International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 15 Issue 1 –MAY 2015

Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques

RANJIT KAUR
M.Tech Scholar, School of Computer Science & Engg.
Lovely Professional University, Phagwara, Punjab, India.
geet18@live.com

RAMINDER PAL SINGH
Asst. Prof., School of Electronics and Communication.
Lovely Professional University, Phagwara, Punjab, India.
rpwilkhu@hotmail.com

***Abstract*-- Cloud computing is a revolutionary movement in the area of IT industry that provides storage, computing power, network and software as an abstraction and as a service, on demand over the internet, which enables its clients to access these services remotely from anywhere, anytime via any terminal equipment. Since cloud has modified the definition of data storage from personal computers to the huge data centers, security of data has become one of the major concerns for the developers of cloud. In this paper a security model is proposed, implemented in Cloud Analyst to tighten the level of cloud storage security, which provides security based on different encryption algorithms with integrity verification scheme. We begin with the storage section selection phase divided into three different sections Private, Public, and Hybrid. Various encryption techniques are implemented in all three sections based on the security factors namely authentication, confidentiality, security, privacy, non-repudiation and integrity. Unique token generation mechanism implemented in Private section helps ensure the authenticity of the user, Hybrid section provides On Demand Two Tier security architecture and Public section provides faster computation of data encryption and decryption. Overall data is wrapped in two folds of encryption and integrity verification in all the three sections. The user wants to access data, required to enter the user login and password before granting permission to the encrypted data stored either in Private, Public, or Hybrid section, thereby making it difficult for the hacker to gain access of the authorized environment.**

***Keywords*— AES, SAES, SHA-1, IDEA, Blowfish, Token.**

I. INTRODUCTION

Cloud Computing enables its clients to store their data on remote database via internet and make use of various other service models provided by it such as Software as a Service, Infrastructure as a Service, and Platform as a Service. Clients are charged for the services, they are using based on some metering mechanism, adopted by the cloud service provider [15]. The primary benefit of cloud computing is that the clients do not need to disburse for the infrastructure, its deployment, the expertise to handle and maintain such infrastructure. As the client stores the most important data externally on the cloud storage so it becomes the prime duty of service provider to guarantee the protection of his/her data from being disclosed to any other person and also guarantee the integrity of stored data. Security is one of the major problems of cloud computing environment [4]. Although the cloud service provider takes several measures to protect data from intruder, hacker or some unauthorized person, still security is an ongoing research topic in cloud. There is a great need to implement tight security measures so that no intruder and not even the cloud service provider can get and make changes in user's data.

The proposed security model provides highly secure cloud environment by making use of various encryption techniques at different levels along with the notification, if anything malicious happens to the client's data. The model works as a strong wall against many security breaches that are affecting the performance and functioning of cloud. Encryption is the primary security technique used in the model. Encryption converts data into cipher form to shield it against any unauthorized access and can be decrypted by the authorized person only, with a valid decryption key [16]. The data gets stored in encrypted form in any of the three sections Private, Public, or Hybrid selected by the user according to own requirements. In all the three sections different encryption algorithms have been deployed. This model provides complete security architecture by employing authentication scheme, storing data in encrypted form in different sections based on security parameters (confidentiality, privacy, integrity, non-repudiation, and accessibility), generating unique tokens for double authentication, using SHA-1 for integrity verification.

The paper is organized as: In Section 2 related work for data security summarized. In Section 3 Cloud Storage Security Model is proposed. Section 4 provides the security analysis of the proposed model. In Section 5 implementation results are shown. Section 6 concludes the paper. In section 7 the future scope has been described.

II. RELATED WORK

A lot of research work has been done to maintain the security and privacy of cloud storage. Data integrity is another measure to take into account to ensure the reliability and truthfulness of data. So many techniques and models have been proposed in this direction, few of which are as follows:

A. Liming Fang et al., (2013) [1], PEKS model is presented in this paper which provides security against chosen cipher text attack, chosen keyword attack, and keyword guessing attack.

IND-SCF-CKCA (provides protection against inside enemy) and IND-KGA (provides protection against outside enemy) the two vital security concepts are presented.

