An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security

Vikas Goyal and Chander Kant

Abstract Cloud computing is one of the most research hot topics in IT industry nowadays. A lot of startup organizations are adopting cloud eagerly due to massive cloud facilities available with minimal investment; but as every coin has two sides, so with cloud. In the cloud, the user data is stored at some off-site location. So cloud data security is one of the main concerns of any organizations, before shifting to the cloud. The data owners can ensure the data security at its premises using firewalls, VPN (Virtual Private Network) like most used security options. But as data owner stores their sensitive data to remote servers and users access required data from these remote cloud servers, which is not under their control. So storing data outside client premises, raises the issue of data security. Thus, one of the primary research areas in cloud computing is cloud data protection. In this research paper, strategies followed include categorization of the data on the basis of their sensitivity and importance, followed by the various cryptography techniques such as the AES (a Symmetric Cryptography technique), SHA-1 (a Hashing technique), and ECC (Elliptic curve Cryptography (an Asymmetric Cryptography technique). Till date, most of the authors were using a single key for both encryption and decryption which is a weak target of various identified malicious attacks. Hence, in the designed hybrid algorithm, two separate keys are used for each encryption and decryption. The cloud user who wants to access cloud data, need to first register with CSP and cloud owner. After registration, user login id, password and OTP (One Time Password) sent to the user registered mobile number, are required to access the encrypted cloud data.

Keywords Cloud · Data security · ECC · AES · SHA-1 · Hybrid algorithm for cloud data security

V. Goyal (✉)
NIT, Kurukshetra, India
e-mail: vikas.goyal_85@yahoo.co.in

C. Kant
Department of Computer Science and Application, Kurukshetra University, Kurukshetra, India
e-mail: ckverma@rediffmail.con

V.B. Aggarwal et al. (eds.), *Big Data Analytics*, Advances in Intelligent Systems and Computing 654, https://doi.org/10.1007/978-981-10-6620-7_20

1 Introduction

Cloud storage mainly maintains user's data on an off-site cloud storage system that is maintained by third-party CSP. Nowadays, owner prefers to store their data on cloud due to facilities provided by cloud vendors instead of storing data on users' system hard disk or other memory devices at their own premises. After storing the owner data on a remote database, it will be accessible later through just an internet link between user and cloud databases. In cloud model, customers are associated with cloud through an internet link to access cloud information and resources are priced and provided, on-demand. Mainly, cloud resources are shared among multiple users as office, apartments or storage places as shared among tenants. The cloud facilities are primarily delivered through an internet link, thus the cloud user is free from the worry of maintaining own data center or servers (as shown in Fig. 1). Nowadays, mostly adopted cloud computing services are offered and maintained by big IT giants Amazon and Google for the startup companies.

There are mainly three components of cloud computing model as listed below.

Cloud service provider (CSP)—The third-party vendor which manages all the cloud services, i.e., infrastructure, platform, and the software's offered to cloud users with his technical team. He is completely responsible for providing safe and uninterrupted services to the cloud users.

Client/Owner: An entity, which is generally, an individual or startup organizations, who want to store their large data files either at own premises or in the cloud.

User: An entity enrolled with the data owner and access owners' cloud data after proper authentication from CSP.

Since data is one of the crucial outsourced entity in cloud computing, thus it may suffer from various threats or attacks by exploring the vulnerabilities present in the outsourcing cloud module. The attackers can be an Insider (CSP or CSP employee itself) or Outsider (some mischievous hacker) who desires to access the owner data, which can be utilized for some gain thereafter.

As the data is one of the most critical assets for any company or data owner, thus, whatever sort of threats to the security and integrity of data can lead to horrific consequences for organizations. So as discussed, cloud data security is the main hurdle in adopting cloud services for most of the organizations. If the data security,

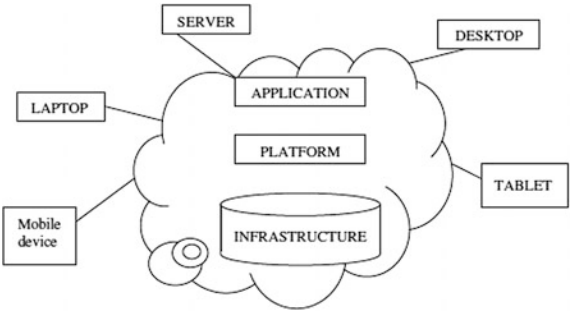

Fig. 1 The cloud

integrity issues will be properly addressed and audited, more data owners, and organizations will switch to cloud storage. One more issue which is to properly address is, resource sharing, such as storage, with other cloud users and CSP (Cloud Service Provider). Thus, if the rival cloud users are sharing the same cloud storage space from same CSP, then their data may be under threat from each other. Thus, it is also the CSP responsibility to isolate one users' data from some other.

