I.J. Education and Management Engineering, **2017, 5, 56-68**
Published Online September 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2017.05.06

Available online at http://www.mecs-press.net/ijeme

Multilevel Authentication based Data Security and Verification over Cloud Computing Environment

Deepak Soni[a], Nishchol Mishra[b]

[a,b,] *School of Information Technology, RGPV University Bhopal*

Received: 01 January 2017; Accepted: 28 March 2017; Published: 08 September 2017

Abstract

There are various algorithm proposed in the area of cloud computing environment. Now a days the cloud computing is the very interesting area for research purpose. Cloud computing environment provides the security of user data and integrity verification with the users data, also cloud provide on demand network access to a shared pool of configurable computing resources like network, servers, storage, applications and services that can be rapidly provisioned and provide with minimum user effort and service provider interaction. Uses of cloud computing services is very easy and also in very low cost. The cloud computing services are on demand over the internet, so it provides the facility to clients that access these services remotely from anywhere, anytime with the help of internet and any devices like pc, laptop mobiles etc. The data or information of cloud user is save in cloud service provider so in the cloud computing environment the security of data and privacy of data is primary issue[1]. In this paper a security model is proposed here we provide a mechanism to cloud user to encrypt their data or sensitive information and generate a integrity verification key then save the data on cloud in encrypted form. The cloud user have many choices like private phase, public phase and hybrid phase and the hybrid phase tier1 and tier 2. In all three sections there are various encryption techniques are implemented like AES (Advanced Encryption Scheme)[9], IDEA, Blowfish[12], And SAES based on the security factors namely authentication, confidentiality, security, privacy, non-repudiation and integrity. In Private phase a Unique token generation mechanism with the help of SHA-2 implemented it helps to ensure the authenticity of the user, The Hybrid section of the model provides On Demand Security Choices Tier one or Tier two and Public section provides faster execution with the help of Blowfish algorithm. Overall the user data Is wrapped in two folds of encryption and integrity verification in all sections.

Index Terms: AES, IDEA, SAES, SHA-2, Blowfish, Hash key, Data Privacy, Data Security.

* Corresponding author. Tel.: +919743220034; fax: 8256237271
E-mail address deepaksoni2021@gmail.com

1. Introduction

Cloud computing environment provide the facility of storage the data and maintaining privacy to the data having lots of advantage and it provide to user a guarantee storage and access of data very easily with the help of internet anytime anywhere in the world. The Cloud computing also offer on demand services with user’s data to support multiple device and compatibility[10]. As compared to the traditional server computing there is limitation of storage and services for the user which user usage for its optimized requirement, such requirement lacking facilities overcome by the cloud computing dynamicity. The cloud computing environment provides a dynamic, scalable and efficient solution for service usage. The dynamic storage of user data, resource pooling , Self-provisioning of resources , Broad network access and pay as per usage concept make cloud more usable as per requirement. The cloud user utilizes a wide variety of available services and user required to pay only for those services that he use for that time only. Security is one of the major problems of cloud computing environment.

Cloud computing provide a certain level of security via its secure structure which contain parts as : CSP (cloud service provider) a party provides the cloud services in the scenario which uses as a owner of cloud services and maintain a data enter, data storage hardware and other related requirement service act as a provider. There are the various vendor such as IBM, AMAZON, INTEL etc they maintain the cloud services and act as a cloud service providers. TPA (third party authenticator) is an another important part of cloud computing environment which deals or communicate in between the user end and CSP. The TPA authenticate the data integrity checksum using different hashing scheme and other required computation done at this end. And a CU cloud user that uses the cloud services that provided by the service provider the cloud user save their data in cloud storage network at the third party end so here in cloud computing there are various security issues in the cloud computing environment like data integrity, authentication, data confidently , access control, non-repudiation [2]etc. basically the Data security and data integrity are major issues for users of cloud computing environment.

Today’s clouds usually place centralized, universal trust altogether the cloud user's because the services of cloud computing is easy to use and available at very low price. the data confidently is also refers to privacy of data the user of cloud computing environment upload their personal details and sensitive information to the cloud service providers so there may be possibility of hacking, any intruder in cloud, and any unauthorized person access the information or data of any other user[13]. In the proposed design creating a highly secure environment for the user firstly user login with correct user id and password then upload the data in multiple security sections as his need. Each section have multiple security encryption technique include data verification, and only authorized user can access the data. The proposed model provides a complete protection of user data that stored in cloud by enhancing the level of authentication, confidentiality, privacy and incorporating the scheme of integrity which generates notification to the user in case of data integrity violation. Various encryption techniques and integrity verification techniques SHA-2 for generating a unique token for each file, are combined to protect data against unauthorized access and security breaches[15].

2. Proposed Work

In the proposed Framework here creating a environment for cloud user with enhanced data security, data integrity verification, encryption service, and authentication which can access data securely, is provided by a trusted third party which is separate from the storage cloud provider. In the proposed framework firstly the cloud user resister and login into the cloud then choose the storage selection section as private, public, and hybrid phase tier one or tier two anyone of these at a time and upload the files.

