Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments

Naveen N, K.Thippeswamy

Abstract*: Among multifaceted useful services offered by Information Technology, the launch of Cloud Computing environment is one of types. But the issues and drawback of cloud computing being that the parameters related to privacy and securities are questionable and pose a threat. Reportedly, because of security issues, there occurs fewer business oriented and real time cloud applications in comparison to applications that are consumer based. Concerning this, providing security and privacy from doubtful vendors also pertaining the cloud manager and service provider is of prime importance. Besides it's also needed to offer real time query outcome to all the authorized users. In this research suggests to the approach of Multi-layer Encryption techniques in cloud computing thus enhancing the security parameters concerning sensitive data Thus with layer ways Encryption technique the data in cloud server can be made more secured with better privacy. Resultant both cloud side and owner of the data gain enhanced security. According to this encryption technique if data-owner's authorization is not granted then the users are restricted from the data access. The strategies proposed are, Symmetric encryption method of the advanced encryption standard (AES) and Asymmetric encryptions method of the Rivest-shamir Adleman (RSA). The cloud applications that are critical can be benefitted from the above suggested algorithm which claims to be simple and efficient. In Symmetric encryption process a single unique key ought to be shared between users who are bound for message receiving whereas in asymmetrical encryption process the encryption and decryption of messages during communication is achieved using both of private and public key. Later the feasibility analysis is carried for above two encryption algorithms responsible for privacy and security of data relating by way of rest of the algorithms.

Index Terms*: Cloud computing, Advanced Encryption Standard (AES), Rivest-shamir Adleman (RSA), Asymmetric encryptions, Symmetric encryptions, feasibility, Multi-layer encryption, Decryption, Privacy, Security.

I. INTRODUCTION

With the introduction and benefits of Cloud Computing technology abundant data storage is possible by outsourcing any amount of data on explicit cloud servers. Granting data security remains a major concern in cloud computing as the data is prone to access and threat by cyber criminals. Cloud storage makes use of third party software for storing necessary records, files and data making security of data as of prime concern. The concept of cloud Storage involves storage of data received from any individual or firm that is made accessible from a cloud of various connected and distributed resources. Here comes the necessity of authenticating the stored data for providing protective communication across connected and distributed resources. The present paper focuses on managing data or file's privacy and security concerning unreliable parties of criminals, hackers and attackers. Digitalized data is usually stored by the user on cloud, accessing it when the need occurs hence authorization of such data becomes mandatory.

Cloud Computing implements various techniques for securing of its data, two of such algorithms are steganography and attacks cryptography. The cloud suffers from vulnerability because of numerous dynamic factors and huge attack surface. On one end the cyber criminals invent different strategies for attack while at the other end researchers put effort in building up preventive measures against vulnerabilities. Being aware of the new risks and attacks associated with security the policy must also be timely and frequently updated. Primarily the risk of attack is confronted by cloud service provider and the cloud manager. In the threat to predict the attacks of cloud based on a multi-layer security algorithm is used.

The prime focus being managing data or file's privacy and security concerning unreliable parties of criminals, hackers and attackers alongside risk associated with cloud manager and cloud service providers. Also the focus extends to granting real time query output to authorized users. In this paper proposed approaches of Multi-layer Encryption Approaches for increase security of sensitive data in cloud computing. To achieve the data security and privacy on cloud server, in proposed Multi-layer encryption methods. Thus with Multi-layer ways Encryption technique the data in cloud server can be made more secured with better privacy. Resultant both cloud side and owner side from data gain enhanced security. According to this encryption technique if data-owner's authorization is not granted then the users are restricted from the data access. The approach makes use of Symmetric encryption scheme of the advanced encryption standard (AES), analyzing various processes and security parameters responsible for the designing and implementation of popular and known symmetric encryption algorithm namely Advanced Encryption Standard. Advanced Encryption Standard (AES) acts as a block cipher related symmetric-key cryptography safeguarding sensitive data. AES key sizes are being 128, 192, 256 bits. Substitution-Permutation technique is the one on which AES relies upon. Asymmetric encryptions scheme of the Rivest-shamir Adleman

Revised Manuscript Received on June 07, 2019

Naveen N, Assistant Professor, Department of Information Science & Engineering, Kalpataru Institute of Technology, Tiptur, Karnataka, India.

Dr. K. Thippeswamy, Professor, Department of Computer Science & Engineering, VTU PG Centre, Mysore, Karnataka, India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

(RSA), analyzes various processes and security parameters responsible for the designing and implementation of popular and known asymmetric encryption algorithms namely Rivest-shamir Adleman (RSA) is the block cipher based on asymmetric-key cryptography to protect the sensitive information. RSA key sizes are being 32, 64, 128, 192, 256 bits. Keeping in accord the parameters like key size, throughput, avalanche effect, encryption and decryption time, security and memory the presented paper computes and evaluates as to how the encryption algorithms perform. The cloud applications that are critical can be benefitted from the above suggested algorithm which claims to be simple and efficient. In Symmetric encryption process a single unique key ought to be shared between users who are bound for message receiving whereas in asymmetrical encryption process the encryption and decryption of messages during communication is achieved using a pair of private and public key. Depending on various set of parameters befitting the user needs an appropriate encryption algorithm is selected. Later the feasibility analysis is carried for above two encryption algorithms responsible for privacy and security of data relating with rest of the algorithms.

Journal classification includes: Section 2 demonstrates earlier author workings. Section 3 portrays the suggested approach of Multi-layer encryption with outlook of various stages. Section 4 lists down tests outcome. At last, Section 5 suggests research work for future thereby concluding the paper.