The proposed hybrid model comprises of different well-known cryptographic techniques and applying them together to achieve cloud data protection. The paper's propose a hybrid algorithm comprising of three different encryption techniques which efficiently protect the three categories of data throughout the data life cycle, i.e., from the owner to the cloud and then to the end cloud user. As the cloud is combinations of dissimilar resources placed together to offer the services, and so a bunch of vulnerabilities may exist in cloud setup, whose exploration may be horrific for the cloud data storage. The proposed hybrid algorithm uses encryption as a primary security policy. Encoding is the technique for alteration of plain text data in an encrypted form called cipher text that can be deciphered and read by the legitimate person having a valid decryption key only. The illegitimate or mischievous person cannot easily decrypt and interpret the ciphertext in the absence of the decryption key.

This rest of the paper is designed as follows: Sect. 2 highlights the various authors' related work regarding cloud data protection in the last years. In Sect. 3, effective hybrid model is designed to address and solve cloud data storage security issue effectively. Section 4 provides the proposed algorithm. Section 5 provides the security investigation of the proposed hybrid model against various identified attacks so far. Section 6 provides the conclusion and future scope of this paper.

2 Related Work

We have gone through some research papers to identify security issues with existing cloud data storage models and the presented solutions so far. Among them, few research efforts are handled directly with the topics of security and privacy-aware data stored in cloud computing.

The Cloud Security Alliance (CSA) [1] and Louai et al. [2] has risen seven security threats to cloud data storage, those are, exploitation of cloud Computing, vulnerable Application Programming Interfaces (APIs), malicious entity insider, shared technology security issues, information leakage, account or service accessing by an illegitimate user, etc.

Louai et al. [2], Singh et al. [3] and Yu et al. [4] has identified many issues, loopholes and attacks to data's security, integrity, and confidentially over the cloud data storage. The attacks studied include Denial of Service (DOS) attack, cloud malware injection attack, side channel attacks due to shared infrastructure, authentication attack, and man-in-the-middle attack. Yu et al. [4] have concluded

that data integrity can be ascertained by the simply SSL protocol during transmission.

Karthik et al. [5] have suggested a new hybrid algorithm using some well-known cryptographic algorithms in a definite array, to enhance and optimize cloud data protection.

Li et al. [6] have presented a hybrid encryption algorithm contains a simple encryption algorithm, which improved to the Vigenere encryption algorithm; and finally, came out with a hybrid encryption algorithm with a Base64 encoding algorithm. The proposed hybrid encryption algorithm significantly improved the data protection.

Tweney et al. [7] have mentioned an incident, back in 2007, from the end of CSP Salesforce.com which sent a letter to all its millions of subscribers demonstrating about how the customer emails, addresses, and rest particulars had been stolen by cybercriminals.

Tang et al. [8], Rong et al. [9], Grobauer et al. [10], Waleed et al. [11], Lin [12] have highlighted the vulnerability of the data security in the cloud, one of the important factors restricting the growth of cloud computing and reviewed the threats to security and privacy of cloud data warehousing.

Divya et al. [13] have proposed a secure cloud storage algorithm using elliptic curve cryptography. The proposed work also concentrates on Online Alert methodology which shows the data owner when an aggressor attempts to alter the data or any malpractice happens during data forwarding.

Kumar et al. [14] have researched elliptic curve cryptography (ECC) encryption technique in particular used for protecting cloud data files which authenticate the legitimate user and refuse the data accessing by mischievous hacker or cloud storage provider.

Fu et al. [15] have focused on safe data deletion on the file systems. The report proposed a file system which supports secure deletion of data. This paper proposed the idea of secret code text-policy trait-based encryption technique (CP-ABE) which supports fine-grained access policy to encrypt files.

Tan et al. [16] have proposed a cloud data security algorithm using fully homomorphic encryption to ensure data protection during both during transmission and storage. The full homomorphic encryption algorithm can process the encrypted data as well.

Sinha et al. [17] has compared the functioning of two asymmetric key encryption algorithm between RSA and ECC experimentally; and concluded that ECC performs better in many respects required key sizes, bandwidth saving, encryption time, small device's efficiency, as well as security as compared to RSA algorithm.

Abdul et al. [18], Pavithra et al. [19] have implemented six most used symmetric key encryption algorithms: DES, 3DES, AES (Rijndael), Blowfish, RC2, and RC6 and comparison was conducted based on several parameters. The report concluded that the AES algorithm is competitive with the rest of algorithm on being fast and flexible.

