of Data Encryption Standard (DES) [16]. The AES is faster and more secure than DES. The Rijndael algorithm was based on 128, 192 and 256-bits block size but for the AES, only 128-bit block size was accepted. The AES thus have the block size of 128-bits and key size of 128, 192 and 256-bits. The algorithm is based on combination of substitutions and permutations. It operates on a 4 by 4 column major order matrix. There are 10 rounds for 128-bits key, 12 rounds for 192-bits key and 14 rounds for 256-bits keys. Thus, the data-in-rest and data-in-transit can be handled securely using this algorithm. The data here refers to the plain text which on encryption becomes cipher text. The cipher text can be converted back to plain text with the help of decryption. In symmetric encryption, the same key is used for encryption and decryption. Fig. 3 depicts the AES encryption and decryption operations.

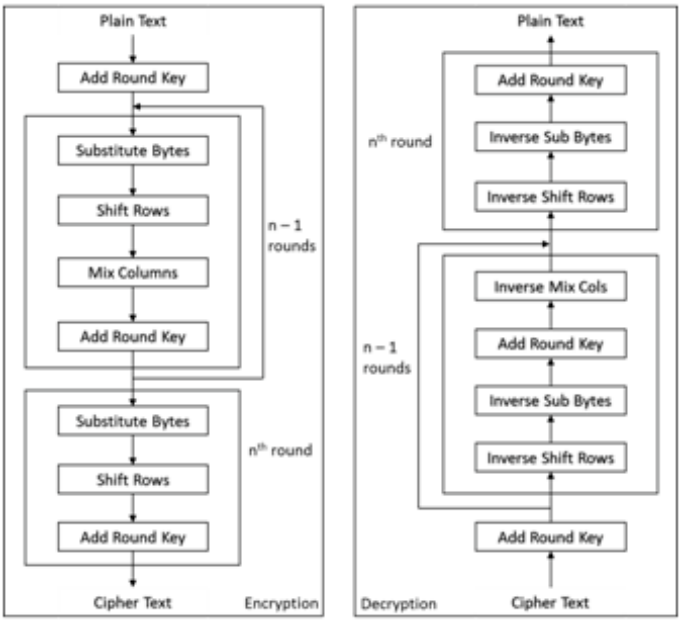

FIG. 4.3. *AES Encryption and Decryption*

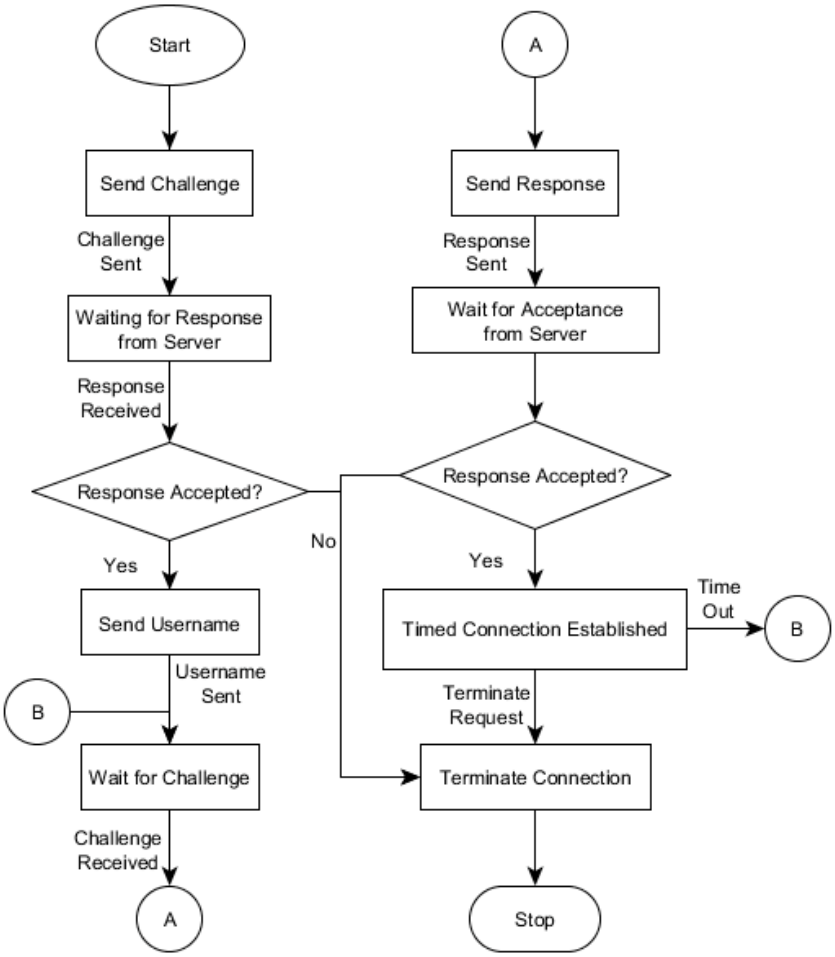

FIG. 5.1. *Proposed Client-Side Authentication Mechanism*

5. Proposed Method. The paper focuses on securing data present in the public cloud computing environment by providing a more secure hybrid of authentication and encryption mechanisms. The two mechanisms are discussed as follows:

5.1. Authentication Mechanism. The authentication protocol proposed in this paper, works on the idea of the PAP and CHAP mechanisms along with TLS. The client-side mechanism for the proposed authentication protocol is depicted in the Fig. 5.1. The client sends a challenge to the server and waits for the response. After the response is received, the response is verified and is either accepted or rejected. If the response is accepted then the client sends the username in encrypted format and waits for the challenge. In case of rejection, the connection is terminated. When the challenge is received, the response is generated and is sent to the server and the client waits for the acceptance of response from the server. Upon Acceptance, a timed connection is established. In case of rejection, the connection request is terminated. Upon connection time-out, the client waits for the challenge from the server and same procedure is repeated until the connection gets established again. During the connection, any terminate request if given, terminates the connection.

The server-side mechanism depicted in Fig. 5.2, shows the authentication procedure from the server side. Initially, the server waits for the challenge from the client. When the challenge is received, a response a generated and sent to the client. If the response is accepted by the client, the server waits for the client to send