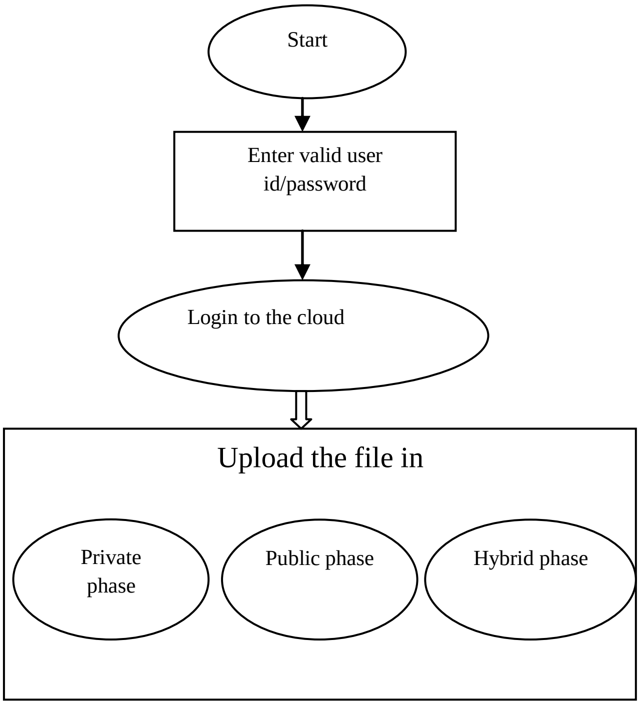


Fig.1. Cloud Storage Selection for User Files

Fig.1.shows the Cloud storage selection for user. The cloud user can choose the any one of the section at a time for uploading files. All the section have multiple functionality and uses. In each section there are different-different encryption technique and hashing technique is applied for security of user data. below we discuss in detail about each section of the model.

3. Private Phase

If the cloud user want to encrypt their data in private phase then he selects the private section the steps depicted in figure are applied on data. First of all user upload their data, while uploading the data is divided into the three blocks and data stored in three different- different location in three parts and after successful upload the user get a unique token in this phase and click in requested tab when the user requested to upload then the data successfully save in cloud in encrypted form. The input file gets encrypted into ciphered form with AES algorithm (Advanced Encryption Standard) technique. And a security hash key is generated with SHA-2 algorithm.

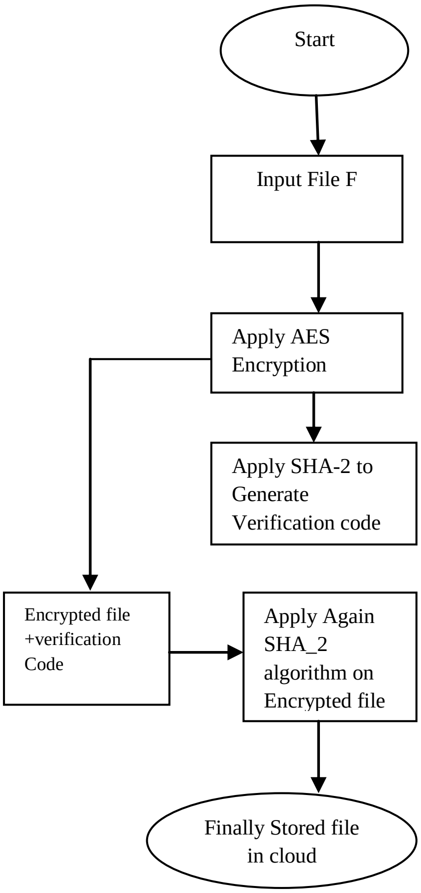

Start
Input File F
Apply AES Encryption
Apply SHA-2 to Generate Verification code
Encrypted file +verification Code
Apply Again SHA_2 algorithm on Encrypted file
Finally Stored file in cloud

Fig.2. Private Section

Private section file upload steps:-

Step 1. Select any file to upload in the Private Section of cloud storage.
Step 2. Upload file data divides into the three parts.
Step 3. Encrypt the user file with the help of Advanced Encryption Standard technique.
Step 4. Apply the SHA-2 on the encrypted file to generate the integrity verification code.
Step 5. This integrity verification code append in front of the uploaded file by user with data before file stored in cloud storage network.
Step 6. Apply SHA-2 algorithm again on encrypted data to generate the unique secure hash key or token.
Step 7. This unique token provide to the user, which is required at the time of downloading the file to authenticate user.
Step 8. Finally the user file stored in the cloud storage.

4. Public Phase

The public section provides limited security. If any user wants the faster computation with minimum cost of encryption and decryption, also if the data is not that very much confidential and sensitive then public section is the best choice for that user. In the public section the data is encrypted by with the help of blowfish algorithm. The blowfish algorithm is very most important and useful encryption technique. The blowfish algorithm is faster than other algorithm and it is license free so the blowfish is easily available for all Users.