Marshall et al. [20] have designed a hybrid encryption model by using RSA and AES algorithms to ensure cloud data protection. Since the private key is exclusively

in user hold and therefore the user's most sensitive will not be useful to anyone except the legitimate user not even the CSP.

Tripathi et al. [21] have given a comparative work between two well-known asymmetric encryption algorithms between elliptic curve cryptography and the RSA cryptography algorithm in respect of the cloud data security parameter. The paper flared up with experimental results which prove the superiority of elliptic curve-based public key cryptography compared to RSA public key cryptography.

Mohamed et al. [22] have suggested Amazon EC2 cloud users, to must use an AES symmetric algorithm which ensures the highest security with minimum time to code.

Dinadayalan1 et al. [23] have proposed all the principal data security issues and their solutions.

3 Proposed Model

The main focus of this algorithm is to maximize the data owner's control of data during transit as well as storing. Since more locks, we will apply the more time it will take to fetch the data back. So it would be better to categorize the data first. Since all data is not of the same importance, so we can categorize the data initially on the basis of their sensitivity and importance. To achieve the 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 Three-Tier Privacy-Aware Cloud Computing Model is proposed for the three categories of the data described as below

- No Privacy (NP)
- Privacy with Trusted Provider (PTP)
- Privacy with non-trusted provider (PNTP)

There are no encryption and decryption used for the storage and accessing of No Privacy (NP) category data, whereas in Privacy with trusted provider (PTP) security scheme the CSP is responsible and trusted to maintain the data security. CSP uses the AES encryption and decryption technique which automatically generate the public key which is known to everyone. Now in the third case, i.e., Privacy with non-trusted provider (PNTP) for the most sensitive data to work upon, a security scheme is proposed. In this security scheme, both data owners (user) and CSP are responsible to ensure cloud data protection. User encrypts the information using AES algorithm before sending to CSP, then CSP again uses the ECC encryption and decryption technique for complete data protection. In this paper, we have described a security scheme for PNTP module only.

The proposed hybrid algorithm comprises of different coding techniques such as AES (Symmetric Cryptography technique), SHA-1 (Hashing technique), and ECC

(Elliptic curve Cryptography, Asymmetric Cryptography technique) for the categorized sensitive data.

The proposed hybrid algorithm is designed to offer complete data security to the data throughout the data life cycle, such as to data in transit, data in storage, etc. To reach this level of assurance, multiple combinations of the encryption techniques are taken to protect vital and sensitive data from mischievous users. The proposed algorithm is categorized into five phases. The data owner who wants to store data in the cloud is first registered with CSP in the first phase of the algorithm. The data is categorized on the basis of its sensitivity and stored in cloud storage in the second phase. The user who wants to recover the data from cloud undergoes the authentication process in the third phase. The auditors at CSP can verify the data integrity of cloud data in the fourth phase. It is required for SLA assurance and archived information. After passing valid authentication process, the user is allowed to retrieve the cloud data and verify the integrity of the fetched data, to provide proper feedback to the CSP about fetching data in the fifth phase.

3.1 Phase 1 (Registration of Data Owner to CSP)

Foremost of all, the user who wants to get the services of cloud storage, will have to register with the cloud service provider. The user requires to enter his particulars, valid username, password, and mobile number. The particulars and username are stored as such at CSP end. But the password is concatenated by the SALT, which increases password security by concatenating a random string to the password entered by the registered users. After Salting password is hashed using SHA–1 hashing technique and output hash code (512 bits) will be sent to the CSP. The concatenation of the SALT will prevent the dictionary attacks, SQL injection attacks and hash code of the salted password will prevent the CSP or unauthorized individual to steal user credentials from cloud storage (as shown in Fig. 2).

After verifying user's credentials and password, the CSP generates an OTP and send it to the user registered mobile number supplied during the registration procedure. The user is supposed to enter sent OTP to the CSP for completing the certification process; CSP matches it with the OTP generated and thus verify the mobile number if matched else refuse the registration procedure.

3.2 Phase 2 (Storing of Data in Cloud Storage)

After successfully completing the registration process, the data is categorized on the basis of its importance and sensitivity. The data are transmitted to the CSP through various steps in a data storing process described in subsections from 3.2.1 to 3.2.4 which provide a stepwise description of all activities done on the data (as shown in Fig. 3).