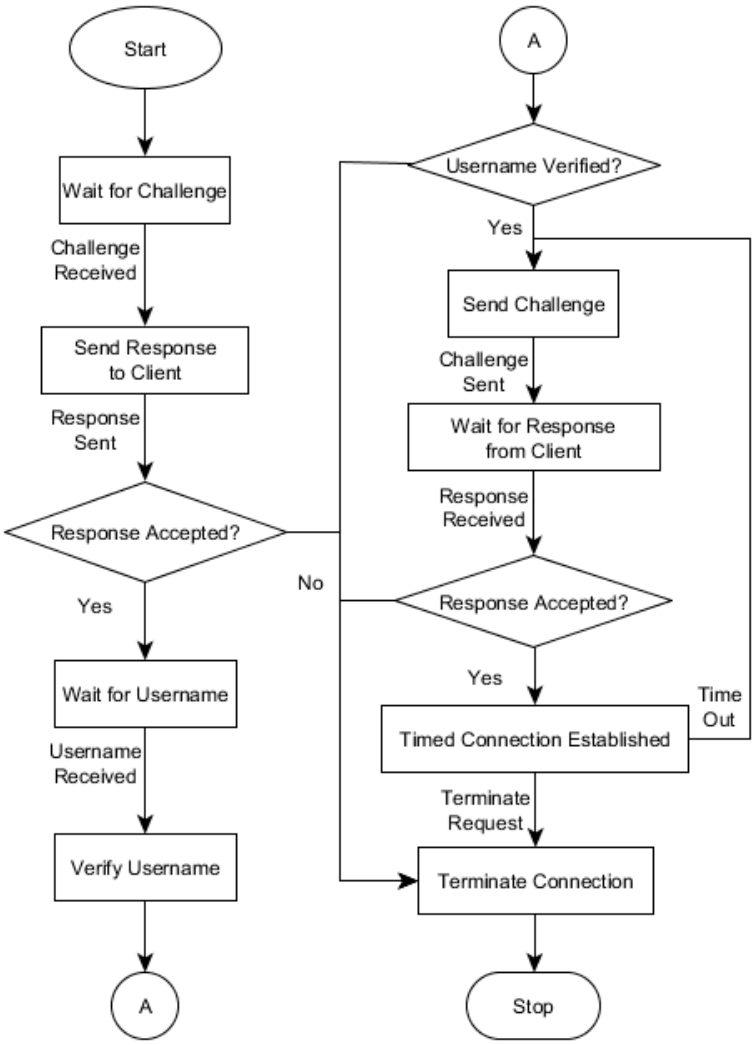

FIG. 5.2. *Proposed Server-Side Authentication Mechanism*

the username. When the client sends the username, the server verifies the username by decrypting encrypted using and matching it in the database. If the username is successfully verified, the server sends a challenge to the client and waits for the response. When the response is received, it is verified and on acceptance of response, a timed connection is established. The mechanism leads to termination in the case of rejection of response, rejection of username or any termination request.

The combined Client-Server Authentication Mechanism is depicted in Fig. 5.3. The mechanism depicted in the figure is based on the interactions of the client and server that does not show the time of propagation and delay. This proposed mechanism is named as Improved Hybrid Authentication Mechanism (IHAP).

5.2. Data Security. The paper proposes the encryption mechanism using the AES algorithm. There are several attacks that AES can handle including brute force and biclique attack due to high time complexity. Nonetheless, the poor key management can compromise the data. Thus, there is a need to deal with this problem by using separate key management technique. For this, the paper suggests to use the algorithm known as Secure Hash Algorithm 3 (SHA-3). This paper presents the key management using the SHA3-256 that have the attack resistance of 2128. Fig. 7 depicts the data security proposed model using AES encryption and SHA-3