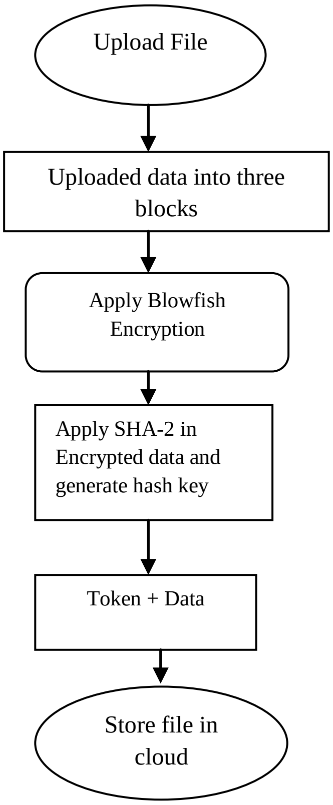

Upload File
Uploaded data into three blocks
Apply Blowfish Encryption
Apply SHA-2 in Encrypted data and generate hash key
Token + Data
Store file in cloud

Fig.3.Public Section

Public section file upload steps:-

Step 1. Select any file to upload in the Public Section of cloud storage.
Step 2. Upload file data divides into the three parts.
Step 3. Apply Blowfish Encryption Technique on Data.
Step 4. Apply SHA-2 on Encrypted data and generate unique hash key for integrity verification.
Step 5. Append generated hash key front of the user data
Step 6. Finally Stored the file in cloud storage network.

5. Hybrid Phase

The Hybrid section of proposed model is the combination of the various encryption technique like IDEA, Blowfish, SAES and many more. The hybrid section is divided into two phases tier one, tier two. User can choose any one of phase at a time and upload the data. The hybrid section is basically provide various encryption techniques and choices for user as his requirement like security of data, faster execution time, response time etc. uploading file in hybrid section is shown in below figure.

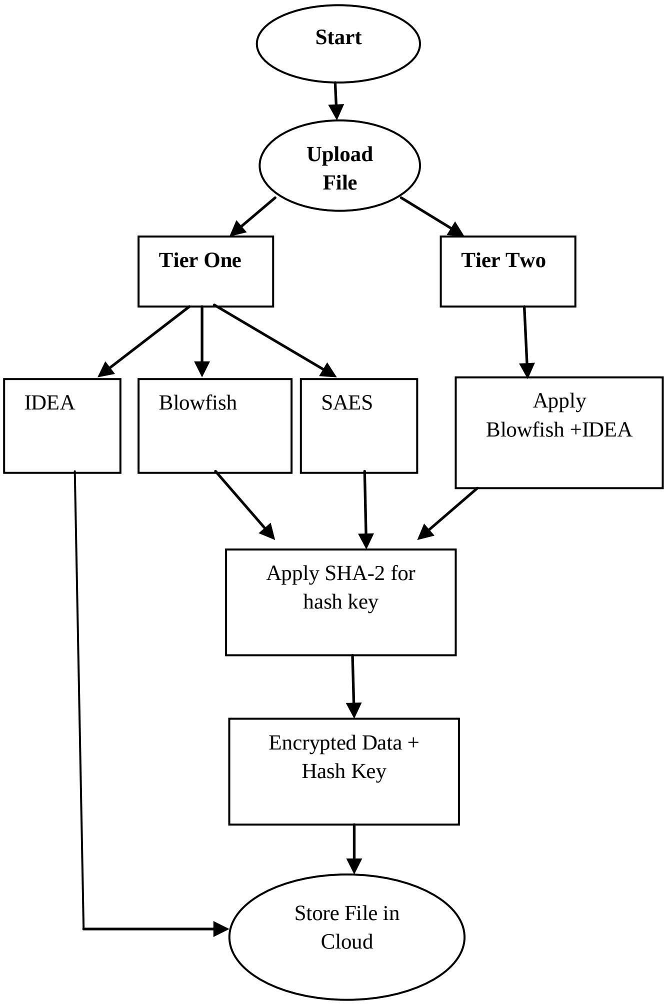


Fig.4.Hybrid Section Tier One and Tier two

Hybrid section file upload steps:-

Step 1. Select any file to upload in the Hybrid Section of cloud storage.
Step 2. Choose Tier One or Tier Two For file upload.
Step 3. If User TIER 1 is selected Then There is options of SAES, IDEA and Blow-Fish encryption Technique.
Step 4. If User SAES is selected Then encrypt user file with SEAS encryption technique and go to Step-7.
Step 5. If User Blowfish is selected Then encrypt user file with Blowfish encryption technique and go to Step-7.
Step 6. If User IDEA is selected Then encrypt user file with IDEA encryption technique and Directly File Stored in cloud.
Step 7. Apply SHA-2 Hashing technique and generate unique 64 bit hash value.

Step 8. Append Hash value front of the data.
Step 9. Finally File Stored in Cloud Storage Network.
Step 10. If tier Two is selected Then Apply Combination of IDEA and Blowfish Algorithm.
Step 11. Go to Step-7.

6. Data Retrieval Phase

In Data retrieval phase the user want to retrieve or download their data from cloud storage network. Firstly user login in cloud network input user id and password. After successfully login user can easily access the data in all three phases .the private files can only download with the help of unique token that is generated at the time of file creation or file upload. If the unique token is correct then file retrieved from cloud storage. public section, hybrid section files directly download by user.

