Hybrid Algorithm for Cloud Data Security

Richa Singla[1], Richa Dutta[2]

[1]M.Tech Student, Yamuna Institute of Engineering & Technology, Gadholi (Yamuna Nagar).

[2]Assistant Professor, Yamuna Institute of Engineering & Technology, Gadholi (Yamuna Nagar).

Abstract: Cloud computing has shifted the concept of computing from local hard disk to remote data centers, providing a lot of benefits. But, in spite of the many potential blessings of cloud computing, this new prototype is also connected with additional risks which cloud consumers, people or organization's leasing cloud resources need to be concerned about.

This research paper proposed a hybrid algorithm which comprises of MD5 hash with AES security algorithms to assure the clients about their data security in cloud. The hybrid algorithm almost guarantee for data security in today's scenario.

Introduction

Cloud computing has attracted significant momentum and attention in both academia and industry. For some, cloud computing fulfills the long-held dream of "computing as a utility," while for others cloud computing is nothing more than an advancement of conventional ideas.

Cloud computing is also connected with additional risks which cloud users, people or organization's leasing cloud resources needs to be concerned about before switching to the cloud. Some of them are discussed here onwards.

Foremost of all, the cloud service provider (CSP), who offers and controls the cloud resources, has full access to all data or computations available in the cloud.

Second, because CSPs share their limited resources to multiple consumers for efficiency reasons. Here is the threat from other cloud users, with whom cloud resources are shared, through breaching or compromising the isolations imposed by the CSP.

Third, by using the cloud offerings through the traditional protocols and channels, it is still prone to the traditional attacks and breaches already practiced by external attackers. In fact, as some researchers identified that, most of the security threats in the cloud-hosted software still occur through traditional attack methods, e.g. web services exposed to the internet.

1.1 Various Data Theft Incidences

There have been a large number of data theft incidences in past which led to loss of consumer's data therefore the companies trust. Some of them are mentioned as under…

(i) February 2015 - Anthem

Theft of personal information on up to 78.8 million current and former customers. $100 million

(ii) September 2014 - Home Depot

Theft of credit/debit card information of 56 million customers. $33 million

(iii) December 2013 - Target Stores

Credit/debit card information and/or contact information of up to 110 million people were compromised. $162 million

(iv) July-August 2011 – ESTsoft

The personal information of 35 million South Koreans was exposed after hackers breached the security of a popular software provider. It is called South Korea's biggest theft of information in history, affecting a majority of the population.

(v) April 2011 - Sony Play Station Network

77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.

(vi) March 2011 - Epsilon

Exposed names and e-mails of millions of customers stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization, College Board.

(vii) March 2011- RSA Security

Possibly 40 million employee records stolen.

and many more

DOI: 10.141079/IJITKM.2016.097

1.2 Literature Survey

[1] Pritesh Jain et al surveyed several aspects of cloud computing security concerns. They concern on the major challenges that faces the cloud computing is how to secure and protect the data and processes the data of the user. To provide secure and reliable services in cloud computing environment is an important issue. One of the security issues is how to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in this environment.

[2] D. S. Abdul et al, [23] S. Pavithra et al provides experimental evaluation of six most common symmetric key encryption algorithms, namely- AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. The comparison has been carried in different contexts for each algorithm. The report concludes that the AES algorithm is competitive over the rest of algorithm on being fast and flexible.

[3] Parikshit Prasad et al proposed a framework works in two phases to focus along the problem of data leak. They categorize the data in first phase known as Data classification done by the client before storing the data depending on the basis of CIA (Confidentiality, Integrity, and Availability). The client who wants to send the data for storage needs to legislate along the value of C (confidentiality), I (integrity), A (Availability). With the help of proposed formula, the priority rating is calculated. Consequently, data having the highest valuation are considered to be critical and 3D security is recommended on that data. In the second phase the user who wants to access the data need to be authenticated, to avoid impersonation and data leakage. The proposed solution ensures availability of data by overcoming many existing problems like denial of services, information leak.