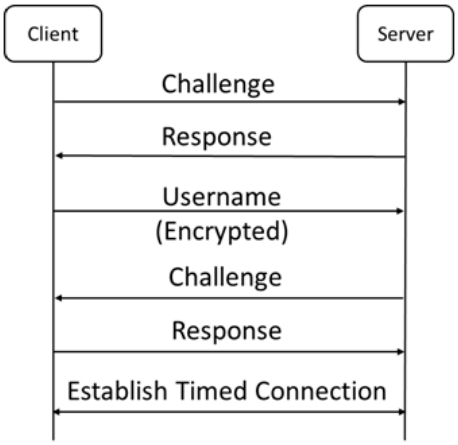

FIG. 5.3. *Proposed Client-Server Authentication*

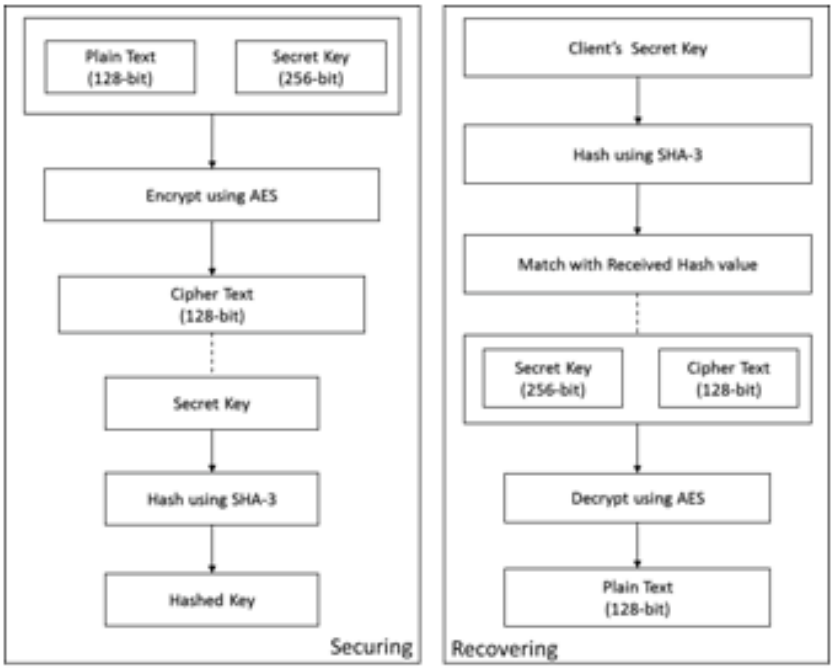

FIG. 5.4. *Data Security Proposed Model using AES and SHA-3*

hashing technique. The key used in AES for ciphering the text is of 256-bit. The size of block for SHA-3 is 256 bits. The data securing is done by first encrypting the plain text of 128-bit block using a secret key [17]. The cipher text obtained on encryption is the required encrypted data. Now, for key management, the secret key is hashed using the SHA-3 and the hashed key is obtained [18]. In recovering process, the original secret key that client is having, is hashed using the SHA-3. Then the hash value of that key is matched with the hashed value received from the server. In case of match, the key can now be used to decrypt the cipher text using the AES algorithm and the cipher text can be converted back into plain text.

6. Analysis. The proposed model for authentication for client and server side can be analyzed based on the possible common network attacks. The possible common network attacks in this scenario are MITM, DoS and DDoS Attacks. Let us consider the more powerful attack DDoS alone among DoS and DDoS as the DDoS

is the distributed attack scenario of DoS attack. Therefore, considering the MITM and DDoS attack possibility at every point of exchange of information, the authentication mechanism procedure is analyzed as follows:

Challenge and Response (Client and Server): In the case of DDoS attack, the attacker may try to send meaningless or irrelevant responses for the challenge. But this makes it impossible to continue the attack as the requests will be dropped after the limit is crossed. The limit is set for requests as it is impossible to receive a large number of requests from a client in a particular time limit. Thus, this point is safe from DDoS attack. In case of MITM attack, the attacker clones the client and tries to capture the response sent. Thereafter, there is a possibility that the attacker clones the server and sends the response to the client. But in this at the connection cannot be established as the username step involves encryption that makes it hard to perform MITM as the cloning of client and server along with decryption of username without knowing the actual algorithm and key is a complex process in real life scenario and hard to be implemented due to very high time complexity. As the time is limited for authentication, the attacker fails to