II. RELATED WORK

Author Rajiv Mishra et.al put forwards the technique of Data Loss Prevention (DLP) mentioning that no data is dispatched to the cloud in straight forward text. DLP is responsible in safeguarding valuable and intimate data and also responsible for not storing private details viz. credit card details, social security numbers, any record details of patients. Since the flow of data takes place from application to application like financial data traversing from credit scoring to that of mortgage originating application its required by the cloud providers to imbibe by the said security standards via access control, encryption [1]. Ali Gholami et.al highlights the research in accordance with cloud reference architecture orchestration, physical resource, cloud service management layers and resource control alongside analyzing current reformations in privacy preserving sensitive data methods in cloud computing namely privacy threat modeling and also privacy enhancing protocols and solutions [2].

Lovejeet Kamboj et.al suggested making use of steganography and cryptography approaches to possess Layer based security in cloud computing. For analyzing the productivity correlation parameters, MSE and PSNR are being considered [3]. Shakeeba S et.al, Cloud user is primarily concerned with secured flow of information. The suggested research eradicates any issues concerning privacy of data by enforcing multilevel cryptographic algorithms improving cloud security according to cloud customer's preference [4]. Xiao Zhang et.al presented a remedy considering systems with normal storage and reduplication storage. The outcome revealed that MLFS (Multi-Layer File Sharing System) claims to be enough space saving offering visible and justified I/O file operations [5].

Osman Hegazy et.al revealed a way with his research to segregate business related activities from security methods moulding the same into services i.e., business service and reusable secured service thereafter merging the two for secured services eliminating the need of recoding the security frequently thus relieving the developer and instead of focusing on security concerns, single mindedly handle business logic services itself. The crux is that once the security service is obtained it can be reused multiple times alongside other independent services. The suggested system is build up and focuses on developers responsible for securely generating cloud services by enforcing security logic [6].

Ashwin Dhivakar M Ret.al Purpose of Cloud Computing being, offering multiple online services linked to storage and computing incorporating services related to platform, software and infrastructure. Generally, cloud computing confronts serious issues concerning security of information. Also the cloud data is scattered across various geographically distributed data centers. The RSA technique is imbibed for security in Cloud environment by following data encryption along with image sequencing password for authorization [7].

Jingxin K. Wanget.al, elaborates multiple techniques for data prevention namely multi-level virtualization, single encryption and authentication interface. Another important concept involves authentication inter cloud the model of which relies on PKI and CA approach extending it to present situation even in the absence of CA system [8].

M2LF, Multi-Level Licensing Framework acclaims safeguarding cloud sensitive data. Safeguarding the intimate and sensitive cloud data is offered by the three layered framework. Those parameters are being the security and privacy policies, safety policies and authorization policies which results from the three layers security framework [9].

Suraj Lolage et.al founded on circuits system, the time-specified cipher text policy attribute based encryption was imbibed. The data is fetched secretly, there is fine grained access control along with rightly computed output [10]. There are two encryption techniques granting security namely Advanced Encryption Standard (AES) and Message Digest 5 (MD5). AES holds responsible for encrypting the data which is dispatched by the user to the third party and thereafter only upload it on the cloud. Also providing a confirmation security key. The data is being re-encrypted by MD5 making the decrypted data more secured [11].

Shrikant S. Patil et.al, the access control methods makes sure that only authenticated users have access to the system and data thus safeguarding users' privacy. For such data access control, the Cipher text-Policy Attribute-based Encryption (CP-ABE) is best suitable technique in the cloud environment [12]. In cloud computing fine-grained access control can be facilitated by imbibing comparison-based encryption technique. It's an attribute dependent encryption utilizing forward/backward derivation functions enforcing different range constraints on integer attributes, also level and temporal attributes [13].

The advancement of cloud computing is inhibited by the security and privacy issues. For applications requiring enhanced and strict security the Attribute Based Encryption (ABE) algorithm is best suited thus reducing access time and also lowering the cost [14].

Mohamed Meeran A et.al as presents that security is mandatory requirement in a cloud environment. Enforcing the technique of Randomized algorithm encryption, cyber thefts and unauthenticated user access can be controlled [15].

Pallavi Kulkarni et.al suggests implementing the identity based Attribute access policy on cloud platform used for encryption technique concerning cloud storage offering shared resources, software and information to users and devices according to their requirement using pay per use model [16].

The process of Cryptography entails two major approaches viz. encryption and decryption. In encryption technique a plain text is transformed to a new text which the others can't read and comprehends other than the receiver. Blowfish and AES algorithms are utilized for implementing a hybrid approach related to Cryptography. This results in a cipher text which can only be decrypted by the receiver itself [17].

The IT Security Specialist (ITSS) methodology of the organization is imbibed for the security. This approach utilizes numerous strategies of partitioning, file encryption and distribution amidst various storage providers thus enhancing confidentiality as the attacker must first fetch file fragments from multiple storage providers, then have the knowledge of merging them before attempting for decryption [18][19].

III. PROPOSED WORK

A. Overview

With the introduction and benefits of Cloud Computing technology abundant data storage is possible by outsourcing any amount of data on explicit cloud servers. The prime focus being managing data or file's privacy and security concerning unreliable parties of criminals, hackers and attackers alongside risk associated with cloud manager and cloud service providers[20-22]. Also the focus extends to granting real time query output to authorized user. The research suggests the approach of Multi-layer Encryption in cloud computing thus enhancing the security parameters concerning sensitive data. The main entity being the Data Owner (DO) requiring to stored abundant data in the cloud. The DO also resembles users possessing constrained devices like PDA, smart phones, TPM chip, etc. The other entity being the Cloud Service Provider (CSP)[23-25] offering services for data storage and computational resources dynamically to Authorized Users (AU) and DO. For authenticated users, the DO grants access to their files and exchanging of key material. The data is fetched from the cloud in an encrypted format by the authorized users and then he original data can be fetched by decrypting it.