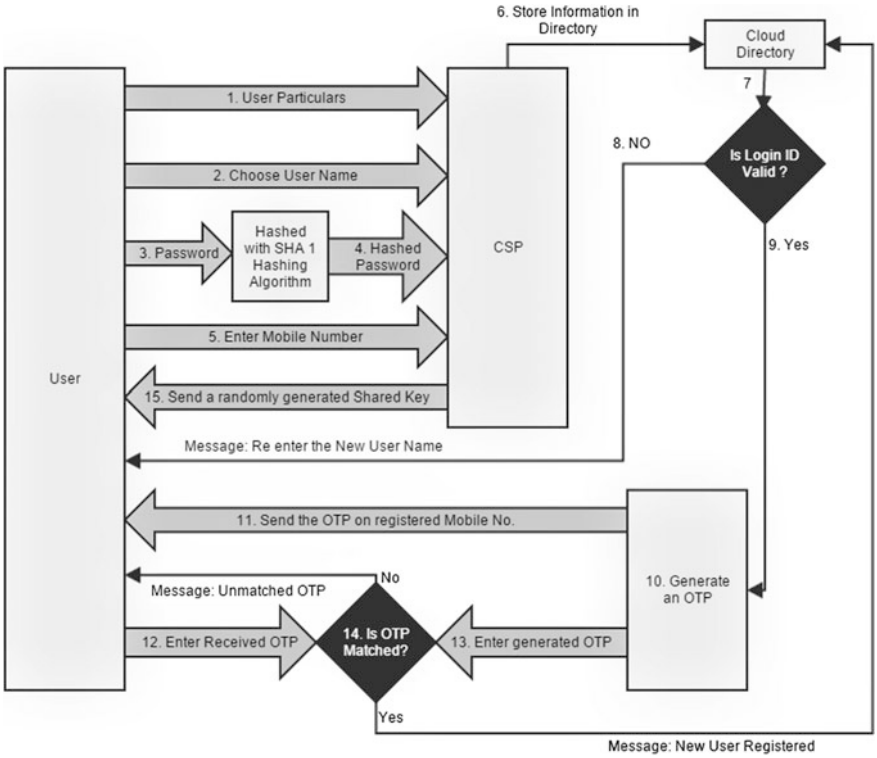

Fig. 2 Registration of cloud user to cloud service provider

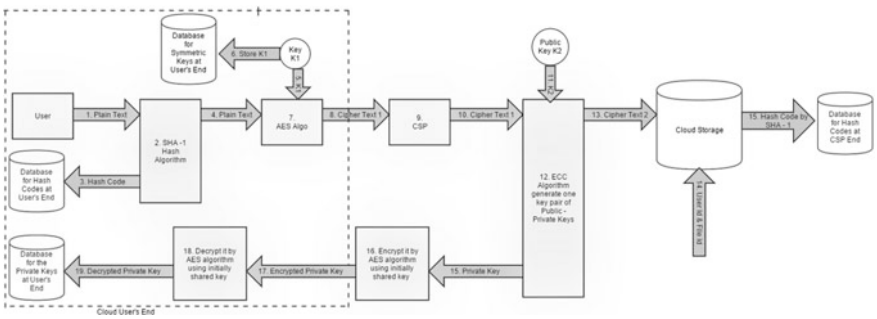

Fig. 3 Storing of data in cloud storage

3.2.1 Encryption at Cloud User (Owner) End

As soon as the user is registered with CSP, he is allowed to store the data in cloud storage. Only instead of sending plain text of PNTP category data directly to CSP, it

is first encrypted with a symmetric encryption algorithm AES (advanced encryption algorithm) to avoid the man-in-the-middle attack, insider job attack, etc. The single key generated by AES algorithm is kept in the data owner's database for the future decryption. Thus, the plain text is first encrypted into cipher text 1, for storage to the CSP. The AES algorithm is secure enough in the today scenario because there is no known attack on the AES algorithm till date.

3.2.2 Hash Key Generation at Cloud User's End

The data integrity assurance is another required feature of the proposed algorithm. Thus to ensure user's data integrity, a hash code is generated at the user's end using a SHA-1 hashing algorithm. The hash code generated is kept up at the user's end database for integrity verification later on. The SHA-1 algorithm is a unidirectional cryptographic technique, which gets a hash code which will be changed even after a minor change in the data and then it will be used to verify the integrity of the information. Then the user will be ascertained that neither CSP nor any unauthorized individual has altered the data stored in cloud storage.

3.2.3 Encryption at CSP End

On receiving the cipher text 1 from the user, the CSP applies another very strong asymmetric key cryptographic technique ECC (Elliptic Curve cryptography). In this cryptographic asymmetric algorithm, a pair of public and private key is generated.

The received cipher text 1 is again encrypted with the generated public key and the paired private key is sent back to the legitimate user by encrypting it with the AES encryption algorithm through initially shared a key which is maintained by the user in its database in a secured way. That's how the data can be only unlocked by the authenticated user with the appropriate private key.