B. Nirmala et al., (2013) [2], a scheme called user authenticator is proposed, according to which the data owner first divides the data file into equal blocks and then performs AES on each block, after that hash code is generated for each of the blocks. After performing all these steps the encrypted file is stored on cloud and while downloading it, user requests the cloud to generate hash code for the requested file and then user matches the hash code with its hash code in order to verify the integrity of data. All this work takes place at user side and cloud is used only for generating hash and storing encrypted data.

C. Eman M. Mohamed et al., (2012) [8], On-demand security software is provided to make a selection from eight encryption algorithms such as RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish. These algorithms are evaluated based on NIST statistical testing and implemented as Pseudo Random Number Generator (PRNG). Performance of the algorithm is measured by testing the encryption speed. Comparison among the eight algorithms is done based on P-value and rejection rate.

D. Sherif El-etriby et al., (2012) [7], a comparison of the eight encryption algorithms such as: AES, DES, 3DES, RC4, RC6, Two-Fish, and Blow-Fish have been performed, at desktop computer and at Amazon EC2 cloud computing environment. The algorithms are evaluated according to the randomness testing by using NIST statistical testing in cloud environment. Pseudo Random Number Generator (PRNG) is used to conclude the most appropriate method.

E. Pradeep Bhosale et al., (2012) [6], In order to provide a more secure cloud computing environment, 3D framework and digital signature with RSA algorithm is used. According to the used 3D structure the client first select the parameters among CIA and after that the digital signature is created by using MD5 algorithm and after that the data is encrypted by making use of the RSA algorithm and finally the ciphered data is stored on cloud environment.

F. G. Jai Arul Jose et al., (2011) [12], A security system is proposed which provides authentication, confidentiality, and integrity of user's data by joining the cloud computing framework with cluster load balancing, SSL over AES and secure session. Security model is divided into different layers.

G. Qin Liu et al., (2011) [14], R3 the time and attribute based re-encryption technique is proposed, using which the cloud server can automatically re-encrypt the user data based on its internal clock and manages and ensures the access control correctness.

H. Dimitrios Zissis et al., (2010), A Trusted Third Party Solution is proposed which provides solutions to maintain the integrity, confidentiality, privacy, and authenticity of the data and communications that takes place over the cloud environment.

Cloud computing architecture is partitioned into four layers of hardware, infrastructure, platform and application layer and the data has to go through all the four layers. Therefore an efficient security model must be developed to provide protection at each level. The proposed model has been designed by keeping all these points in mind which provides protection against various security attacks.

III. PROPOSED CLOUD STORAGE SECURITY MODEL

The proposed model provides a complete protection to the data stored on cloud storage 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. Several novel encryption techniques and other mechanisms are combined to shield data against unauthorized access and security breaches. The model works in two phases: the first phase deals with storing data securely on cloud storage. Second phase deals with data retrieval from cloud by enabling double authentication, integrity verification thereby providing data only to the legitimate user by passing all the security phases.

A. Phase 1 (Data Storage Phase):

During this phase, user first needs to login onto cloud to authenticate identity. This phase is further divided into sub phases (storage section selection and encryption phase, and integrity key generation).

a) Storage Section Selection and Encryption Phase:

Cloud offers three storage sections namely Private Section (Highly secure), Public Section (limited security), and Hybrid Section (desirable security) as shown in figure 1. The primary benefit of this storage selection scheme is that the cloud can offer the different levels of security to the users according to their own choice, it will provide totally 'pay as you choose' environment which means there will be different cost for the three sections and if user wants a very highly secure storage and money is not a problem then he can go for 'highly secure section'.

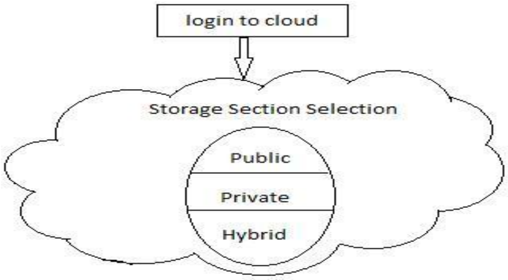


Fig 1: Storage Section Selection

As the user selects the appropriate section according to the data confidentiality aspect, cloud server converts the user's data into encrypted form by passing the data through the specified encryption technique in that particular section. The entire process of three sections is depicted in fig 2, 3, and 4 respectively.