[4] Vadym Mukhin et al analyzed vulnerabilities and security risks specific to cloud computing systems. They defined four indicators for cloud-specific vulnerability, including

(i) It is intrinsic to or prevalent in core technology of cloud computing,

(ii) It has its origin in one of NIST's essential cloud characteristics,

(iii) It is caused by cloud innovations making security controls hard to implement,

(iv) It is prevalent in conventional state-of-the art cloud offerings.

[5] Ashutosh Kumar Dubey et al proposed a new cloud computing environment where we approach a trusted cloud environment which is controlled by both the client and the cloud environment admin. The approach is mainly divided into two parts. The first part is controlled by the normal user which gets permission by the cloud environment for performing operations and for loading data. The second part shows a secure, trusted computing in the cloud, if the admin of the cloud wants to read and update the data then it takes permission from the client environment. This provides a way to hide the data and normal user and can protect their data from the cloud provider. This provides a two-way security protocol, which helps both the cloud and the normal user.

[6] Eman M. Mohamed et al advised to Amazon EC2 cloud users, must use AES, which is the highest security algorithm which it is the most secured and also consumes less time to write in code.

[7] Gurudatt Kulkarni et al paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. The authors mainly propose the core concept of secured cloud computing. They indicate the cloud computing based on separate encryption and decryption services from the storage service. The authors embarked on with the DDoS (Distributed Denial of Service) attack, a man in the middle attack, SSL discrepancies, data loss, phishing and Botnet issues faced in cloud data protection. The authors firstly discussed service provider security issues those are Identity and access management, Privacy, Securing Data in Transmission, User Identity, Audit and Compliance. Secondly, infrastructure security issues are discussed those are Secure Data storage, Network and Server Server-Side Protection. Thirdly end user security issues are discussed those are Security-as-a- service, Browser Security, Authentication, Loss of Governance, Lock-In, Data Protection.

[8] Hyun-Suk Yu et al addressed the potential attacks on the cloud i.e. Denial of Service (DoS) attacks, Side Channel attacks, Authentication attack, Man-in-the-middle cryptographic attacks, Inside-job attack etc. the paper concludes that the integrity of the data during the transmission can be guaranteed by the SSL protocol.

[9] Singh et al stated different attacks that may take place at any time on cloud those are DOS attacks, Cloud malware injection, side channel attack, authentication attacks, and Man-In-The-Middle (MITM) cryptographic attack.

[10] Sandeep K. Sood proposes a solution for that data security which starts the classification of the first data on the basis of three most adopted cryptographic parameters passed by the user, i.e., Confidentiality (C), Availability (A) and Integrity (I). Thereafter to protect the data before transmitting it to cloud uses various standard encryption techniques such as SSL (Secure Socket Layer) 128-bit, MAC (Message Authentication Code) for integrity verification of data, indexing of the data and partitioning of data into three categories stored in the cloud.

[11] Stolfo SJ et al proposed an approach that uses user behavior and decoy information to mitigate insider data theft. In this advance, data access patterns are monitored by profiling the user behavior. Decoy documents that are stored in

the Cloud along with the user's real data act as detectors to detect illegitimate access. When an unauthorized access is found, it is verified using challenge questions.

[12] Jingyu Wang et al presented a method of data security access to protect sensible data in cloud computing based on virtual adversary structure. The method partitions sensitive data into segments or partitions and distributes them to each participant. It can assure that only legitimate participants can connect with their petitions to reconstruct sensitive data. At the same time the illegal participants associate with their partitions cannot obtain any data about sensitive information.

[13] Louai A et al showed several threats to data's privacy, confidentiality and integrity over the Cloud. The threats include abuse and nefarious use of Cloud Computing, insecure APIs, malicious insiders, shared technology vulnerabilities, data loss or leakage, account or service hijacking, and unknown risk profile.

[14] Lekshmy D. Kumar et al discussed various data security threats and challenges such as data confidentiality, data location, data breaches, control issues, service traffic hijacking, insecure interfaces and APIs, Denial of service, shared technology vulnerabilities, regulatory and legislative issues, forensic evidence issues, auditing issues, business continuity and disaster recovery issues, security policy issues, etc which are to be considered and counter measures to be taken by the organization before moving their information into the cloud.