Since the information stored is encrypted two times back to back with strong algorithms which eliminate the loopholes of the past researchers' proposals. The double encryption is must since the data are always vulnerable to the unethical CSPs.

3.2.4 Hash Key Generation at CSP End

To maintain the integrity of the user's data, the CSP also generates a hash code at the CSP end using a SHA-1 hashing algorithm and maintain it in its database. Thus, it can be used later during routine auditing at the CSP end by matching the generated hash code. Then that user will be ascertained that neither CSP nor any unauthorized individual has altered the data in cloud storage stored for a long time.

3.3 Phase 3 (User Authentication on Data Retrieval Request)

This phase deal with the user authentication process for data retrieval from cloud storage. The user enters his login ID and password to CSP who in turn verify the entered credentials. After verifying the user credentials and password, the CSP generates an OTP, and send it to the user registered mobile number supplied during the enrollment procedure. The user is supposed to enter sent OTP to the CSP for completing the certification process; CSP matches it with the OTP generated, and thus verify the mobile number if matched else refuse the data recovery requests (as indicated in Fig. 4).

3.4 Phase 4 (Auditing at Cloud End)

This phase is mainly concerned with the auditing at the CSP end. Since the information stored by the user may not be required of him for a long time, so that to avoid the tempering of the data, one hash code of cipher text 2 is also maintained at the CSP end by SHA–1 hash algorithm. So that during regular auditing the CSP end, the tempering of the data can be distinguished and the proper message will be given to cloud user or data owner. This phase also ensures the SLA (service level agreement) between user and CSP.

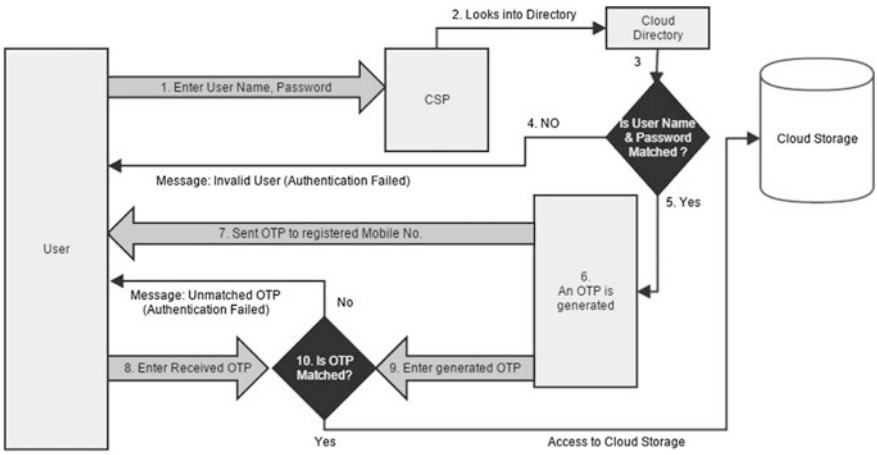

Fig. 4 User's authentication on data retrieval request

3.5 *Phase 5 (Retrieval of Data and Integrity Verification)*

In this phase, the authenticated user retrieves, convert to plain text, and verify the integrity of data. As shortly as the user is authenticated, he is permitted to access the cloud storage and brings in the required data present in cipher text 2 forms and carries it to its own premises to convert plain text mode (as indicated in Fig. 5).

This phase is further categorized into three Sects. 3.5.1 to 3.5.3 providing stepwise actions performed on data. Since all these steps performed on user's premises, then there will be no security breaches.

3.5.1 Private Key Decryption

First, the cipher text 2 is decrypted with the private key generated by ECC algorithm and stored in the user database to convert the retrieved data in cipher text 1 form.

3.5.2 Public Key Decryption

Second, the received cipher text 1 is further decrypted with the public key of the AES algorithm stored in the user database to change the data from cipher text 1 form in plain text configuration.

3.5.3 Hash Code Verification

To verify the integrity of the retrieved data, the user again generates a hash code for the transformed plain text using the SHA-1 algorithm. The generated hash key will be compared with the hash value stored in the database at owner end. If matches the integrity of the information is verified else the problem is reported to be CSP which can result into and legal process against CSP. That's how the user will be ascertained that neither CSP nor any unauthorized individual has altered the data stored in cloud storage.