1) Need of the data owner lies in outsourcing the data files on the cloud in encrypted format simultaneously making it available through keyword search to obtain better and efficient data utilization
2) A request for search is placed to CSP by the authorized user for retrieving the file collection.
3) Files an long with hash values is then returned by the CSP to the user.
4) Lastly, there is a integrity check by authorized user and the file is decrypted to obtain the plain text.

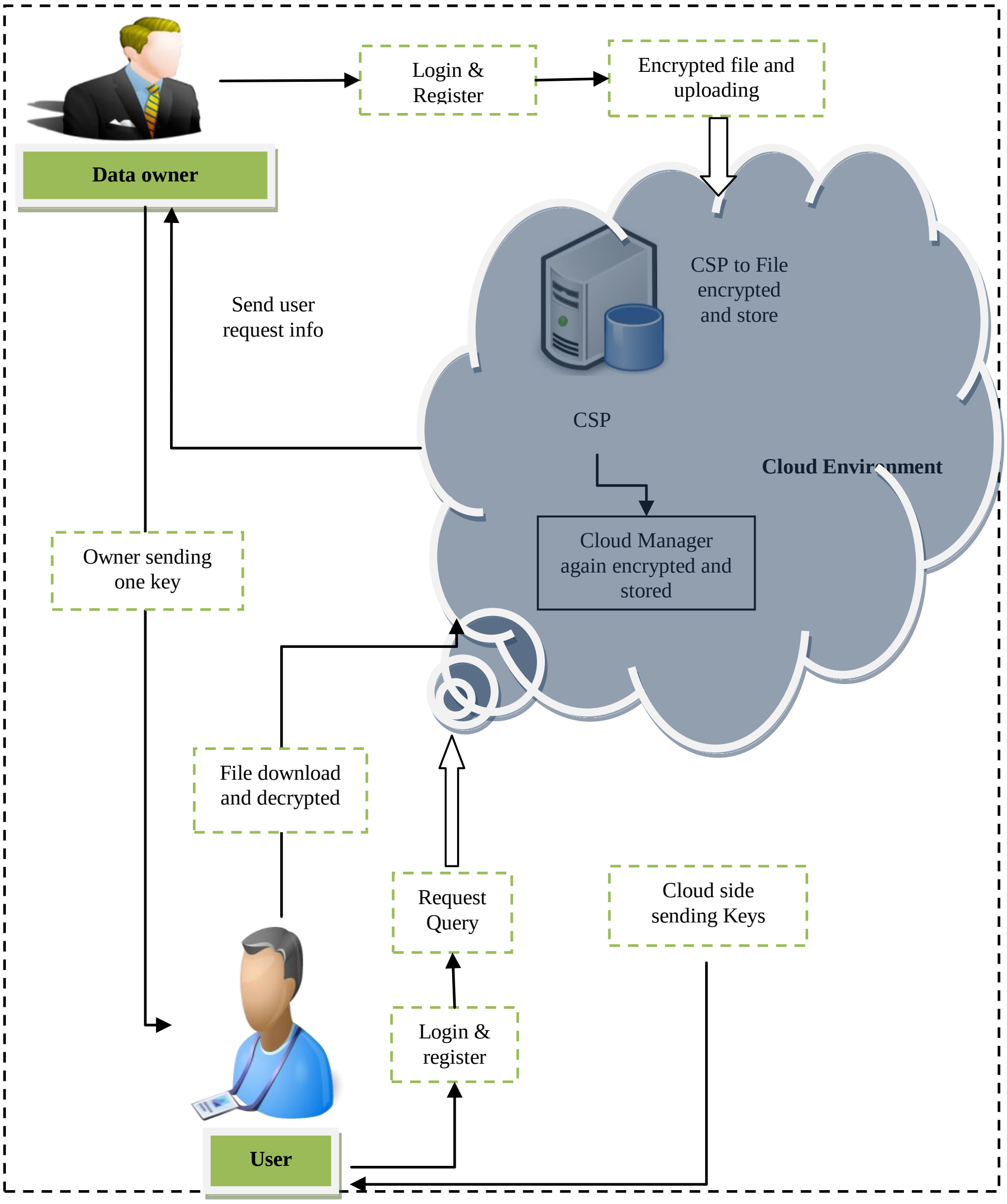


Figure 1: *Overall Proposed Security Architecture*

B. *Cloud Services*

Cloud services are founded on three technical models namely, Infrastructure as a service, and Platform as a service and Software as a service. Depending on the applications need suitable and apt services are offered to the users. The three unique service layers setup by Cloud Service Providers for imbibing various technologies in cloud environment are:

1) **Infrastructure as a service**: The management task and cloud resources storage is managed at this level. Since cloud functions on virtual resources, users are granted access to multiple virtual resources viz. software, hardware, servers, etc. in an extent to satisfy application's requirement.
2) **Platform as a service**: Applications and Software's are build up at this next level facilitating deployment and management of user's application. Software and hardware tools offered by service providers are also included accommodating application frameworks thereby supporting Software as a Service.
3) **Software as a service:** The cloud users can actually coordinate with the application at this level as high class service is offered at this level eliminating the requirement of installing software and hardware at users end. Also there is no need to pay attention on managing service and infrastructure[26][27].

C. *Multi layer Encryption Approach*

Information Technology offers advanced and useful technique of cloud computing that is being intensively spreading among internet users. The present approach lacks safeguarding of uploaded data on the server also lacks proper tracking of abolished users thereby the user authentication process is hampered. A resolution can be that the user authentication process is performed twice. Firstly, authenticating the user by making use of password, thereafter using the interfacing technology in sending secret code to authentic users email. The data owner encrypts the data twice before uploading it cloud server. Later the cloud

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

server and then the cloud manager again re-encrypt the data and finally stored in the cloud.

