International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.3.25

Secure Authentication and Key Management Protocol in Cloud Computing

Umaima Fatima[1] and Dr. Sheeba Parveen[2]
[1]Department of Computer Science & Engineering, Integral University, Lucknow, Uttar Pradesh, INDIA
[2]Department of Computer Science & Engineering, Integral University, Lucknow, Uttar Pradesh, INDIA

[1]Corresponding Author: umaima0112@gmil.com

Received: 26-05-2023 **Revised:** 12-06-2023 **Accepted:** 29-06-2023

ABSTRACT

Cloud computing has brought revolution in IT (Information Technology) sector. It has transform the way organizations and individuals process, store and access applications and data , by offering scalable and on-demand access to computing resources including networks, servers, storage and applications. It is a flexible service that allows users to dynamically scale up and down their resources based on demand which enhances efficiency and optimizes resource utilization .Cloud computing offers number of benefits and saves cost. It eliminates the need for investing in hardware and software. Cloud computing allows users to work from anywhere over internet connection which enhances productivity .However, cloud computing has some challenges such as Security concerns that include unauthorized access and data breach. To provide security in cloud computing environment various authentication and authorization protocols exist but they also suffers from various security attacks. Nowadays three factor MAKA (Mutual Authentication and Key Management) protocol has gained popularity but they also lacked as they don't have dynamic revocation mechanism .To address these issues we have proposed a system based on id , password and biometric based authentication that has dynamic revocation mechanism and can resist various known attacks.

Keywords-- Cloud Computing, Security Issues, Authentication, Authorization, Encryption, Key Management

I. INTRODUCTION

Cloud computing technology provides on demand computing resources to access remotely over the internet .It allows individuals and business to access a network of servers and computing resources over the internet by paying the cost of resources they access, without actually maintaining the physical infrastructures. These network of remote servers and infrastructure on cloud provides a flexible and scalable and cost efficient computing environment. Cloud computing offers a wide range of services[1], like storage, networking, database, applications, computing resources and platforms. All these features of cloud computing makes it an attractive option for startups and large organizations[2]. Despite all these advantages Security is an important concern in cloud computing[3] as it stores and process data over remote servers. There are various measures available to overcome security issues which are taken by cloud provider and users to protect their data and applications. Most common security issues of cloud computing are Data Breaches, Insufficient Data Protection, Account Hijacking ,Insecure APIs, Data Loss. Authorization and authentication plays vital role in ensuring security in cloud computing environments. They only allow authorize user to access data, they also implement access control mechanism to protect sensitive data.

The traditional method of authentication based on id and password are no longer effective to provide security, hence nowadays multi factor authentication (MFA) is used which acts as an additional layer of security by authenticating users at various stages. It requires them to provide ids, password, in first stage and OTP, token or biometric information in further stages.

Authorization is the process of allowing or stopping users to access specific resources or services based on the access permissions they have. It ensures that only the permissible users can access the particular data or resources . Authorization is done through access control mechanisms.

Apart from authentication and authorization Encryption[4] also plays an important role in ensuring security and privacy of data in cloud computing environments. Encryption technique encodes data and information in some non-understandable ciphertext, hence it becomes impossible to read it without having it's decryption key which only authorize users have. Encryption helps protect sensitive data and information from unauthorized access.

There are basically two main types of encryption technique exists Symmetric and Asymmetric encryption[5].In symmetric encryption a single key is use to encrypt and decrypt the data. Popular Symmetric

Encryption methods are Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Blowfish.

In asymmetric encryption two keys are used a public key for encryption and a private key for decryption. It is also known as public-key encryption. Popular Asymmetric Encryption methods are Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC). Many times unencrypted data is stored and processed in cloud computing environment ,in this situation if any attacker gets into system then it may result in data breaches, loss of confidentiality and integrity of data. Encryption helps maintain the confidentiality, integrity, and privacy of data, allowing only authorize parties to access and interpret the information, hence along with authentication and authorization encryption of data is also important to ensure security in cloud computing environment.

We have proposed a system based on id, password and biometric based multi factor authentication it shares data over cloud in encrypted form . We have done security and performance evaluation to prove effectiveness of our system.