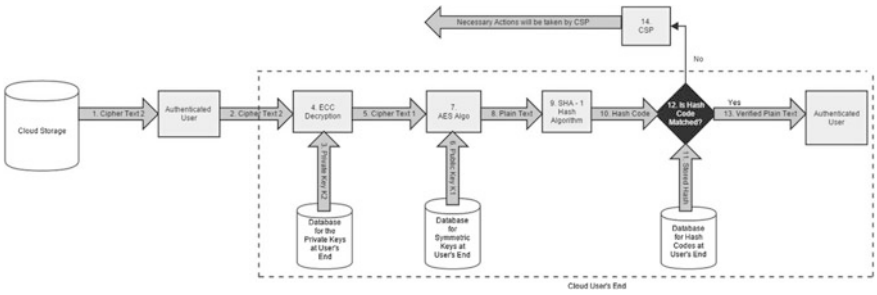

Fig. 5 Retrieval of data and integrity verification

4 Algorithm

Step 1: Registration of the user with CSP
(a) Enter User Particulars,
(b) Choose USER_Name, PWD
(c) Enter M_Number
Step 2: if (USER_Name is valid) then
(a) Generate a random key Rkey at CSP end and send it to user
(b) Generate an OTP at CSP end
(c) UserOTP ⟵ CSPOTP
(d) Enter the User OTP received on user registered mobile
(e) if (Entered OTP == CSPOTP) then
(i) Message: New User is registered
(ii) go to step 3
else
(i) Message: Unmatched OTP & registration is canceled
(ii) go to step 10
else
(i) Message: Invalid USER_Name, Choose some other USER_Name
(ii) Go to step 2
Step 3: Selecting the category of the data
(a) Based on the sensitivity of the data FPFID, categorize it into following categories
(i) NP (No Privacy) – Mainly Public Data so no encryption is required
(ii) PTP (Privacy with Trusted Provider) – Data with little importance and the trusted CSP is allowed to store it into encrypted mode
(iii) PNTP (Privacy with NON Trusted Provider) – Data with more sensitivity and importance and the encrypted data is sent to non trusted CSP which again store it into encrypted mode
Step 4: Uploading of user file to CSP
(a) Select file FP in Plain text mode & assign a unique file ID FID
(b) δ_{pc} = Privacy Category of file FPFID
Step 5: if δ_{pc} = NP then
(a) Send (FPFID, NP, USER_ID) to CSP via SSL
(b) Store in CSP storage with replication factor 3 in plain text form.
Step 6: if δ_{pc} = PTP then
(a) Send (FPFID, PTP, USER_ID) to CSP via SSL
(b) Generate a symmetric key CSPpub1 at CSP end
(c) CSP_FCFID ⟵ Encrpt_AES (FPFID, FID, CSPpub1)
(d) Store CSPpub1 at CSP end database.
(e) Store CSP_FCFID at CSP storage with replication factor 3
Step 6: if δ_{pc} = PNTP then
(a) Generate a Hash code for the file
HCFID ⟵ HASH CODE_SHA1 (FPFID, FID)
(b) Generate a symmetric key USERPub for FID by AES algorithm
FC1FID ⟵ Encrpt_AES (FPFID, FID, USERPub)
(c) Store HCFID and USERPub in User's Database
(d) Send (FC1FID, User_ID) to CSP via SSL
(e) Generate a Public – Private key pair CSPPr and CSPPub2by ECC asymmetric algorithm
(i) FC2FID ⟵ Encrypt_ECC(CSPPub2, FC1FID, User_ID)
(ii) Generate a Hash code for the file FC2FID
CSP_HC_FC2FID ⟵ HASH CODE_ SHA1 (FC2FID, FID)
(iii) Store CSP_HC_FC2FID at CSP end for Auditing
(iv) Store FC2FID and δ_{pc} at CSP storage with replication factor 3
(v) Send ECC private key back to the user
ECSPPR ⟵ Encrpt_AES(CSPPr, Rkey)

(vi) CSPPr ⟵ Decrpt_AES (ECSPPr ,Rkey)
(vii) Store CSPPr in User's Database

Step 7: User's Authentication Request to CSP
(a) Enter USER_Name, PWD
(b) if (USER_NAME is valid? && Password matched?) then
(i) Generate an OTP at CSP end
(ii) UserOTP ⟵ CSPOTP
(iii) Enter the User OTP received on the user registered mobile
(iv) if (Entered OTP == CSPOTP) then
1. Message: Cloud access is allowed
2. Send USER_ID to CSP
3. go to step 8
else
1. Message: Unmatched OTP & login is canceled
2. Exit
else
(i) Message: Invalid User Credentials, Re enter the correct credentials
(ii) go to step 7