The data to be uploaded on the cloud is granted additional security using Multi- layer encryption technique. The paper projects performance of multi-layer encryption on the data to be uploaded on cloud server as data being more confidential and secure. The major concern of the paper is to perform the user authentication twice. The work suggests three-layers of encryption is to offer enhanced and higher safety of data and perform two types of login for user authentication. First, using the original user login name and password the validation is performed and secondly, to test whether user is authorized or not, a secret code is mailed to authentic users E-mail ID. On entering the correct secret code only the user is granted data access on cloud server. The purpose of authenticating the user twice is that only the authentic users can fetch the data from cloud server. The two algorithms being used for achieving security are AES and RSA encryption techniques.

D. Data owner

The DO outsources set of data or documents D={*D*1, *D*2,,,,*Dn*} along with few keywords. Also these documents and keywords must be encrypted in a specific way so that that later they can be searched easily thereafter sending the cipher texts to the server. Before the data or documents are dispatched to cloud server the data owner ensures that it is encrypted via Advanced Encryption Standard (AES) algorithm. The AES algorithm which is cipher based makes use of varied combination of algebraic expression operations. In this approach, Data undergoes combination of dual shifts of all bits and keys completing all rounds. The process is primarily based upon key generation algorithm which is straight forward. The confirmation is done using confirmation security key 1.

E. Cloud Service provider

The data centre acts as the host to perform cloud services allowing people or organizations to access it through network connections. The entity of Cloud Server is maintained by the cloud service provider, which holds necessary storage room and various calculation assets to manage records of customer’s information. Primarily, the cloud service holds cipher oriented data documents. After the data undergoes encryption, the data is forwarded by the auditor to public clouds where the data is again re-encrypted using RSA by the cloud Service provider thereafter re-encrypted data to storing in public cloud, possessing the confirmation with a security key 2. The Rivest–Shamir Adleman (RSA) approach is being implemented by cloud service provider to encrypt the uploaded data or files. Once the encryption process is over, the encryption key is being dispatched to the user. The files then reside in storage area[28]29].

F. Cloud Manager

Once the third party receives the data submitted by the Data owner, it undergoes encryption process by the third party. Using AES algorithm the data encryption is performed and then the third party forwards the data to the cloud. That is when the public clouds receive the encrypted data, the cloud manager is responsible to once again re-encrypt the data using RSA and later store it in public cloud. The data is re-encrypted using the process of Multi-layer encryption process with help of RSA algorithm having the confirmation with a security key 3.

G. Key Generation

Before the files are being outsourced to the cloud the DO processes the files using the two algorithms: (1) Encryption (2) Key Generation. The key pairs are generated in this algorithm by the DO as following: By choosing two greatest primes value of N is computed as, N = p*q. Values of r and s are computes using extended Euclidian algorithm as p*r + q*s =1. The public key is PK={N} and the private key being PR ={p; q; r; s}. Key generation method is shown in

Algorithm: Key Generation

```
1 Select two large random primes p,q
2 Calculate N= p * q
3 Compute r & s using Euclidian algorithm where p*r + q*s =1
4 Public Key PK={N} and Private key PR ={p; q; r; s}
```

H. Advanced Encryption Standard (AES) algorithm

AES is symmetric key block cipher text oriented algorithm published as FIPS-197 in December 2001 in the Federal Register by NIST-National Institute of Standards and Technology. Symmetric key encryption claims to be of prime importance under AES algorithm. These algorithms work by using the similar key for performing encryption and for decryption too. Thus its mandatory to keep this key hidden and secured. Also, the advantage of this algorithm being that while performing it consumes very less computing power and functions with a greater speed. These algorithms are categorized as: Block cipher and Stream cipher. The block cipher takes plaintext of block as input having fixed size relying on the type of symmetric encryption algorithm, a fixed size key is given to the block of plain text thereafter output block of the same size as the plaintext block is generated.

To achieve secured and classified encryption and decryption of data, AES algorithm which is symmetric-key block cipher oriented, is considered the best. Its primarily implemented to safeguard digitalized information concerning varied data forms. The present work uses 128bit version AES[30].

***Encryption**:*

```
EncryptCipher(bytein[16],byteout[16],key_arrayround_key [Nr+1])
begin
byte state[16];
state = in;
AddingRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
subbytes(state);
shiftrows(state);
mixcolumns(state);
AddingRoundKey(state, round_key[i]);
end for
subbytes(state);
shiftrows(state);
AddingRoundKey(state,
round_key[Nr]);
End
```

Decryption:

```
DecryptCipher(byte[] in,byte[] out,byte[] w)
begin
byte[][] state=new byte[4][Nb];
state =in;
AddingRoundKey(state,w,Nr*Nb,(Nr+1)*Nb-1);
for round=Nr-1 round>=1 round=round-1 do
InvShiftRows(state);InvShiftBytes(state);
AddingRoundKey(state,w,round*Nb,(round+1)*Nb-1);InvMixColumns(state);
end for
InvShiftRows(state);
InvSubBytes(state);
AddRoundKey(state,w,0,Nb-1);
out=state;
end
```

I. Rivest–Shamir Adleman (RSA) algorithm

RSA and Diffie-Hellman Key Exchange are classified as asymmetric sort of algorithms. RSA and Diffie-Hellman Key Exchange are implemented in cloud computing to produce encryption keys for symmetric algorithms. The need occurs for the security algorithms providing help in performing functions (such as searching) on the decrypted data, also maintaining the data confidentiality. The Asymmetric-key algorithms work with two different keys to perform the encryption and decryption process. These keys being: Private Key and Public Key. The sender uses the Public key for encrypting data and the receiver uses the private key for decrypting the data. Cloud computing thus imbibes the asymmetric-key algorithms for generating encryption keys.