[15] Mrudula Sarvabhatla et al proposed cryptographic schemes, which ensure the mutual ticket based authentication between the third-party cloud server and the distant cloud user. This mutual validation system is very secure and resistant to all majorly known cryptographic attacks. The strength of the proposed authentication scheme is very much high even when there will be the large number of cloud users.

[16] Chaparala Pushya et al proposed a scheme, to verify the authenticity of the user without knowing the user's identity before storing data. The proposed algorithm ensures that only valid users will be able to decrypt the stored information, as well as prevents replay attacks and supports creation, modification, and reading data stored in the cloud.

[17] Debasish Jana et al discussed various newer privacy and security challenges across enterprises during the communicating or exchanging data to the cloud. As smartphones and tablets are storing users' private data with the data of his knowns - such as friends, family members, customers, vendors or any other individual. They addressed a secure framework against Denial of services, data leakage, account confiscation, exposure to insecure application program interface, isolation of virtual machine, mischievous attacks from an insider, losing the key used in encryption.

[18] Zhongbin Tang et al., [19] Chunming Rong et al., [20] Bernd Grobauer et al., [21] AL-Muslim Waleed et al, [22] Guoman Lin highlighted the critics of the data security in the cloud, one of the important factors restricting the growth of cloud computing and reviewed the faults on the protection of their data storage and its secrecy.

1.3 Proposed Hybrid Algorithm for Cloud Data Security

The basic idea of the algorithm is that, the use of a weak encryption for both encryption and decoding is very prone to malicious attacks. Hence, in the proposed algorithm, this issue is resolved by the using advanced encryption techniques for encryption as well as decryption. The user who wishes to access the information is required to furnish the login id, password, OTP (one-time password) & CAPTCHA sent to the user registered mobile number, before he gains admission to the specific cloud service.

The primary focus of this algorithm is to maximize the data owner's control on user data during transit as well as during storage. Since more we will apply the locks more time it will take to fetch the data back. As all data is not of the same importance, so we can categorize the data initially on the basis of its sensitivity. So, that different security layers can be used for the different categories of the data. To achieve above defined objective the data is split into three different protection layers for each privacy categorized data that has different privacy aspects according to the need of sensitive data. For this a cloud computing model is proposed for ensuring data security. Data is firstly divided into following categories:

(i) Category 1- Not Sensitive data

(ii) Category 2- Sensitive data and Trusted Provider

(iii) Category 3- Sensitive data and non-Trusted Provider

At this point, no encryption and decryption are done for category - 1 data during its storage and accessing.

Whereas in category – 2, the CSP is fully trusted and he is fully responsible to establish the security of data. CSP used the DES encryption and decryption technique which automatically generate the public key which is known to everyone.

In the third case for the most sensitive category - 3 data to act upon we adopt a security scheme in which both User and CSP are responsible to ensure the protection of data. User encrypts the information using AES algorithm before sending to CSP, and then CSP may or may not use any encryption and decryption technique for complete data protection. In this chapter, we have described category – 3 data security module in detail.

Section 1.4 describes the proposed model. The section identifies the complete algorithm in detail and all the steps followed.

Section 1.5 presents the security analysis of the proposed model. The section identifies the study of various attacks against proposed model in detail.

1.4 Proposed Model

Proposed framework has been structured to provide complete protection to the data throughout the process of cloud computing, be it in the cloud or in passage. Therefore, multiple mechanisms and available techniques are utilized to shield the critical information from unauthorized parties. The suggested framework is split into four phases. First phase deals with process of registration of the user to CSP. Second phase deals with the storing of the data in cloud storage. Third phase deals with the user authentication on data retrieval request. Fourth and last phase deals with the recovery of data from cloud by the authenticated user and verification of integrity of the recovered data, thereby providing information back to authorized user with passing all security mechanisms.

1.4.1 Phase 1 (Registration of Cloud User to Cloud Service Provider)

As expressed in figure 1.1, foremost of all, the user will have to register himself with the cloud service provider by providing its credentials, user name, password, registered mobile number. The password is hashed with MD5 hashing technique and resultant hash code will be preserved by the CSP. Storing hash code of the password in the CSP database will prevent the data from account hijacking and insider job attack.