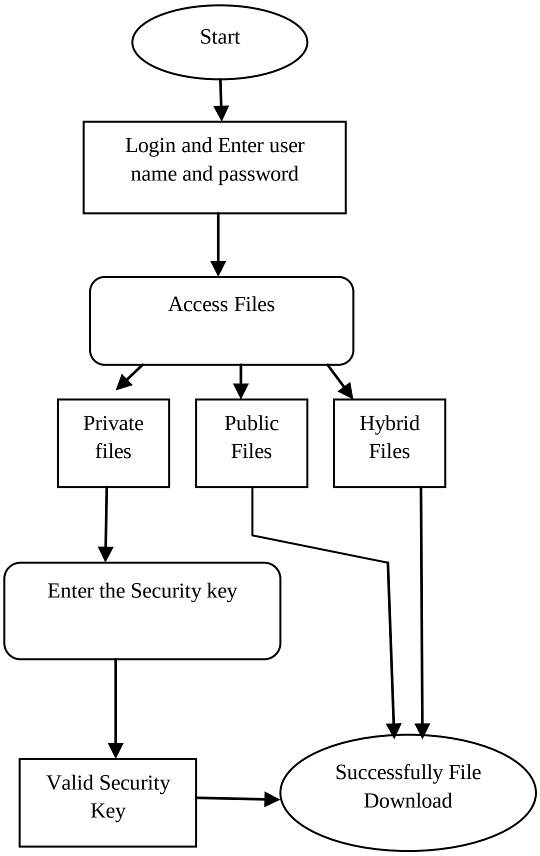


Fig.5. Data Retrieval Process from Cloud Storage

7. Security Analysis

The proposed Framework provides security and protection in various Security breaches like data leakage, modification, data integrity, authentication, data confidently, access control, non-repudiation etc[7]. The designed framework provide the security against following issues in an efficient and effective manner.

7.1. Privacy:-

The Privacy[17] is a wide concept that varies among countries, cultures and jurisdictions. Giving a precise definition is difficult if not impossible, and this matter, by itself, poses a problem when trying to establish a consensus so according to cloud computing environment privacy is the keeps all the information or data provided by user is secret[7].

7.2. Confidentiality:-

Confidentiality[14][17] ensures that data or user information is not disclosed to unauthorized user. Maintaining the Confidentiality of the data is very most important and it is one of main security issue in cloud computing environment Confidentiality loss means that when data or users critical information can accessed by any other individuals who are unauthorized to access that information. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the user and cloud server's not encrypting the data[1].

7.3. Availability:-

Availability[14] ensures that data processing resources are made available by action. The Availability is simply refers to when a user want to access something in the cloud computing environment that it is available to be accessed. This is vital for mission critical systems[1].

7.4. Integrity:

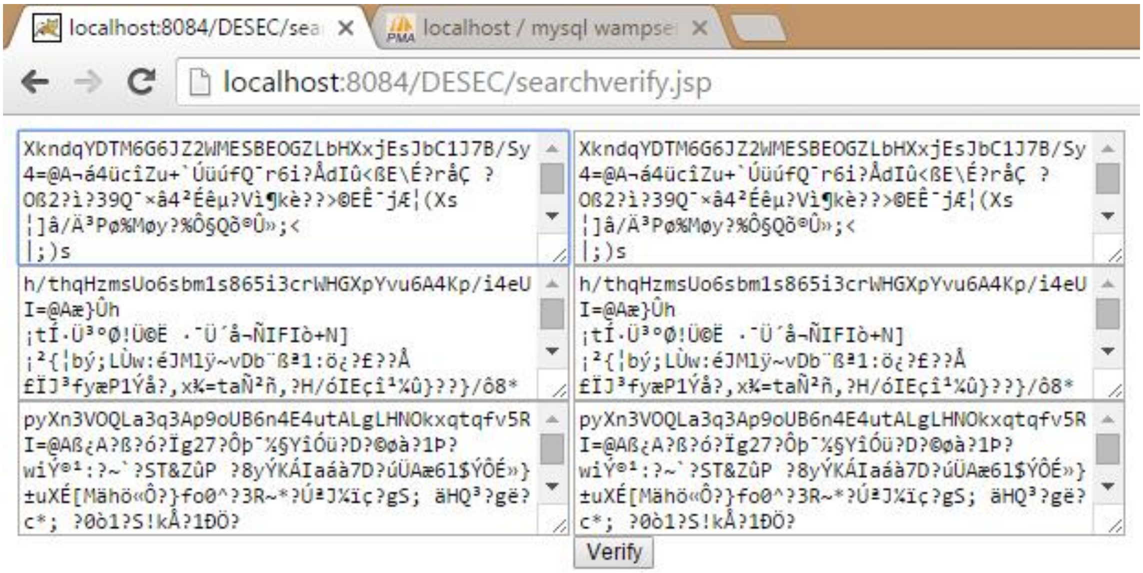
Integrity[14] of the any data refers that the original representation of data in the system. Means the present data is the proper representation of the original data or not. the integrity ensures that data has not been modified by an unauthorized user or person. the data integrity is very most important for data. in simple language we can say that the data integrity of data refers to the The accuracy and consistency of stored data[1].