perform the attack due to all this complex process. Also, there is a possibility that the attacker tries to fetch the challenge and solve it. In that case, the attacker may get the information of challenge that contains some random string along with hash of password. As the irreversible process is followed, the attacker cannot reverse engineer it, making it impossible to find the actual response value for that challenge thus making it highly safe from MITM attack at these points.

Username: In case of MITM attack, as the username sent is encrypted, so even if the attacker succeeds in capturing the username, it is hard to decrypt it without knowing the encryption algorithm and the value of key. Considering the worst-case scenario, the attacker successfully decrypts the username but in this case, the time limit by that time is already crossed and the process is already completed thereby making it meaningless to decrypt the username. Also, DDoS attack again becomes irrelevant at this point as the meaningless requests sent at this point will not be accepted thus making it highly safe from DDoS and MITM attack at this point.

Established Connection: In case of MITM attack, considering the only possibility that the attacker succeeds in bypassing authentication by somehow cloning the client successfully and establishes connection to server. Nonetheless, the attacker though gets the connection but as the connection is actually a timed connection, thus it will make it impossible to remain into the system after the time gets expired as the challenge and response process is further continued after time gets expired. Also, in case of DDoS attack at the time of established connection, no meaningless request is accepted from client and server side thus making it safe from MITM and DDoS attack at this point.

Thus, this proposed authentication mechanism is highly secure from common network attacks, MITM and DDoS attack. Considering the case of other attacks like phishing and sniffing attack etc., these attacks either comes under these MITM attacks which makes shows that this mechanism is secured from all these attacks. Consider an example of sniffing attack, where the attacker captures the packets being sent. As here the username sent is encrypted so it makes it safe from sniffing attack. Also, as the web page is SSL secured, it makes the webpage safe from phishing attack. Therefore, the mechanism is safe from many network attacks including the most common ones, MITM and DDoS attack.