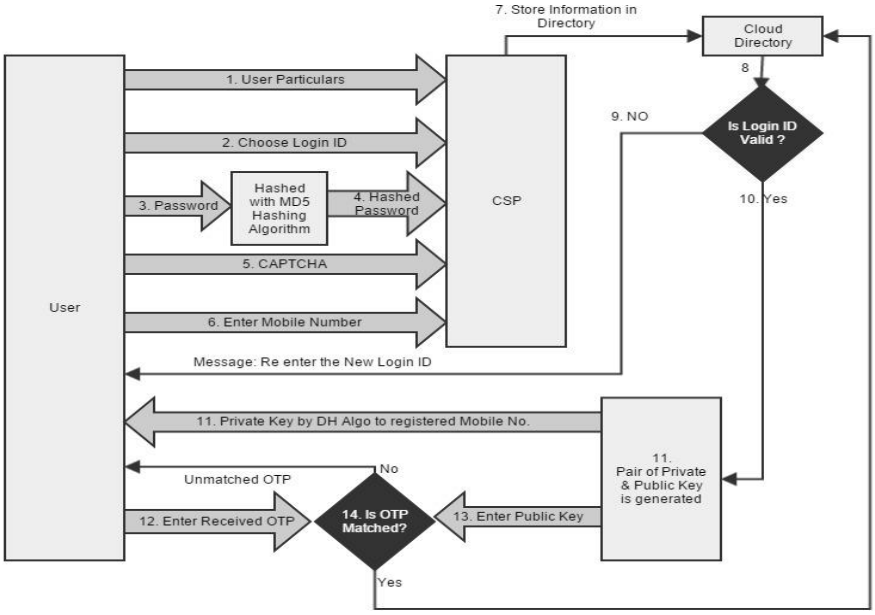

Figure 1.1 - Registration of cloud user to cloud service provider

After verifying the user particulars, the CSP generates an OTP and send it to the cloud user which is reentered by the user and verified by the CSP; this policy prevents the user account from unauthorized person login.

Then users will have to enter a CAPTCHA as well, which make it secure from the software designed for breaking passwords. This concept assures the manual entering of the user data.

1.4.2 Phase 2 (Storing of Data in Cloud Storage)

As expressed in figure 1.2, this phase transmits and store the data securely to the cloud in encrypted form. This phase further divided into three subsections which includes, encrypt information at the user's end, hash code generation and encryption at CSP end.

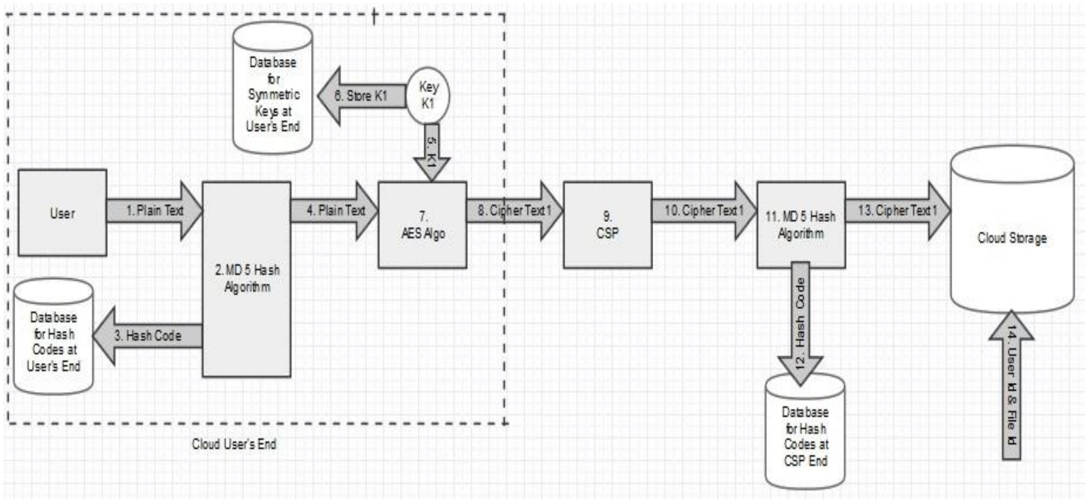

Figure 1.2 - Storing of data in Cloud storage

1.4.2.1 Encryption at User End

After the successful enrollment with CSP, now the data should be transferred to cloud storage. The user encrypts the data by using the AES symmetric key algorithm and stores the generated public key at the user end database itself, against the file ID allotted to an encrypted file. Now plain text will be translated to cipher text 1.