7.5. Non-Repudiation:-

The Non- repudiation[14] ensures that the data provided by sender is same found at receiver end or cloud storage network. The Non-Repudiation is proofs the integrity of the user data. The user can also use the hash value generated by SHA-2 [5] for ensuring the integrity of the data[1].

8. Implementation Details and Results

To implement proposed framework java script which is one of the three languages called HTML, CSS, is used over NETBEANS IDE simulator. As mentioned above NETBEANS simulator provide an enhanced functionality to implement projects in java, java script and some other languages. In this dissertation an enhanced security of user data in all three public, private and hybrid sections with the use of various encryption algorithms like AES(Advanced Encryption algorithm)[16], Blowfish , IDEA(International Data Encryption Algorithm), SAES and SHA-2(Secure Hashing Algorithm).In below figures a output of the implementation or how the encrypted file stored in cloud of the project is presented.



```
XkndqYDTM6G6JZ2WMESBEOGZLbHXxjEsJbC1J7B/Sy
4=@A¬á4üciZu+`ÚüúfQ¯r6i?ÅdIû<ßE\É?råÇ ?
Oß2?ì?39Q¯×â4²Éêµ?Vì¶kè??>®EÊ¯jÆ¦(Xs
¦]â/Ä³Pø%Møy?%Ô§Qõ®Û»;<
|;)s

h/thqHzmsUo6sbm1s865i3crWHGXpYvu6A4Kp/i4eU
I=@Aæ}Ûh
¡tÍ·Ü³°Ø!Ü©Ë ·¯Ü´å¬ÑIFIò+N]
¡²{¦bý;LÙw:éJM1ÿ~vDb¨ßª1:ö¿?£??Å
£ÏJ³fyæP1Ýå?,x¾=taÑ²ñ,?H/óIEçî¹¼û}??}/ô8*

pyXn3VOQLa3q3Ap9oUB6n4E4utALgLHNOkxqtqfv5R
I=@Aß¿A?ß?ó?Ïg27?Ôþ¯%§YîÓü?D?®øà?1Þ?
wiÝ®¹:?~`?ST&ZûP ?8yÝKÁIaáà7D?úÜAæ61$ÝÔÉ»}
±uXÉ[Mähö«Ô?}fo0^?3R~*?Úª J¼ïç?gS; äHQ³?gë?
c*; ?0ò1?S!kÅ?1ÐÖ?
```

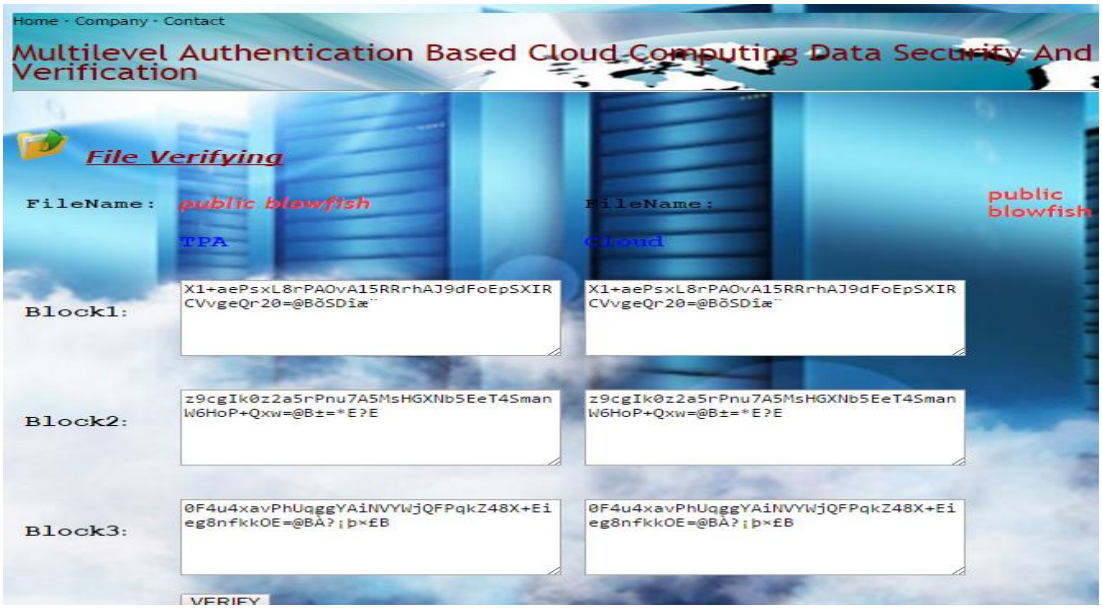
```
XkndqYDTM6G6JZ2WMESBEOGZLbHXxjEsJbC1J7B/Sy
4=@A¬á4üciZu+`ÚüúfQ¯r6i?ÅdIû<ßE\É?råÇ ?
Oß2?ì?39Q¯×â4²Éêµ?Vì¶kè??>®EÊ¯jÆ¦(Xs
¦]â/Ä³Pø%Møy?%Ô§Qõ®Û»;<
|;)s

h/thqHzmsUo6sbm1s865i3crWHGXpYvu6A4Kp/i4eU
I=@Aæ}Ûh
¡tÍ·Ü³°Ø!Ü©Ë ·¯Ü´å¬ÑIFIò+N]
¡²{¦bý;LÙw:éJM1ÿ~vDb¨ßª1:ö¿?£??Å
£ÏJ³fyæP1Ýå?,x¾=taÑ²ñ,?H/óIEçî¹¼û}??}/ô8*

pyXn3VOQLa3q3Ap9oUB6n4E4utALgLHNOkxqtqfv5R
I=@Aß¿A?ß?ó?Ïg27?Ôþ¯%§YîÓü?D?®øà?1Þ?
wiÝ®¹:?~`?ST&ZûP ?8yÝKÁIaáà7D?úÜAæ61$ÝÔÉ»}
±uXÉ[Mähö«Ô?}fo0^?3R~*?Úª J¼ïç?gS; äHQ³?gë?
c*; ?0ò1?S!kÅ?1ÐÖ?
```