Step 8: Data retrieval and verification Process
(a) CSP will list all users' file against that USER_ID
(b)The user will opt FC2FID with its privacy category δ_{pc} from the list
(c) if (δ_{pc} == NP) then
(i) CSP will send the file (FPFID, USER_ID) to user via SSL
(d) if (δ_{pc} == PTP) then.
(i) At CSP end, the encypted file is decypted
FPFID ⟵ Decrpt_AES
(CSP_FCFID, FID, CSPpub1)
(ii) CSP will send the file (FPFID, USER_ID) to user via SSL
(e) if (δ_{pc} == PNTP) then
(i) (FC2FID, USER_ID) will be sent back to user via SSL
(ii) FC1FID ⟵ Decrypt_ECC(CSPPr, FC2FID, User_ID)
(iii) FP FID ⟵ Decrpt_AES (FC1FID, USERPub, FID)
(iv) NEW_HCFID ⟵ HASH CODE_ SHA1 (FPFID, FID)
(v) if (NEW_HCFID == HCFID) then
1. Message: File is retrieved successflly
2. Send ACK to CSP
3. go to step 10
else
1. Message: File is Corrupt
2. Send NAK to CSP and start legal procedure
3. go to step 10

Step 9: Auditing at CSP End
(a) Generate a New Hash code for the file FC2FID
(i) NEW_CSP_HC_FC2FID ⟵ HASH CODE_SHA1(FC2FID, FID)
(ii) if (NEW_CSP_HC_FC2FID == CSP_HC_FC2FID) then
1. Message: File is verified
2. Send Positive Report to User else
1. Message: File is Corrupt
2. Send Negative Report to User and start a legal procedure

Step 10: EXIT

5 Security Analysis of Proposed Model

Designed and implemented algorithm is secure enough against most of the identified attacks, so that the data owner or organizations can store their data to the cloud storage with no worries at all. The proposed hybrid solution can prevent all these attacks described as:

5.1 Brute Force Attack

This attack is mainly concerned about using every possible combination of the key to crack the actual key.

In the proposed algorithm, the introduction of the AES encryption algorithm will fail this attack because only the cracking of AES—256 require about 2^{255} combination, which is not feasible in real time even by using fastest super computer available in today's scenario.

5.2 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 fail this attack because only the user with credentials and registered mobile number can access the cloud account.

5.3 Dictionary Attacks

This attack is mainly concerned about using all the possible dictionary words to crack the password of the authorized user to log into his cloud account.

In the proposed algorithm the introduction of the saltiest, the concatenation of an arbitrary string in the user password secures it from being error-prone to a dictionary attack.

5.4 Man-in-the-Middle Attack

This attack is mainly concerned about being a forged authenticated user for the data retrieval from cloud storage.

In the proposed algorithm even if an unauthorized user will be able to retrieve the data from cloud storage, it will be in the form of cipher text 2, which will be of no use in the absence of the private key and public key stored within the authorized user's secure premises.

5.5 Cloud Malware Injection

This attack is mainly concerned with introduction of a suspicious malware in the cloud itself so that cloud data can be retrieved from cloud storage without the permission of cloud user and CSP.

In the proposed algorithm even if an unauthorized user will be able to retrieve the data from cloud storage, it will be in the form of cipher text 2, which will be of no use in the absence of the private key and public key stored within the authorized user's secure premises.

5.6 Side Channel Attack

Since the data from various users share same cloud storage in an isolated environment. This attack 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 retrieve the data from side cloud storage, it will be in the form of cipher text 2, which will be of no use in the absence of the private key and public key stored within the authorized user's secure premises.

5.7 Inside-Job Attack

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

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.

5.8 SQL Injection Attack

This attack is one of the many web attack mechanisms used by hackers to steal data from organizations by using simple SQL commands.

In the proposed algorithm, salting to the password and adding hashing to the salt as well as the OTP concept makes SQL injection attack nearly impossible.

So the proposed algorithm is enough to secure to handle all the main concerned of a cloud user. So the cloud user now can submit its data to the cloud storage with no issues.

6 Conclusion and Future Scope

As discussed earlier, a lot of the startup organizations are adopting cloud eagerly due to huge cloud facilities with minimal investment. Apart from it, cloud data security is one of the main concerns of the organizations, before adopting cloud.

This paper designed and implemented a new hybrid algorithm for securing cloud data using three different security policies for three different types of sensitive data to maximize control of data owner on storing, processing and accessing on it. The proposed hybrid algorithm is found to be highly secure for all types of sensitive data cloud environment.

In future, the algorithm can be tested against the various security attacks practically, the concept can be checked for efficiency and work can be extended to minimize the required time for all processing, even the concept can be combined with biometric traits those can be used for generating keys for encryption and decryption processes to gain an edge in the field of cloud storage.