1.4.2.2 Hash Key Generation at User's End

The integrity of the user's data is maintained by generating a hash code at the user's end using the MD5 hashing algorithm and maintained it into a user database against the same file ID. All hash algorithms are one way cryptographic techniques, those generates a hash code which will be altered even one character is modified in the file, which is used to verify the integrity of the data fetched back from cloud storage. This prevents intentional or accidental damage to the data.

1.4.2.3 Hash Key Generation at CSP End

The CSP receives cipher text 1 of the sent file and the integrity of the user's cipher data is again maintained by generating a hash code at the CSP end using the MD5 hashing algorithm and maintained it into a user database against the same file ID. All hash algorithms are one way cryptographic techniques, those generates a hash code which will be altered even one character is modified in the file, which is used to verify the integrity of the data. This prevents intentional or accidental damage to the data.

Now each file stored is encrypted with AES, which counter the drawbacks of the past proposals by several researchers

1.4.3 Phase 3 (User Authentication on Data Retrieval Request)

As shown in figure 1.3, the user has to be authenticated by the CSP before the granting permission for the data retrieval. The user has to pass his login id, password (hashed) and CAPTCHA to the cloud service provider. The CSP matches and verifies the credential passed with the details mentioned in its cloud directory. After verification, the CSP sends an OTP to the user registered mobile number. The user reenters the OTP to the CSP to match it and permit the user access to cloud storage.

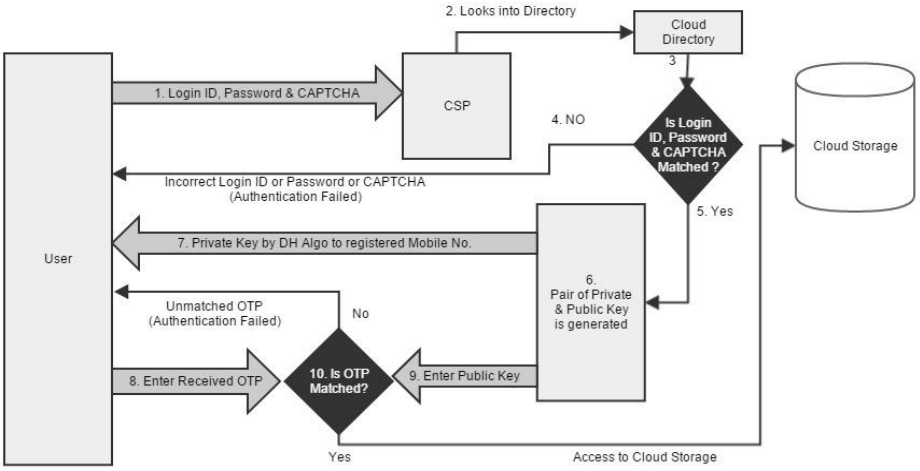
2. Looks into Directory
Cloud Directory
3
User
1. Login ID, Password & CAPTCHA
CSP
4. NO
Is Login ID, Password & CAPTCHA Matched ?
Cloud Storage
Incorrect Login ID or Password or CAPTCHA (Authentication Failed)
5. Yes
7. Private Key by DH Algo to registered Mobile No.
6. Pair of Private & Public Key is generated
Unmatched OTP (Authentication Failed)
No
8. Enter Received OTP
10. Is OTP Matched?
9. Enter Public Key
Yes
Access to Cloud Storage

Figure 1.3 - User's Authentication on data retrieval request

4.3.4 PHASE 4 (RETRIEVAL OF DATA AND INTEGRITY VERIFICATION)

As shown in figure 1.3, the authenticated user transform the fetched cipher text 1 to Plain text by AES symmetric key maintained at user's end database. Then the hash code is generated from the retrieved plain text using the MD5 hashing algorithm and matches it with the stored key values, if matches, then job done, else the CSP is informed of the legal procedure.