Private Section:

As user selects the private section the steps depicted in fig 2 are applied on data. First of all input file gets encrypted into ciphered form with AES (Advanced Encryption Standard) technique.

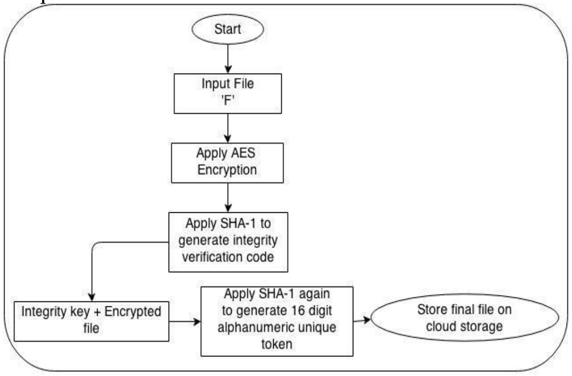

Start
Input File 'F'
Apply AES Encryption
Apply SHA-1 to generate integrity verification code
Integrity key + Encrypted file
Apply SHA-1 again to generate 16 digit alphanumeric unique token
Store final file on cloud storage

Fig 2: Private Section

Secondly the 16 digit integrity verification code of alphanumeric form is generated by applying SHA-1 (Secure Has Algorithm) on encrypted file and the then the integrity code is appended at the front of encrypted file. After that, SHA-1 is applied again to generate the 16 digit alphanumeric unique token for providing double authenticity mechanism at downloading time of file 'F'.

Private Section Data Storage Steps:

STEP 1: Select file to upload in the Private Section of cloud storage.

STEP 2: Enter the encryption key of 16 digits.

STEP 3: Encrypt the user file by applying AES algorithm.

STEP 4: Apply SHA-1 on the encrypted file to create a 16 digit integrity verification code.

STEP 5: Append the integrity verification code at the front of encrypted file before storing it on cloud storage.

STEP 6: Apply SHA-1 once again on the file to generate a unique token of 16 digits.

STEP 7: Provide unique token to the user, which is required at the time of downloading the file to authenticate user.

STEP 8: Store file on cloud storage.

Public Section:

The public section provides limited security. If user wants the faster computation, minimum cost of encryption and decryption, also if the data is not that much confidential then public section is the best choice.

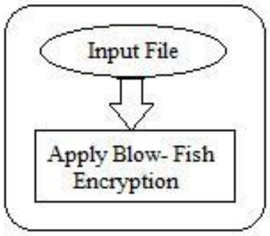


Fig 3: Public Section

Public Section Data Storage Steps:

STEP 1: Select file to upload in the Public Section of Cloud Storage.

STEP 2: Enter the encryption key of 16 digits.

STEP 3: Encrypt user file by applying Blow-Fish algorithm.

STEP 4: Apply SHA-1 to generate integrity verification code of 16 digits.

STEP 5: Append integrity verification code at the front of encrypted file.

STEP 6: Store the encrypted user file on cloud storage.

Hybrid Section:

Hybrid Section provides the Two Tier Security Architecture based on which user is allowed to select either tier 1 or tier 2 to store data on cloud. Tier 1 can be selected if the probability of hacking is low and also the data does not require highly protected environment. Tier 1 offers three encryption algorithms to select from SAES (Selective Advanced Encryption Standard), Blow- Fish, and IDEA (International Data Encryption Algorithm) as shown in fig 4. Tier 2 offers a combination of two encryption techniques to encrypt file 'F'. Input file first go through Blow- Fish and after that IDEA is applied on the encrypted file. This section provides a glimpse of Private and Public section by deploying SAES (based on AES), Blow- Fish, and IDEA in a combination.

So the user can make a choice of storage section selection by analyzing the various security aspects of data.