Fig.6. Data stored in cloud via Private Section

The Fig.6 shows the how to Save data of Private phase in the cloud storage. In the private section the data is encrypted with the help of advanced encrypted algorithm AES and then apply the SHA-2 for generate the token and this token append with user data. here differentiate between data and token we use "@A" symbol in stored file. Before the @A hash key is stored and after @A user data is stored in cloud. The data of private phase only access with the help of token key otherwise data can't be access.


Home · Company · Contact
Multilevel Authentication Based Cloud Computing Data Security And Verification
File Verifying
VERIFY

FileName: public blowfish

TPA

FileName: public blowfish

Cloud

Block1:

```
X1+aePsxL8rPAOvA15RRrhAJ9dFoEpSXIR
CVvgeQr20=@BõSDîæ¨
```

```
X1+aePsxL8rPAOvA15RRrhAJ9dFoEpSXIR
CVvgeQr20=@BõSDîæ¨
```

Block2:

```
z9cgIk0z2a5rPnu7A5MsHGXNb5EeT4Sman
W6HoP+Qxw=@B±=*E?E
```

```
z9cgIk0z2a5rPnu7A5MsHGXNb5EeT4Sman
W6HoP+Qxw=@B±=*E?E
```

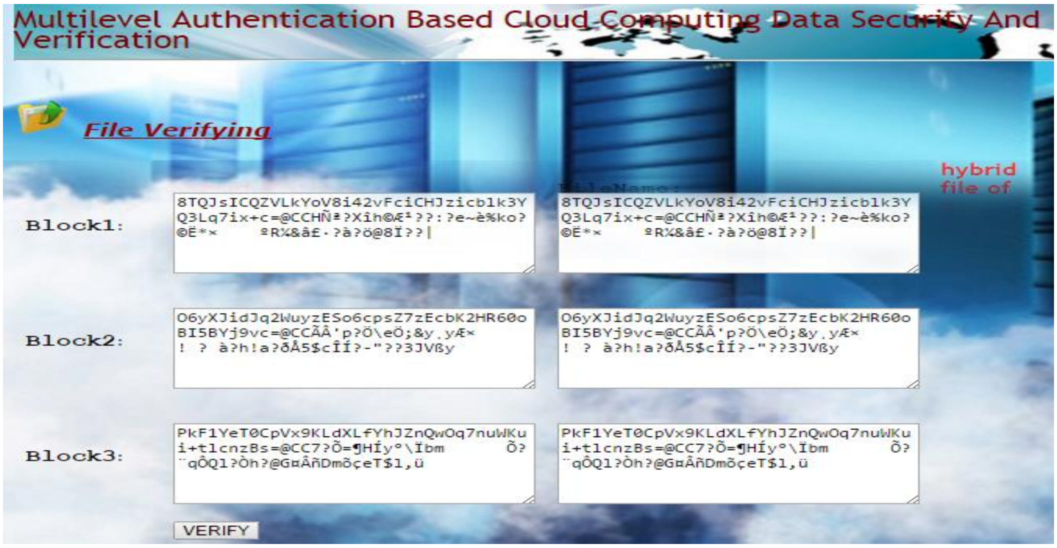
Block3:

```
0F4u4xavPhUqggYAiNVYWjQFPqkZ48X+Ei
eg8nfkkOE=@BÀ?¡þ×£B
```

```
0F4u4xavPhUqggYAiNVYWjQFPqkZ48X+Ei
eg8nfkkOE=@BÀ?¡þ×£B
```

Fig.7. Data stored in cloud via Public Section

The Fig.7 shows the how to Save data of Public phase in the cloud storage. Uploaded user data is divided into the three blocks it means the data is stored in three different locations in three parts so it should be more secure for hacking and various attacks in data. the public section the data firstly encrypted with blowfish then apply the SHA_2 algorithm on encrypted data and generate a unique token or hash function. This token append in stating of data and for understanding the encrypted data and hash value we use "@B" symbol in encrypted data. Before the @B symbol there is token and after @B symbol data is stored in cloud storage as shown in the figure7.