In RSA which acts as a block cipher, there is mapping of each message with an integer. It contains both Public and Private Keys. Talking about Cloud environment, all are aware of Pubic-Key, whereas the user who is actually the owner of data is aware of the Private-Key. So it can be stated that the CSP performs the encryption whereas the cloud user is responsible for decrypting the data. After the data undergoes encryption using the public key the decryption of the data is possible only with related private key.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation: At first, the key is generated in order to perform the data encryption. And this processing takes place among the user and the Cloud service provider.

Steps:

1. Two unique prime numbers a and b are selected. These integers (a and b) must be randomly selected from security point of view and they must measure same bit length
2. N is computed as, n = a * b.
3. Evaluate Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Select integer e, so as 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. e now becomes the Public-Key exponent.
5. d is evaluated as: d = e-1(mod Ø(n)) i.e., d is multiplicative inverse of e mod Ø(n).
6. d remains as Private-Key component, so as d * e = 1 mod Ø(n).
7. The Public-Key holds public e as exponent e and n as modulus i.e, (e, n).
8. The Private-Key hold modulus n and d as private exponent that ought to be a secret i.e, (d, n).

Encryption: The process of converting original plain text (data) into cipher text (data) is called Encryption.

Steps:

1. Any user willing to store the data in the cloud server must be assigned a Public- Key (n, e) by the CSP.
2. Making use of padding scheme the mapping of user data with an integer is done with the aid of reversible protocol.
3. Encryption of data is performed and the generated output cipher text (data) C is C = me (mod n).
4. Finally this encrypted data or cipher text is ready for storage within the Cloud Server.

Decryption: The process of converting cipher text (data) back to the original plain text (data) is termed as Decryption.

Steps:

1. The data request is send by the cloud user to the Cloud service provider.
2. CSP then validates the user's authenticity and the only outputs the encrypted data i.e, C.
3. The data is then decrypted by the Cloud user by evaluating, m = Cd (mod n).
4. After m is computed, the user is allowed to fetch the original data by reversing the padding scheme.

J. Key Sharing

The initial key being the pass code is given to CSP, data owner, Cloud manger to data user using authenticated user Email ID. Once the passcode is entered successfully, the data user can now jump to the next level, authorization of which is granted by cloud admin only.

K. File Decrypt

Once the user is authenticated successfully, the use is allowed to fetch or download the file that was requested. Upon downloading the file is automatically decrypted. The existing work offers data exchange among data owner and the user under a safe and secure gateway. As a result, secured data uploading and downloading can be performed with the given encryption and authentication techniques. The work acclaims that using the above techniques one can avoid and eliminate cyber thefts and unauthenticated users. When the matching files are received from the cloud service provider against the corresponding search query, then the authentic user can use the private key to decrypt it and get the resultant plain text.

IV. RESULTS AND DISCUSSION

In the realm of Cloud Computing parameters like Authenticity, Confidentiality, Privacy Integrity and Availability are of prime focus for the cloud consumer and Cloud service providers too. Critical issues concerning Cloud computing is that of Security, which further can lead to multiple complications and serious concerns. To safeguard the customer from data loss or theft, the CSP and cloud service consumer must take effective measures to protect the cloud from any threats or attacks. Multi-layer encryption technique is suggested for providing privacy and security of data. This approach claims to provide enhanced security measures to DO and cloud server too. The advantage using this technique being that data access is strictly prohibited to users not having DO authorization. Hence the introductions of multi-layer encryption approach with aim of fulfilling confidentiality and security of data. To implement the tight security the users are authenticated twice and then only data access is granted. The users detected as unauthorized are tracked down and blocked. The abolished users are detected and completely suspended to reduce any future attacks on data or files. To retrieve data from cloud by the authorized users a two-step verification approach is imbibed.

The work implements the techniques and approaches in Cloud computing environment and numerous CSPs are successfully evaluated. Trails were based on the given configuration: Windows 8, Intel Pentium (R), CPU G2020 and processer speed 2.90 GHz respectively. The software configuration requirements are as mentioned, Operating System →Windows 8, CloudSim.

Table 1: *Comparative of Accuracy*

S.No	Encryption techniques	Security (%)	Time (ms)
1	CP- ABE	88.5	3.53
2	K-NN	92.3	2.65
3	Multilayer Encryption Approach	96.6	0.96

Table 1 mentioned above demonstrates evaluation of Multi-layer encryption approach compared with K-NN, and CP- ABE. The suggested Multi-layer encryption technique proves to be effective providing enhanced performance in comparison with rest of the existing techniques.

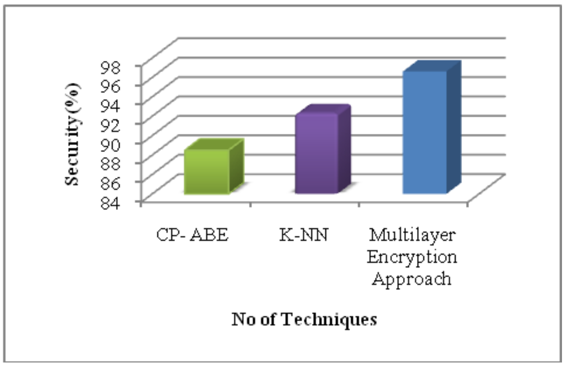


Fig 2: *Comparison of Accuracy Analysis*

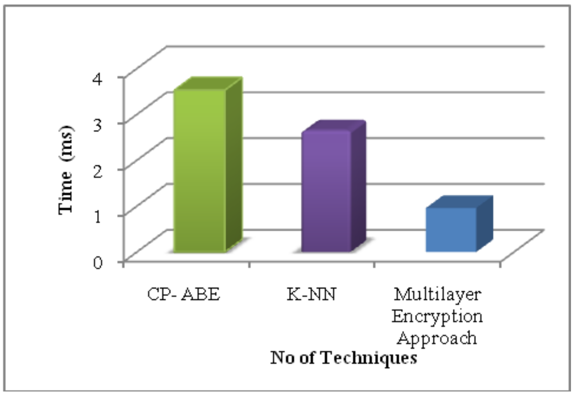


Fig 3: *Comparison of time evolutions*

Figure 2 and 3 mentioned above compares security based encryption models performing with Multi-layer encryption approach with K-NN, and CP- ABE. The suggested Multi-layer encryption technique is efficient offering greater performance compared with rest of the current techniques.