II. LITERATURE REVIEW

There are a lot of techniques available to ensure security in cloud computing some are discussed here. In [6] a model was proposed that used the password based mathematical method to provide single server and two server Authentication Systems. In single-server architecture a single authentication server was involved for authentication purpose, it stored password of all clients in database which was required when authenticity of client is verified, if in case here server fails then complete system halts. To recover this two servers, a front- end and a back-end authentication server were used .The first server acts as a public server, and second server is required for maintaining an updated list passwords of clients .A multi-level authentication was proposed in [7] where user's password were verified at three level first at organizational level by checking whether user has privilege to access the services , then secondly at team level where access was granted to particular cloud services. At last third level authentication of user was done, where permissions and privileges for a specific purpose were granted to the user. A three step security system was given in [8]that used steganography and cryptography techniques. This model was composed of three levels. The first level consist of cryptography using RSA to prevent unauthorized access to data, at second level data was recovered using stegnography where it was hidden in an image in form of cipher text. In third level data was taken from the image and it is decrypted using RSA .In [9]an ECC based authentication technique was proposed that used digital signature based identification for authentication. It does not required any modular inversion which made it more efficient. However it required a method to find index using multiplicative group of finite fields. A light-weight authentication method was proposed in [10]that comprises of three phase. where cloud server and client both produce a random number and request is send to third party which verifies and responds with a timestamp and a random number to mutually authenticate each other. This system had a disadvantage as it used a third party agency .A lightweight authentication system was also proposed in [11]based on message digest and location that used symmetric key encryption. It uses client's current location and timestamp to authenticate user .A multimodal based biometric authentication method was developed in[12],using finger print and iris. Symmetric and asymmetric cryptographic techniques was used here to maintain data security. This method was efficient , cost-effective and scalable. In[13] a CC framework based model was proposed that provide user a secure connection to access cloud. The environment of cloud orchestration and single sign-on token was considered to provide better experience and smooth functioning. In [14], an authentication system based on the RSA was given, however, it had a complex key generation process. In [15] a blockchain based authentication and authorization scheme was proposed .This scheme was efficient and scalable and it enhanced security of mobile cloud computing , but it had a high storage cost. After analysing all these previous work we have proposed our own system which is discussed in this paper.

III. PROPOSED METHOD

Our proposed consists of different cloud users and servers who access uploads and downloads files from cloud server.

1) Registration Phase

It is the first phase here users enters its user-id , email, mobile number and password and biometric information (fingerprint) the server verifies all information and validates user.

2) Login and Authentication

Our proposed system uses two-factor authentication for verifying the identity of user. In the first phase user enters its registered email and password after successful verification of this entered information from server the user is brought into second phase of authentication. In second phase user enters its biometric information (fingerprint) after the successful verification of these information user is logged In into the system.

3) Simulations Environment

In our proposed system we have created an environment where user uploads and downloads files from server. The files that are stored over server in cloud

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.25

computing environment hence they may suffers from various security attacks . To prevent our system from security threats two factor authentication has been implemented, further for secure uploading and downloading of data and files, these files are encrypted using 256 bit AES encryption at various levels.

We encrypted our file with 256 bit AES encryption and stored in over cloud server, to prevent from network attack we will outsource our encrypted data in a digital envelope. Encryption process isdescribed as follows.

Input: file F, public key K1
Output: DE
1: Demand symmetric key K1
2: Perform (AES) encryption based on
K1. CF = EK1(F)
3: Generate Digital Envelope: DE on encrypted file K1.CF

After generation of encrypted file this file is stored over server .If any authorize user wants to view or download this file then user needs to get a secret key to download this file. To generate secret key the user submits the required information based on that a key is generated and share to user via a secured medium. Then user can decrypt and download the requires file using the secret key provided to him.

Decryption of file is shown below
Input: Encrypted file EK, secret key K1
Output: F
1: Decrypt with AES the ciphertext for the secret key CT and obtain K1 D(EK , K1)
2: Decrypt with K1 the data ciphertext CT and get decrypted file F