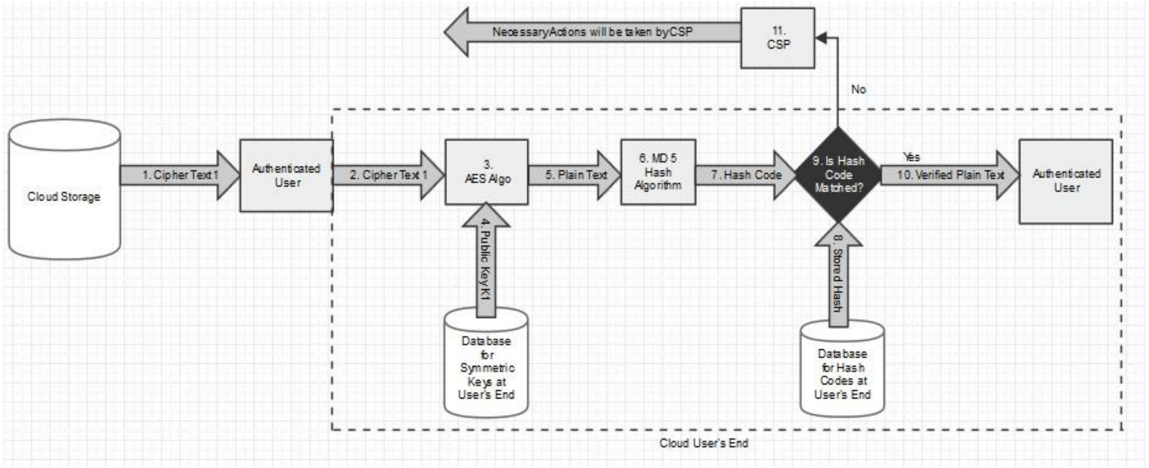

Figure 1.4 - Retrieval of data and Integrity verification

1.5 Security Analysis of the Proposed Model

The proposed algorithm is enough secure, so the cloud user can submit its data to the cloud storage with no issues at all. The proposed algorithm can prevent all these threats and attacks discussed as below

1.5.1 Secure Data in Transit

In the proposed algorithm, even if an unauthorized user will be able to steal the data during transmission, it will be in the form of cipher text 1, which will be of no use in the absence of the public key stored within the authorized user's secure premises and the key breakage will require significant time generally in years.

1.5.2 Secure Stored Data

In the proposed algorithm, even if an unauthorized user will be able to steal the data from cloud storage, it will be in the kind of cipher text 1, which will be of no use in the absence of the public key stored within the authorized user's secure premises and the key breakage will require significant time generally in many years.

1.5.3 Man-In-The-Middle Attack

In the proposed algorithm, even if forged authenticated user will be able to recover the data from cloud storage, it will be in the kind of cipher text 1, which will be of no use in the absence of the public key stored within the authorized user's secure premises.

1.5.4 Side Channel Attack

Since the data from several users share same cloud storage in an insulated environment. This approach is mainly concerned of intentional crossing the boundaries of the own cloud storage to penetrate into some other cloud storage.

In the proposed algorithm, even if an unauthorized user will be able to recover the data from side cloud storage, it will be in the kind of cipher text 1, which will be of no use in the absence of public key stored within the authorized user's secure premises.

1.5.5 Insecure Cryptographic Storage/ Poor Encryption Technology

Since the information is stored in cloud storage in cloud owner control. This approach is mainly concerned of breaking the encryption techniques used.

In the proposed algorithm, even if CSP will steal the data from cloud storage, it will be in the AES encrypted which will secure enough in near future too due to its security strength.

1.5.6 Service or Account Hijacking

In the proposed algorithm, even somehow any mischievous attacker will be able to log in into cloud user account, on feting data from cloud storage it will be in the form of cipher text 1, which will be of no use in the absence of the public key stored within the authorized user's secure premises.