Simulation results

The research includes implementation which is being performed on Cloud computing domain, JAVA environment, CloudSim and entire data is managed using MYSQL databases and an output results that are fetched are also stored in MYSQL databases.

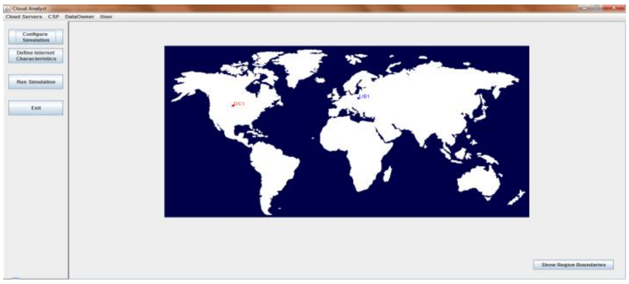
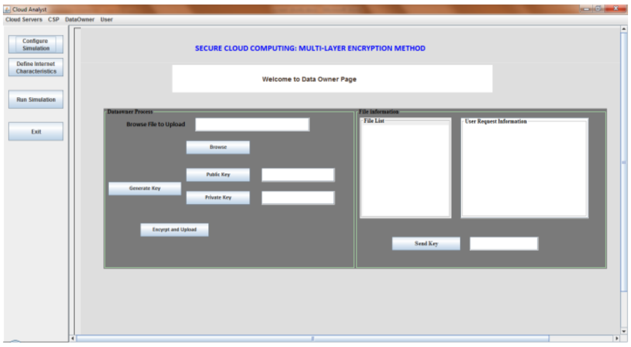


Fig 4: *CloudSim home page*

Fig 4, represents start to cloudsim homepage and start the cloud servers. It's designed to data cloudsim configuration part. Then click to overall process has been start from in this processing and after configuration process to start the cloud server process.


SECURE CLOUD COMPUTING: MULTI-LAYER ENCRYPTION METHOD

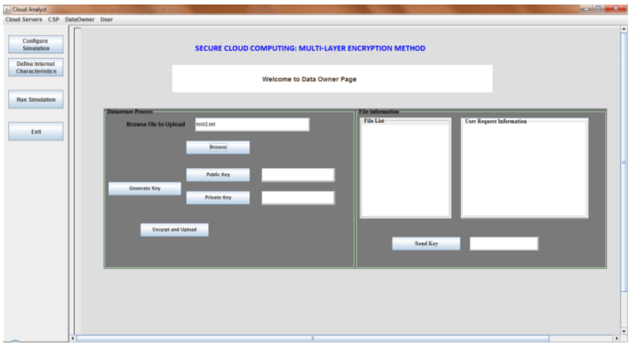
Welcome to Data Owner Page

Fig 5: *Data Owner processing*

Fig 5, represents after cloud server start processing and then start to data owner process windows and user normally register and login the cloud environment. Data Owner

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

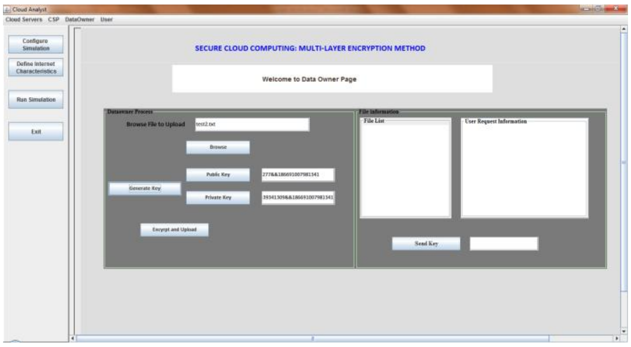
once register and login in cloud environment to cloud server to allocate the sing id and memory areas.



Browse File to Upload: test2.txt

Fig 6: *Uploading the file*

Fig 6, represents user normally register and login the cloud environment its security purposes and then to start to data owner process windows. user if want to store into cloud sectors in own data to sending before encrypted the file into the cloud environment at the same time to generate keys



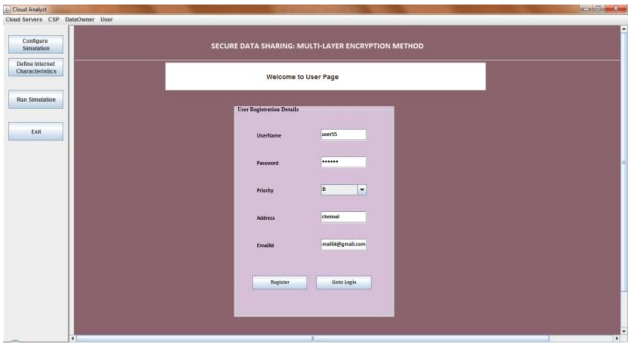
Browse File to Upload: test2.txt

Public Key: 277&&186691007981341

Private Key: 39341309&&186691007981341

Fig 7: *Key generations*

Fig 7, represents start to data owner process windows and user sending before encrypted the file into the after that to generate the keys for security purpose in cloud environment. Here generate to two keys private key and public key both are generate same time. In private key1 for encryption key2 for decryption. And both are stored in cloud databases.