The flow chart of our proposed system is as follows

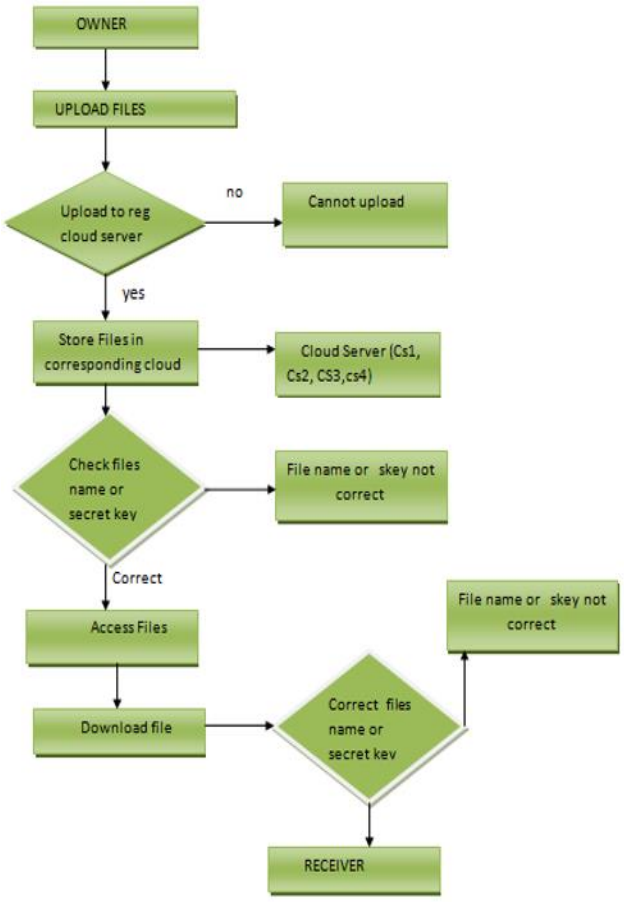

Figure 1: Flow Chart

IV. SECURITY EVALUATION

To show security of our proposed system we have presented a security discussion based on some security attack and issues.

1) Account Service and Traffic Hijacking

It involves denial-of service attacks (DOS), man-in-the-middle attacks (MITM), and phishing attacks. Moreover the confidentiality and integrity of data in cloud computing get compromised by accessing sensitive data and stolen credentials by attackers. To prevent this credentials are being stored in encrypted form which becomes impossible for attacker to steal them.

2) Man-in-the-Middle Attack

MITM is an attack through which attackers secretly intercepts communication between two parties. Our proposed model implements two factor authentication using password and fingerprint, which prevents it from MIMT attack.

3) Brute Force Attack

A brute force attack is a method used to access a system in unauthorized way or decrypt encrypted data by

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.25

systematically trying all possible combinations of keys or passwords until the correct one is found. Our proposed system uses one-way hash in iterative manner to prevent brute force attack.

4) Cloud Account Hijacking

In this attack attackers pretend as cloud owner by stealing account information of owner. In our proposed model, we have implemented verification of user using fingerprint to prevent this type attack.

5) Replay Attack

A replay attack is a type of network-based attack where an attacker intercepts and maliciously replays valid data transmission between two parties in an attempt to gain unauthorized access or deceive one of the parties. It involves capturing network traffic containing authentication credentials, session tokens, or other sensitive information and replaying it at a later time. In our proposed system, this type of attack is being prevented by using two-factor authentication using passwords with biometric information that is fingerprint.

Further our systems continuously monitors for attack in iterative manner. If it found any attack it immediately informs administrator which recovers from attack and retrieves data or file successfully using recovery method setup in system.

V. PERFORMANCE EVALUATION

We have done a comparative evaluation on our proposed system which is on AES with DES algorithm. DES algorithm is symmetric cryptographic algorithm DES algorithm is block cipher and it works on block of data .We have compares DES with our proposed system that is based on AES.

In table 1 throughput of DES and our proposed system is compared .In table 2 processing time of both is compared the results proves superiority of our proposed system over DES. Fig 2 shows graphical comparison of both.

encryption algorithms	Proposed scheme	DES
Throughput	27.76	10.13

Table 1: Throughput

Input size(KB)	Proposed scheme	DES
15	3.8	5.07
30	7.5	17.9
45	8.5	19.96
60	8.8	22.91
75	9.33	29.99
90	10.7	38.15
Average Time	8.105	22.195
KB/sec	27.76	10.13

Table 2: Processing time

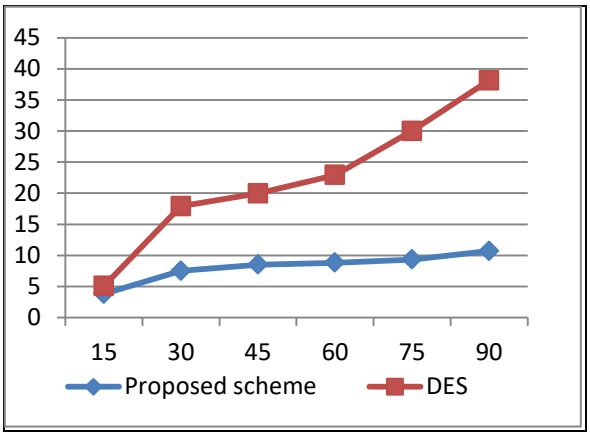

Figure 2: Time taken in encryption & decryption of our scheme and DES

VI. RESULTS

A two factor based dynamic authentication scheme with a mix of traditional id, password and modern biometric method has been proposed. That authenticates and authorizes user based on two factor authentication and resist some known attacks such as man in the middle attack, brute force attack, session hijacking attack and replay attack. Our system created an interface for secure sharing of file and data over cloud by encrypting files and data using AES encryption hence it becomes difficult for attacker to access it. If any how an attackers gets into system and manipulates file content our system was successfully able to recover the original file. Further we have compared our proposed system with DES algorithm and results were recorded in tabular form. Further graph were also plotted for the results. Results shows that our proposed system is superior than DES.