Multilevel Authentication Based Cloud Computing Data Security And Verification

File Verifying

hybrid file of

Block1:

```
8TQJsICQZVLkYoV8i42vFciCHJzicblk3Y
Q3Lq7ix+c=@CCHÑª?Xîh©Æ¹??:?e~è%ko?
©Ë*×     ºR¼&â£·?à?ö@8Ï??|
```

```
8TQJsICQZVLkYoV8i42vFciCHJzicblk3Y
Q3Lq7ix+c=@CCHÑª?Xîh©Æ¹??:?e~è%ko?
©Ë*×     ºR¼&â£·?à?ö@8Ï??|
```

Block2:

```
O6yXJidJq2WuyzESo6cpsZ7zEcbK2HR60o
BI5BYj9vc=@CCÃÂ'p?Ö\eÖ;&y¸yÆ×
! ? à?h!a?ðÅ5$cÎÍ?-"??3JVßy
```

```
O6yXJidJq2WuyzESo6cpsZ7zEcbK2HR60o
BI5BYj9vc=@CCÃÂ'p?Ö\eÖ;&y¸yÆ×
! ? à?h!a?ðÅ5$cÎÍ?-"??3JVßy
```

Block3:

```
PkF1YeT0CpVx9KLdXLfYhJZnQwOq7nuWKu
i+tlcnzBs=@CC7?Õ=¶HÍy°\Ïbm       Õ?
¨qÔQ1?Òh?@G¤ÅñDmõçeT$1,ü
```

```
PkF1YeT0CpVx9KLdXLfYhJZnQwOq7nuWKu
i+tlcnzBs=@CC7?Õ=¶HÍy°\Ïbm       Õ?
¨qÔQ1?Òh?@G¤ÅñDmõçeT$1,ü
```

Fig.8. Data stored in cloud via Hybrid Section

The Fig.8 shows the File upload by user in with the help of Hybrid phase Tier two. In this phase two level encryption is used. The Uploaded user data is divided into the three blocks it means the data is stored in three different locations in three parts so it should be more secure for hacking and various attacks in data In this phase the uploaded file firstly encrypted with blowfish technique and then IDEA technique is applied. In this phase the user data is encrypted with these two techniques and SHA_2 algorithm is applied on encrypted data and hash key is generated in this phase .This hash key append in stating of data and for understanding the encrypted data and hash value we use "@CC" symbol in encrypted data. Before the @CC symbol there is Hash value and after @CC symbol data is stored in cloud network.

9. Results Analysis

In this section a result analysis for the proposed model is presented. a comparison table is shown between the various encryption scheme that is used in all three sections and enhance the efficiency of the encryption in public, private and hybrid section and provide a speedy way to encrypt data with different-different techniques and save the encrypted data in cloud storage. The Execution time of hybrid section here we used various encryption algorithm SAES, Blowfish and IDEA respectively in tier one and two level encryption in tier two. The execution time is the time to upload the file, encrypt the file and save into the cloud storage network here we take a fixed size file to uploading purpose it vary for different-different file sizes.

Table 1. Execution Result and Compare Analysis in Various Techniques.

Phases/sections		Execution time (in m. seconds)	Key size (in bits)	Block size (in bits)	Security Level
Private phase		348 ms	32 bit	128 bits	Highly Secure
Public Phase		583 ms	32bit	64bits	Less Secure
Hybrid Phase	Tier One	137 ms	128 bits	64bits	More secure as compare to public but less secure as private phase
		460 ms	16 bits	16bits	
		92 ms	32bit	64bits	
	Tier Two	197 ms	128/32 bit	64 bits	

In the proposed model there are various encryption technique is used which takes data from the user then encrypt data, thus that technique increases the efficiency of the whole process and a SHA-2 a hashing algorithm is used to generate hash value of the encrypted file. That hash value is used for the verification purpose by the TPA and the owner of the data. With the help of hash key file can be accessed otherwise not. Hash value of the file provided to the TPA by the user then TPA match that value with HASH value of the file that are stored at the cloud server. if match found then that file provided to the TPA for auditing or verification purpose. Execution time, key length, block size which is generated by the encryption algorithm is taken as parameter to compare proposed technique with existing technique. Table also shows the security level in all three sections and Integrity Verification technique which is used in proposed model.

10. Conclusion

Here The proposed cloud storage security model provides a highly secure cloud environment by introducing the three sections Private, public And Hybrid section to store user data based on the user choices and security characteristics like authentication, confidentiality, integrity, availability, non-repudiation, data security, and privacy of data. The proposed framework restricts unauthorized entities to get control of the user’s data by implementing double encryption techniques and authentication mechanisms. The data is stored in cloud in encrypted form and contain different-different hashing key or token append with encrypted data. In all three sections user data is encrypted in different- different algorithms. It also provides protection against various security breaches such as brute force attack, masquerade attack, data tampering, and cryptanalysis of integrity key. It also enables the cloud user to choices the encryption techniques in hybrid section, in tier one and tier two according their need, security of data etc.