Cloud Analyst
Cloud Servers CSP DataOwner User
Configure Simulation
Define Internet Characteristics
Run Simulation
Exit
SECURE DATA SHARING: MULTI-LAYER ENCRYPTION METHOD
Welcome to User Page
User Registration Details
Register
Goto Login

UserName: user55

Password: ******

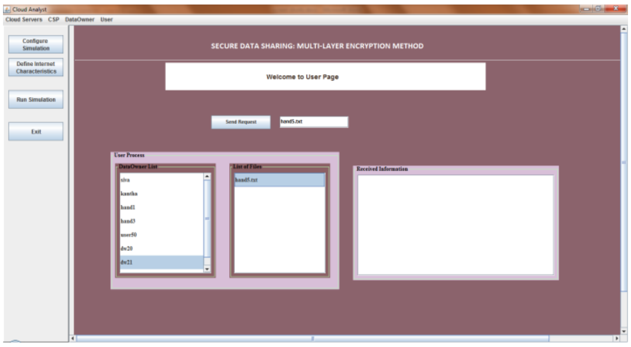
Priority: B

Address: chennai

EmailId: mailid@gmail.com

Fig 8: *User processing*

Fig 8, represents after data owner process is completed in to start to user process windows and user normally register and login the cloud environment. Here users search to data to search box. If data is visible but not copy and downloaded and all so that, user sends to request to cloud via particular data owner.



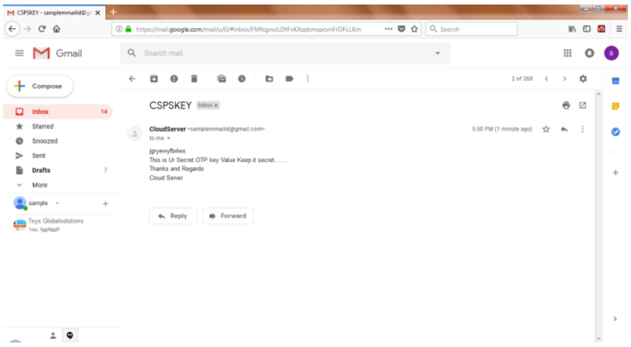
Send Request: hand5.txt

DataOwner List: siva, kantha, hand1, hand3, user50, dw20, dw21

List of Files: hand5.txt

Fig 9: *User selects file and sending request*

Fig 9, represents start to user process windows and user normally register and login and if want the access to the any file to select and send request to particular data owner cloud environment. Here cloud server have to 3 layer authentication process is happing and after in that user valid or not to checked in part.



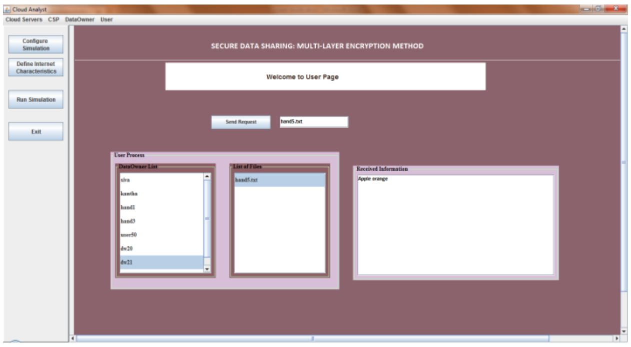
CSPSKEY Inbox

CloudServer <samplemmailid@gmail.com>
to me
5:50 PM (1 minute ago)

jgryewyfbvlwx
This is Ur Secret OTP key Value Keep it secret.......
Thanks and Regards
Cloud Server

Fig 10: *Authentication and 3-keys sending via Email*

Fig 10, represents start to three way authentication process after to send key from cloud sector to valid user. Here to after check in that user was valid so send to 3-key are cloud server, cloud service provider and data owner to sending key via email.



Send Request: hand5.txt

DataOwner List: siva, kantha, hand1, hand3, user50, dw20, dw21

List of Files: hand5.txt

Received Information: Apple orange

Fig 11: *File decrypted and view*

Fig 11, represents start to three way authentication process after to send key from cloud sector to valid user. Then, after the getting the 3 key to access the data. Here priority based visible to data. If user is selecting “A” whole data to visible and reading and downloaded it. if user selecting to “B” data only visible but not download it.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

V. CONCLUSION

To achieve confidentiality and security of data the paper work suggests multi-layer encryption approach. Intense security is offered where confidential data is concerned. Also the user authorization process is conducted twice so as only authenticated users are granted data access. Users that are detected as unauthorized are traced and completely blocked. This paper presents a new strategy of Multi layer encryption oriented on the algorithm of Advanced Encryption Standard (AES) and Rivest-Shamir Adleman (RSA) which claims to offer security and privacy of entire public cloud content. Such data communication among the systems will lead to improvised security concerning the data that is shared over the cloud. With the suggested scheme or approach, authorization is given to user, in accessing the public cloud data thereby leading to improvised security and privacy concerning the cloud computing through multi layer encryption.