1.5.7 Data Loss and Leakage

Since the information is stored in cloud storage in Cloud owner control. This approach is mainly concerned of intentional stealing the user's information by CSPs itself for some more profit-making use.

In the proposed algorithm, even if CSP will steal the data from cloud storage, it will be in the form of at least cipher text 1, which will be of no use in the absence of the public key stored within the authorized user's secure premises.

1.5.8 Malicious Insiders/ Inside-Job Attack

Since the data is stored in cloud storage in Cloud owner control. This approach is mainly concerned of intentional stealing the user's information by CSPs itself for some more profit-making use.

In the proposed algorithm, even if CSP will steal the data from cloud storage, it will be in the form of at least cipher text 1, which will be of no use in the absence of the public key stored within the authorized user's secure premises.

1.5.9 Authentication Attacks

This attack is mainly concerned about using the credentials of the authorized user to log into his cloud account.

In the proposed algorithm, the introduction of the OTP (one-time password) will run out this attack because only the user with certification and registered mobile number can access the cloud account

1.5.10 DoS (Denial of Service) Attack

In this attack, the attacker injects enormous amount of junk packets into the network which leads to the loss of network resources and causes congestion among the wireless networks. But due to CAPTCHA used, the attack can be prevented.

1.5.11 Dictionary Attacks/ Password Based Attacks

This attack is mainly concerned of using the all possible dictionary words to crack the password of the authorized user to log into his cloud account. But since the password is hashed before sending it through SSL. No such attack is feasible.

1.6 Conclusion

Cloud computing is a model to scale capabilities easily without investing much as in new infrastructure, hiring new personnel or licensing new software. It provides massive storage for data and quicker computing to clients over internet.

It shifts the database and application software to massive cloud data centers, where business data and services may not be completely trustworthy. That's why companies are unenthusiastic to deploy their business data in the cloud even it offers a wide range of luxuries. Security of the data in cloud is one of the key issues which act as barrier in deploying of business data on cloud.

Though cryptographic techniques used are not a magical answer that solves all security, integrity and authentication concerns and also it may not guarantee for 100% accuracy and protection.

It is too early to anticipate where and how the new cloud data attacks and cryptographic techniques would evolve in the future.

1.7 Future Scope

In this algorithm, we have specifically worked on ensuring the security and integrity of the data to be stored in the cloud, but on applying a set of encryption algorithms the encryption and decryption processes will require a lot of time and processing of the data will not be finished in a minimal amount of time. So, that, this research can be further extended for increasing the efficiency of the proposed algorithms.

References

[1] Pritesh Jain, Prof. Vaishali Chourey and Prof. Dheeraj Rane," An Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Real Environment" published in International Journal of advanced Computer Research (IJACR), ISSN (Print): 2249-7277, ISSN (Online): 2277-7970 Volume 1, pp. 23-28, September, 2011.

[2] D. S. Abdul, H. M. Abdul Kader and M. M. Hadhoud "Performance Evaluation of Symmetric Encryption Algorithms" published in Journal Communications of the IBIMA, ISSN: 1943-7765, Volume 8, pp. 58-64, 2009.

[3] Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan Shahi, Ratan Lal "3-Dimensional Security in Cloud Computing" published in IEEE Xplore, 978-1-61284-840-2/11/$26.00 ©2011, pp. 198-201, 2011.

[4] Vadym Mukhin, Artem Volokyta, "Security Risk Analysis for Cloud Computing Systems" The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September, 2011.

[5] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev and Shiv Shakti Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment" published in CSI Sixth International Conference on Software Engineering (CONSEG), Indore, M.P (INDIA), IEEE Xplore, ISBN: 978-1-4673-2174-7, pp. 1 – 8, 5-7 Sept. 2012.

[6] Eman M.Mohamed, Hatem S. Abdelkader and Sherif EI-Etriby "Enhanced Data Security Model for Cloud Computing" published in the 8th International Conference on informatics and Systems (INFOS2012), IEEE Xplore, ISBN: 978-1-4673-0828-1, pp: 12-17, 14-16 May, 2012.