11. Future Work

This proposed Framework has been implemented on text files and directly file input by user which can be further enhanced to encrypt the all files like audio file, pdf, mp3 file and video files also. And The confidentiality can also be enhanced by introducing the some more combinations of encryption techniques in all the three private, public and hybrid sections.

References

[1] Mandeep Kaur, and Manish Mahajan, “Implementing Various Encryption Algorithms to -Enhance

The Data Security of Cloud in Cloud Computing”, International Journal of Computer Science &Information Technology Volume: 2, pp. 831-835, 2012.

[2] Wood K, Pereira E. (Nov.2010) 'An Investigation into CLoud Configuration and Security', 2010 International Conference for Internet Technology and Secured Transactions, 1-6.

[3] Expert Group Report, K. Jeffery [ERCIM], B. Neidecker-Lutz [SAP Research]: “The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond “2010 (2010)Elsevier.

[4] Syed rizvi, Katie cover, Christopher gates, “A trusted third party(TTP) based encryption scheme for ensuring data confidentiality in cloud environment”, Procedia Computer Science 36 (2014) 381 – 386, Elsevier.

[5] Robert P. McEvoy, Francis M. Crowe Colin, CMurphyWilliam Marnane Optimisation of the SHA-2 Family of Hash Functions on FPGAs” March 2, 2006. ISBN: 0-7695-2533-4 pp: 317-322 Elsevair.

[6] Musa, M., Schaefer, E. F., and Wedig, S. 2003. ”A Simplified AES Algorithm and its Linear and Differential Cryptanalysis,” Cryptologia 27(2), 148 - 177.

[7] Krešimir Popović, Željko Hocenski” Cloud computing security issues and challenges” MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[8] Ranjit Kaur, Raminder Pal Singh ”Enhanced Cloud Computing Security andIntegrity Verification via Novel Encryption Techniques” 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[9] Stallings, W. 2002. ”The Advanced Encryption Standard,” Cryptologia 26(3), 165 - 188. University of Texas.

[10] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter” Cloud Computing A Practical Approach”, TATA McGRAW-HILL Edition 2010.

[11] Mr. Bhavesh Rahulkar#1, Mr. Praveen Shende#2” Data Encryption by Blowfish Encryption Algorithm to Protect Data in Public Cloud" International Journal of Research in Advent Technology, Vol.2, No.7, July 2014 E-ISSN: 2321-9637.

[12] Bruce Schneier, Dr. Dobb's” The Blowfish Encryption Algorithm” Journal, v.19, n. 4, April 1994, pp. 38-40.

[13] G. Manikandanet al., “A Hybrid Approach for Security Enhancement by Modified Crypto-Stegno Scheme”, European Journal of Scientific Research, Vol. 2, pp: 206-212, 2011.

[14] Manpreet kaur, Hardeep Singh “A Review of Cloud Computing Security Issues” I.J. Education and Management Engineering, 2015, 5, 32-41.

[15] Published Online October 2015 in MECS (http://www.mecs-press.net) DOI: 10.5815/ijeme.2015.05.04.

[16] Sumit Goyal “Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review” International Journal of Computer Network and Information Security(IJCNIS) ISSN: 2074-9090 (Print), ISSN: 2074-9104 (Online) DOI: 10.5815/ijcnis Published By: MECS Publisher.

[17] Omer K. Jasim Mohammad, Safia Abbas, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem” Innovative Method for Enhancing Key Generation and Management in the AES-Algorithm” International Journal of Computer Network and Information Security(IJCNIS) ISSN: 2074-9090 (Print), ISSN: 2074-9104 (Online) DOI: 10.5815/ijcnisPublished By: MECS Publisher.

[18] Seyyed Yasser hashemi, Parisa Sheykhi Hesarlo” Security, Privacy and Trust Challenges in Cloud Computing and Solutions” I.J. Computer Network and Information Security, 2014, 8, 34-40.

[19] Published Online July 2014 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2014.08.05.

Authors' Profiles

Deepak Soni - He recived B.E. Degree in Information Technology from Radharaman Institute Technology & Science Bhopal. He is currently pursuing the M.Tech in Information Technology at state university, RGPV Bhopal (Madhya Pradesh). His research interests include Data Security Encryption Scheme Over Cloud Storage.(1School of Information Technology, RGPV University Bhopal).

Nishchol Mishra – He received the Ph.D. degree in computer science and engineering. His research interests include Mining over Social Media Data. He is currently Assistant Professor with state technical university of Madhya Pradesh, RGPV Bhopal.**(**2School of Information Technology, RGPV University Bhopal).

How to cite this paper: Deepak Soni, Nishchol Mishra,"Multilevel Authentication based Data Security and Verification over Cloud Computing Environment", International Journal of Education and Management Engineering(IJEME), Vol.7, No.5, pp.56-68, 2017.DOI: 10.5815/ijeme.2017.05.06