REFERENCE

1. Rajiv Mishra, Meenaxi Kumari (2015), "Need of Multi-Layer Security in Cloud Computing for on Demand Network Access", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 4, pp. 398 – 404.
2. Ali Gholami and Erwin Laure, "Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments", Computer Science & Information Technology (CS & IT), pp. 131 – 150.
3. Lovejeet Kamboj, PawanLuthra (2017) "Multi-Layer Data Security in Cloud Computing", International Journal of Computational Engineering Research (IJCER), Vol. 7, pp. 1-7.
4. Shakeeba S. Khan, R. R. Tuteja (2016)"Cloud Security Using Multilevel Encryption Algorithms", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, pp. 70 – 75.
5. Xiao Zhang, Wan Guo, Zhanhuai Li, Xiaonan Zhao, Xiao Qin, (2014)"MLFS:A Multiple Layers Share File System for Cloud Computing", Globecom Workshop, pp. 99 – 105.
6. Sahar Mohammed Abduljalil, Osman Hegazy, Ehab E. Hassanein,(2013) "A Novel Approach for Handling Security in Cloud Computing Services", International Journal of Computer Applications (IJCA) Vol. 69, No.5, pp. 9 - 14.
7. Ashwin Dhivakar M R, Parveen Kumar, "To Implement a Multi-Level Security in Cloud Computing Using a Cryptographic Novel Approach".
8. Jingxin K. Wang, XinpeiJia,(2012) "Data Security and Authentication in Hybrid CloudComputing Model", IEEE Global High Tech Congress on Electronics, pp. 117 – 120.
9. Haifaa Jassim Muhasin, RodziahAtan, MarzanahbintiA.Jabar, Salfarinabinti Abdullah,(2016) "Cloud Computing Sensitive Data Protection usingMulti Layered Approach", ICSIT, IEEE, pp. 69 – 73.
10. Suraj Lolage,Hema Mangtani, Komal Dongare, Akash Labade, Prof.Shikha Pachouly,(2018) "A Time-Specified Ciphertext-Policy Attribute- Based Encryption with Circuit's Technique in Cloud Computing", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 7, pp. 3712 – 3719.
11. C Nalini, R G Suresh,(2018) "The Service of Trusted Third Party in Multiple Public Clouds in Dual Encryption Security Mechanism", International Journal of Pure and Applied Mathematics (IJPAM), Vol. 119, No. 12, pp. 10847-10856.
12. Shrikant S Patil, B R Solunke,(2015) "Literature review on Efficient and Revocable Data Access Control Scheme for Multi-Authority Cloud Storage Systems", International Journal of Modern Trends in Engineering and Research (IJMTER), Vol. 2, p.p. 205 – 208.
13. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Mengyang Yu, Hongjia Zhao, Comparison-Based Encryption for Fine-grained Access Control in Clouds, p.p. 105 – 116.
14. Saravana Kumar N, Rajya Lakshmi G V, Balamurugan B,(2014) "Enhanced Attribute Based Encryption for Cloud Computing", International Conference on Information and Communication Technologies (ICICT), pp. 689 – 696.
15. S Keerthivasan, K Viswanath, Mohamed Meeran.A, M S Muralidhar,(2018) "Secured File Sharing of Encrypted Data on Cloud using Dual Authentication", SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) - Special Issue ICRTECITA, pp. 109 – 113.
16. Ankita Nandgaonkar, Pallavi Kulkarni,(2016) "Encryption Algorithm for Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7, No. 2, pp. 983 – 989.
17. Diaa Salama AbdElminaam (2018) "Improving the Security of Cloud Computing by Building New Hybrid Cryptography Algorithms", IJEIE, Vol.8, No.1, pp. 40 - 48.
18. Dhurate Hyseni, Artan Luma, Besnik Selimi, Betim Cico,(2018) "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 9, No. 2, pp. 203 – 210.
19. K Satyanarayana,(2016) "Multi level Security for Cloud Storage using Encryption Algorithms", IJECS, Vol. 5, pp. 17338 - 17346.
20. Bing He, Jie Tang, Ying Ding, Huijun Wang, Yuyin Sun, Jae Hong Shin, Bin Chen, Ganesh Moorthy, Judy Qiu, Pankaj Desai, David J. Wild,(2011) "Mining Relational Paths in Integrated Biomedical Data", Plosone, Vol. 6, pp. 1 – 14.
21. N.Jayapandian, Dr.A.M.J.Md.Zubair Rahman, M.Koushikaa, S.Radhikadevi,(2016) "A Novel Approach to Enhance Multi Level Security System Using Encryption with Fingerprint in Cloud", IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16), IEEE.
22. Alok Ranjan, Mansi Bhonsle (2016), "Advanced techniques to Shared &Protect Cloud Data using Multilayer Steganography and Cryptography", 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), IEEE, pp. 35 – 41.
23. SADIA SYED, P.Srinivas Teja "Novel Data Storage and Retrieval in Cloud Database by using Frequent Access Node Encryption" 2014 IEEE, International Conference on Contemporary Computing and Informatics (IC3I), pp. 353 – 356.
24. Saad Khan and Simon Parkinson and Andrew Crompton,(2017), "A Multi-layered Cloud Protection Framework", UCC Companion pp. 233 – 238.
25. Shridhar B, Pavan Gujjar Panduranga Rao may (2014)"Advanced Multi-Encryption Technique in Cloud Computing", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol. 1, pp. 26 – 29.
26. P Sabitha, V B Narasimha, "An Approach to Multi-Cloud Securities", International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 4, pp. 89 – 92.
27. Sanchi Kalra, Kunal Atal, Rachna Jain (2017), "Security Issues in Cloud Computing", International Journal of Computer Applications, Vol. 167, No. 2, pp. 37 – 41.
28. Jeena Jha, Jalak Pansuriya "Multi-Level authentication in Cloud Computing using 3D security", National Conference on Cloud Computing & Big Data, p.p. 215 – 218.
29. Syed Asad Hussain, Mehwish Fatima , Atif Saeed , Imran Raza, Raja Khurram Shahzad (2017), "Multilevel classification of security concerns in cloud computing", Applied Computing and Informatics, Vol. 13, pp. 57 – 65.
30. Taehwan Park, Hwajeong Seo, Sokjoon Lee and Howon Kim (2018), "Secure Data Encryption for Cloud-Based Human Care Services", Journal of Sensors, pp. 1 – 10.

AUTHORS PROFILE

Naveen N. Currently working as Asst.Professor in Department of ISE at Kalpataru Institute of Technology, pursuing Ph.D degree in Computer Science and Engineering from VTU, Karnataka , India..

Dr. K. Thippeswamy. Currently working as Professor in CSE at VTU PG-Center, Mysore, Karnataka , India. His research interest includes Data Mining & Cloud Computing.