VII. CONCLUSION

Cloud computing allows access of computing resources remotely over the internet in pay-per-use-model. Despite having numerous of benefits it lacks in area of

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.25

security and privacy. To overcome these issues various measures are taken. Authentication, authorization and encryption plays an important role in ensuring security and integrity of data in cloud platform. The traditional method of authentication based on username/id and password are no longer enough to ensure security in cloud platform. Nowadays, multifactor authentication techniques (MFA) have emerged and are being used widely. These MFA techniques requires users to go through multiple stages of verification such as basic username and password and advanced techniques like OTP, Security Tokens, Biometric. An authentication system should be able to protect cloud from various authentication attacks. Our proposed method is based on id, password and biometric. It is successfully able to resist known attacks and provide better performance.

REFERENCES

[1] C. N. Hoefer & G. Karagiannis. (2010). Taxonomy of cloud computing services. *IEEE Globecom Work. GC'10*, pp. 1345–1350. DOI: 10.1109/GLOCOMW.2010.5700157.

[2] H. Gangwar. (2017). Cloud computing usage and its effect on organizational performance. *Hum. Syst. Manag.*, *36*(1), 13–26, DOI: 10.3233/HSM-171625.

[3] M. M. Alani. (2016). Security attacks in cloud computing. *SpringerBriefs Comput. Sci.*, pp. 41–50. DOI: 10.1007/978-3-319-41411-9_4.

[4] D. K. R. Shukla, V. K. R. Dwivedi & M. C. Trivedi. (2020). Encryption algorithm in cloud computing. *Mater. Today Proc.*, 37(2), 1869–1875. DOI: 10.1016/j.matpr.2020.07.452.

[5] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi & H. Sastry. (2016). Security algorithms for cloud computing. *Procedia Comput. Sci.*, 85(Cms), 535–542. DOI: 10.1016/j.procs.2016.05.215.

[6] D. Chattaraj & M. Sarma. (2018). Dependability quantification of cloud-centric authentication frameworks. *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 840–844. DOI: 10.1109/CLOUD.2018.00117.

[7] H. A. Dinesha & V. K. Agrawal. (2012). Multi-level authentication technique for accessing cloud services. *Int. Conf. Comput. Commun. Appl. ICCCA*. DOI: 10.1109/ICCCA.2012.6179130.

[8] V. K. Pant, J. Prakash & A. Asthana. (2015). Three step data security model for cloud computing based on RSA and steganography. *Int. Conf. Green Comput. Internet Things, ICGCIoT 2015*, pp. 490–494. DOI: 10.1109/ICGCIoT.2015.7380514.

[9] L. Wang & T. Song. (2016). An improved digital signature algorithm and authentication protocols in cloud platform. *IEEE Int. Conf. Smart Cloud, SmartCloud* pp. 319–324. DOI: 10.1109/SmartCloud.2016.46.

[10] J. Shen, D. Liu, S. Chang, J. Shen & D. He. (2015). A lightweight mutual authentication scheme for user and server in cloud. *1st Int. Conf. Comput. Intell. Theory, Syst. Appl. CCITSA*, pp. 183–186. DOI: 10.1109/CCITSA.2015.47.

[11] S. Dey, S. Sampalli & Q. Ye. (2015). A light-weight authentication scheme based on message digest and location for mobile cloud computing. *IEEE 33rd Int. Perform. Comput. Commun. Conf. IPCCC*, *1*, pp. 1–2. DOI: 10.1109/PCCC.2014.7017041.

[12] S. K. Khatri, Monica & V. R. Vadi. (2018). Biometrie based authentication and access control techniques to secure mobile cloud computing. *2nd Int. Conf. Telecommun. Networks, TEL-NET 2017*, pp. 1–7. DOI: 10.1109/TEL-NET.2017.8343558.

[13] S. H. Na, J. Y. Park & E. N. Huh. (2010). Personal cloud computing security framework. *IEEE Asia-Pacific Serv. Comput. Conf. APSCC*, pp. 671–675. DOI: 10.1109/APSCC.2010.117.

[14] P. Yellamma, C. Narasimham & V. Sreenivas. (2013). Data security in cloud using RSA. *4th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT*. DOI: 10.1109/ICCCNT.2013.6726471.

[15] L. Yu, M. He, H. Liang, L. Xiong & Y. Liu. (2023). A blockchain-based authentication and authorization scheme for distributed mobile cloud computing services. *Sensors*, 23(3), 1264. DOI: 10.3390/s23031264.