Now, for the proposed data security model, the securing and recovering mechanism was implemented using the python program and the simulation was done on the system having specifications as: 16GB RAM and Intel i7, 7th Generation Processor on the Windows 10 environment. The simulation results were received for 1 MB, 10 MB, 100MB, 1GB and 10 GB file sizes and the running time for the securing and recovering process was recorded. The observed values for the proposed model of recovering and securing process is given in the Table I. Also, the graph depicting the securing and recovering time is shown in the Fig. 6.2. The securing process contains the results for running time that involves the encryption using AES 256-bit key and the generation of the hash value using the SHA-3 256-bit for that key after the encryption process is completed. The recovery process contains the results for the running time that involves generation of hash value for the clients key and matching this hash value with the received hash value from the server followed by decryption of the data using the clients key if the hash value of the clients key matches with the hash value received from the server.

Therefore, the proposed model for securing the data using AES and SHA-3 is safe from most of the known attacks including the password cracking brute force attack, birthday attack, biclique attack, timing attacks etc. as the AES is found to be safe from all these attacks. The only possible vulnerability was that the poor key management can compromise the data encryption. This problem is also solved by the proposed mechanism as

	File Size	Running Time (sec)
Proposed Securing Mechanism (Encryption + Hash Generation)	1 Megabyte	0.0150
	10 Megabytes	0.2000
	100 Megabytes	1.9300
	1 Gigabyte	19.2430
	10 Gigabytes	199.5580
	File Size	**Running Time (sec)**
Proposed Recovering Mechanism (Hash Generation + Hash Matching + Decryption)	1 Megabyte	0.0220
	10 Megabytes	0.1849
	100 Megabytes	1.7699
	1 Gigabyte	19.0590
	10 Gigabytes	128.0299

FIG. 6.1. *Observed running time values for proposed model*

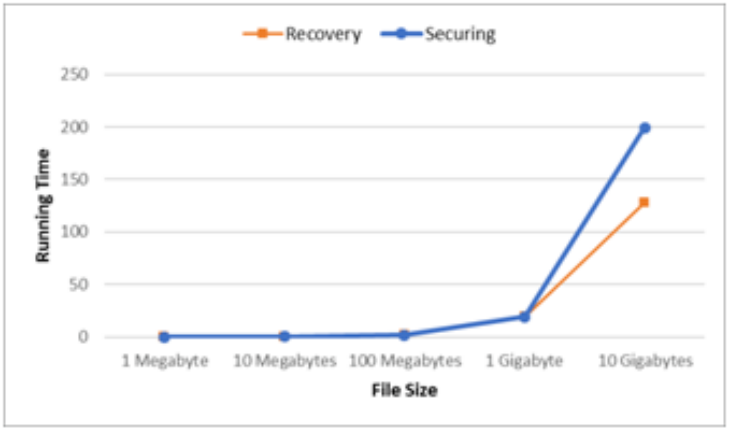

FIG. 6.2. *Graph depicting Securing and Recovering Time*

the mechanism hashes the key with the help of SHA-3. So, overall the security get user enhanced in terms of authenticity and data security. Thus, due to highly enhanced security during authentication and during accessing the data, it becomes almost impossible for the intruder to fool the security mechanism to get access to the resources and steal information and kept data in the cloud environment.

7. Conclusion. In this paper, a model for security of data in cloud computing environment is proposed that provides a detailed visualization of the security mechanism. The work done in this paper contributes in providing the highest possible security mechanism suitable for public cloud storage with the use of authentication and encryption mechanisms. The proposed model uses the hybrid approach from the existing mechanisms that helps in achieving the highly enhanced security. Future work is to implement further authentication mechanisms such as biometric authentication that includes fingerprint, iris and face recognition techniques as multilevel authentication mechanism. The biometric technique is currently not cost effective considering the cost of highly accurate iris and face recognition. Hence, this paper may also provide a scope for the integration of the biometric authentication into the cloud security mechanism along with the use of proposed authentication mechanism.