[7] Gurudatt Kulkarni, Jayant Gambhir, Tejswini Patil and Amruta Dongare, "A Security Aspects in Cloud Computing" published in IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS), Beijing, IEEE Xplore, ISBN: 978-1-4673-2007-8, pp. 547 – 550, 2012.

[8] Hyun-Suk Yu, Yvette E. Gelogo, and Kyung Jung Kim "Securing Data Storage in Cloud Computing" published in Journal of Security Engineering, pp 251-260, June-2012.

[9] Singh, A. and Shrivastava, M., "Overview of attacks on Cloud computing" published in International Journal of Engineering and innovative Technology. Volume -1, No. - 4, pp: 321-323, 2012.

[10] Sandeep K.Sood, "A combined approach to ensure data security in cloud computing" published in Journal of Network and Computer Applications (Elsevier), ISSN: 1831-1838, pp. 1831-1838, 2012.

[11] Stolfo SJ, Salem MB, Keromytis AD, "Fog computing: mitigating insider data theft attacks in the cloud" published in the IEEE symposium on security and privacy workshops. IEEE Press, New York, pp 125–128, 2012.

[12] Jingyu Wang and Ruichun Gu, "Cloud Data Security Access with Privacy-Preserving" published in 2014 5th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, IEEE Xplore, ISBN: 978-1-4799-3278-8, pp. 268 – 271, 27-29 June 2014.

[13] Louai A. Maghrabi "The Threats of Data Security over the Cloud as Perceived by Experts and University Students" published in IEEE Xplore Digital Library, ISBN: 978-1-4799-2805-7, pp: 1-6, 18-20 Jan., 2014.

[14] Lekshmy D. Kumar and B.R. Shankar "Security threats to Cloud Computing" published in International Journal of Research in Engineering & Technology, ISSN (E): 2321-8843, 2014.

[15] Mrudula Sarvabhatla, M.Giri and Chandra Sekhar Vorugunti, "A Robust Ticket-Based Mutual Authentication Scheme for Data Security in Cloud Computing" published in IEEE International Conference on Data Science & Engineering (ICDSE), IEEE Xplore, ISBN: 978-1-4799-6870-1, pp. 62-67, August, 2014.

[16] Chaparala Pushya, G Syam Prasad, "Anonymous Authentication of Data Stored in Clouds with Decentralized Security Mechanism" published in International Journal of Science, Engineering and Advance Technology, IJSEAT, Vol.3, Issue 8, ISSN 2321-6905, pp. 351-355, August, 2015

[17] Debasish Jana, Debasis Bandyopadhyay, “Controlled privacy in mobile cloud” published in the IEEE 2nd International Conference on Recent Trends in Information Systems (ReTIS), Kolkata, India. IEEE Xplore DOI: 10.1109/ReTIS.2015.7232860, pp. 98 – 103, 9-11 July 2015

[18] Zhongbin Tang, Xiaoling Wang, Li Jia, Xin Zhang, and Wenhui Man” Study on Data Security of Cloud Computing” published in IEEE Xplore, IEEE: 978-1-4577-1964-6 © 2012 IEEE, 2012.

[19] Chunming Rong, Son.T.Nguyen, and Martin Gilje Jaat un,”Beyond lightning: A Survey on security challenges in Cloud Computing” published in Elsevier Computers and Electrical Engineering, 2012.

[20] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker Siemens, “Understanding Cloud Computing Vulnerabilities”, published in IEEE Journal on Computer and Reliability Societies, Vol. 9, Issue: 2, pp. 50-57, March/April, 2011.

[21] AL-Museelem Waleed, Li Chunlin, Naji, and Hasan.A.H “The faults of Data Security and Privacy in the Cloud Computing” published in Journal of networks, vol. 9, no. 12, pp: 3313-3320, December 2014.

[22] Guoman Lin “Research on electronic Data security strategy based on Cloud Computing” published in IEEE Xplore, ISBN: 978-1-4577-1415-3, pp: 1228-1231, 2012.

[23] D.H. Patil, Rakesh R. Bhavsar and Akshay S. Thorve “Data Security over Cloud” published in proceedings of International Conference on Emerging Frontiers in Technology for Rural Area (EFITRA), pp.11-14, 2012.