References

1. Cloud Security Alliance “Top Threats to Cloud Computing” published in USA: Cloud Security Alliance, (2010)
2. Maghrabi, L.A.: The threats of data security over the cloud as perceived by experts and university students. University of the West of England, Bristol, United Kingdom (2013)
3. Singh, A., Shrivastava, M.: Overview of attacks on cloud computing. Int. J. Eng. Innovative Technol. **1**(4), 321–323 (2012)
4. Yu, H.S., Gelogo, Y.E., Kim, K.J.: Securing data storage in cloud computing. J. Secur. Eng. 251–260 (2012)
5. Nandakumar, K., Jain, A.K., Pankanti, S.: Fingerprint-based fuzzy vault: implementation and performance. In: IEEE Transactions on Information Forensics and Security, Vol. 2, no. 4 (2007)
6. Li, X., Yu, L., Wei, L.: The application of hybrid encryption algorithm in software security. 978-1-4799-2860-6, IEEE, (2013)

7. Tweney, A., Crane, S.: Trust guide: An exploration of privacy preferences in an online world. In: Expanding the Knowledge Economy Applications Case Studies. IOS Press, Amsterdam (2007)
8. Tang, Z., Wang, X., Jia, L., Zhang, X., Man, W.: Study on data security of cloud computing. IEEE Xplore: 978-1-4577-1964-6 © 2012 IEEE, pp. 1–3 (2012)
9. Rong, C., Nguyen, S.T., JaatUN, M.G.: Beyond lightning: A Survey on security challenges in cloud computing. In: Elsevier Computers and Electrical Engineering. pp. 47–54 (2012)
10. Grobauer, B., Walloschek, T., Stöcker Siemens, E.: Understanding cloud computing vulnerabilities. IEEE J. Comput. Reliab. Socities **9**(2), 50–57 (2011)
11. Waleed, Al.W., Li, C., Naji, H.A.H.: The faults of data security and privacy in the cloud computing. J. Netw. **9**(12), pp. 3313–3320 (2014)
12. Lin, G.: Research on electronic Data security strategy based on cloud computing. In: IEEE Xplore: 978-1-4577-1415-3 ©2012 IEEE, pp 1228–1231 (2012)
13. Divya, S.V., Dr.Shaji R.S.: Security in data forwarding through elliptic curve cryptography in cloud. In: 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 978-1-4799-4190-2 ©2014 IEEE, pp. 1083–1088 (2014)
14. Kumar, A., Lee, B.G., Lee, H.J., Kumari, A.: Secure storage and access of data in cloud computing. ICTC 2012, IEEE Xplore: 978-1-4673-4828-7 ©2012 IEEE, pp. 336–339 (2012)
15. Fu, Z., Cao, X., Wang, J., Sun, X.: Secure storage of data in cloud computing. In: 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE Xplore: 978-1-4799-5390-5 © 2014 IEEE, pp. 783–786 (2014)
16. Tan, Y., Wang, X.: Research of cloud computing data security technology. In: IEEE Xplore: 978-1-4577-1415-3 © 2012 IEEE, pp. 2781–2783 (2012)
17. Sinha, R., Srivastava, H.K., Gupta, S.: Performance based comparison study of rsa and elliptic curve cryptography. Int. J. Sci. Eng. Res. ISSN 2229–5518, **4**(5), 720–725 (2013)
18. Abdul, D.S.H., Abdul Kader, M., Hadhoud, M.M.: Performance evaluation of symmetric encryption algorithms. J. Commun. IBIMA, ISSN: 1943–7765, **8**, 58–64 (2009)
19. Pavithra, S., Ramadevi, E.: Performance evaluation of symmetric algorithms. J. Global Res. Comput. Sci. ISSN 2229-371X, **3**(8), 43–45 (2012)
20. Mahalle, V.S., Shahade, A.K.: Enhancing the data security in cloud by implementing hybrid (RSA & AES) Encryption Algorithm. IEEE 978-1-4799-7169-5 ©. (2014)
21. Tripathi, A., Yadav, P.: Enhancing security of cloud computing using elliptic curve cryptography. Int. J. Comput. Appl. ISSN: 0975–8887, **57**(1), pp. 26–30 (2012)
22. Mohamed, E.M., Abdelkader, H.S., EI-Etriby, S.: Enhanced data security model for cloud computing. In: 8th International Conference on informatics and Systems (INFOS2012), pp. 12–17 (2012)
23. Dinadayalan1, P., Jegadeeswari, S., Gnanambigai, D.: Data security issues in cloud environment and solutions. In: 2014 World Congress on Computing and Communication Technologies, IEEE Xplore: 978-1-4799-2876-7 © 2013 IEEE, pp. 88–91 (2013)
24. Daemen, J., and Rijmen, V.: Rijndael: the advanced encryption standard. Dr. Dobb's J. 137–139. (2001)