REFERENCES

[1] M.G. Avram, *Advantages and challenges of adopting cloud computing from an enterprise perspective*, 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013), Volume 12, pp. 529-534, 2014.

[2] Rashmi V. Deshmukh and Kailas K. Devadkar, *Understanding DDoS Attack and Its Effect In Cloud Environment*, Procedia Computer Science (2015), Vol. 49, pp. 202-210, 2015.

[3] S. Subashini and V. Kavitha, *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, Volume 34, pp. 1-11, July 2010.

[4] Md. Tanzim Khorshed, A.B.M. Shawkat Ali and Saleh A. Wasimi, *A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing.*

[5] Madhuri B. Shinde, *Design and Implementation of Asymmetric Cryptography Using AES Algorithm*, IJARIIE-ISSN(O)-2395-4396, Vol-1 Issue-4, pp. 371-378, 2015.

[6] Dr. Ramalingam Sugumar and Sharmila Banu Sheik Imam, *Data Security in Public Cloud Storage Environment*, International Journal of Engineering Research and Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 06, pp. 101-105, June-2015.

[7] Sanjoli Singla and Jasmeet Singh, *Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm*, Global Journal of Computer Science and Technology Software and Data Engineering, Volume 13, Issue 5, 2013.

[8] G.L. Masala, P. Ruiu, A. Brunetti, O. Terzo and E. Grosso, *Biometric Authentication and Data Security in Cloud Computing*, Int'l Conf. Security and Management, SAM'15, pp. 9-15.

[9] Nesrine Kaaniche and Maryline Laurent, *Data Security and privacy preservations in cloud storage environments based on cryptographic mechanisms*, Computer Commincations (2017) Vol. 111, pp. 120-141, October 2017.

[10] Minhaj Ahmad Khan, *A survey on security issues for cloud computing*, Journal of Network and Computer Applications (2016), Vol. 71, pp. 11-29, August 2016.

[11] Sadia Marium, Qamar Nazir , Aftab Ahmed, Saira Ahthasham and Mirza Aamir Mehmood, *Implementation of EAP with RSA for Enhancing The Security of Cloud Computing*, International Journal of Basic and Applied Sciences , Volume 1, Issue 3, pp. 177-183, 2012.

[12] Atewologun Olumide, Abeer Alsadoon, P.W.C. Prasad and Linh Pham, *A Hybrid Encryption model for Secure Cloud Computing*, 2015 Thirteenth International Conference on ICT and Knowledge Engineering, pp. 24-32, November 2015.

[13] Babitha M.P and K.R. Remesh Babu, *Secure Cloud Storage Using AES Encryption*, 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 859-864, September 2016.

[14] Sanjoli Singla and Jasmeet Singh, *Cloud Data Security using Authentication and Encryption Technique*, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Volume 2, Issue 7, pp. 2232-2235, July 2013.

[15] Mrs. S. M. Barhate and Dr. M. P. Dhore, *User Authentication Issues In Cloud Computing,*, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 4, pp. 30-35, 2016.

[16] Shakeeba S. Khan and R.R. Tuteja, *Security in Cloud Computing using Cryptographic Algorithms*, International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 1, pp. 148-154, January 2015.

[17] Zaid Kartit, *Applying Encryption Algorithm to Enhance Data Security in Cloud Storage*, Advances in Ubiquitous Networking. Lecture Notes in Electrical Engineering, Vol 366, pp. 141-154, Springer, Singapore.

[18] J R Ngnie Sighom, Pin Zhing and Lin You, *Security Enhancement for Data Migration in the Cloud*, Future Internet, Volume 9, Issue 3, pp. 1-13, June 2017.

Edited by: Rajkumar Rajasekaran
Received: Jul 24, 2018
Accepted: Dec 4, 2018