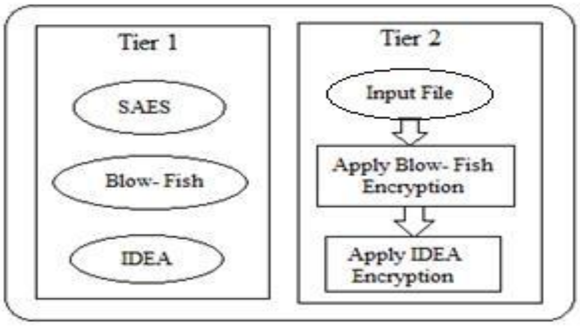


Fig 4: Hybrid Section (Two Tier Security Architecture)

Hybrid Section Data Storage Steps:

STEP 1: Select file to upload.

STEP 2: Enter encryption key of 16 digits.

STEP 3: IF TIER 1 is selected THEN provide options of SAES, IDEA and Blow-Fish encryption.

STEP 4: IF SAES is selected THEN encrypt user file with SEAS encryption.

STEP 5: IF Blow-Fish is selected THEN encrypt user file with Blow-Fish encryption.

STEP 6: IF IDEA is selected THEN encrypt user file with IDEA encryption.

STEP 7: Apply SHA-1 on encrypted file to generate 16 digits integrity checker code.

STEP 8: Append integrity checker code at the front of encrypted file before storing it on cloud storage.

STEP 9: Store alphabet 'S' at the first place of encrypted file to recognize the SAES encryption at the time of decryption. **STEP 10:** Store alphabet 'B' at the first place of encrypted file to recognize the Blow-Fish encryption at the time of decryption.

STEP 11: Store alphabet 'I' at the first place of encrypted file to recognize the IDEA encryption at the time of decryption.

STEP 12: IF TIER 2 is selected THEN firstly apply Blow Fish and then apply IDEA encryption on user file.

STEP 13: Repeat steps 7 and 8.

STEP 14: Store alphabet 'C' at the first place of encrypted File to recognize the TIER 2 (Blow-Fish + IDEA) encryption at the time of decryption.

b) Integrity Key Generation Phase:

After data encryption in the selected section the integrity verification key is generated by applying SHA-1 (Secure Hash Algorithm) on the ciphered file, which is stored on cloud by appending it at front of the encrypted file. This works as a checksum of 16 digit alphanumeric form, used to check whether the data is modified or not.

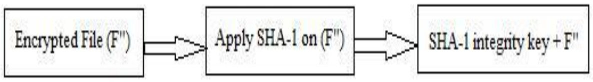


Fig 5: SHA-1 Integrity Key

The verification of data integrity is performed at cloud side when user requests the cloud provider to access the stored file. If the integrity has been sacrificed then a notification message is generated alerting the user about the unauthorized tampering of data.

B. Phase 2 (Data Retrieval Phase):

Now after storing the data successfully on cloud environment, the user will retrieve it back from cloud whenever required. Therefore the retrieval process should also be carried out with equally best schemes and techniques. In order to sustain the security of retrieval phase the entire procedure implemented in the storage phase is applied in the reverse process to offer a secure downloading of data. For retrieving stored data user first needs to register with user name and password on cloud to authenticate the identity as shown in fig 6.

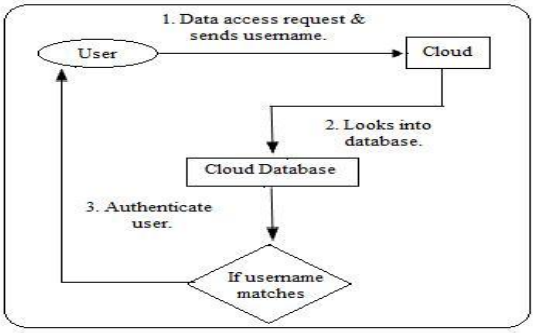


Fig 6: Data Access Request

After the valid authentication, user prompted to click on the 'download' button. After clicking on it, further user is requested to enter the valid password. Then user selects one of the sections. If the Private section is selected then the user has to enter the valid token which was generated at the time of uploading the data in private section. Further the entire process of Data Retrieval phase is explained in fig 7. As this model uses SHA-1 for integrity verification, the cloud server ensures the integrity by comparing the integrity code generated during download time with the one generated during upload time.

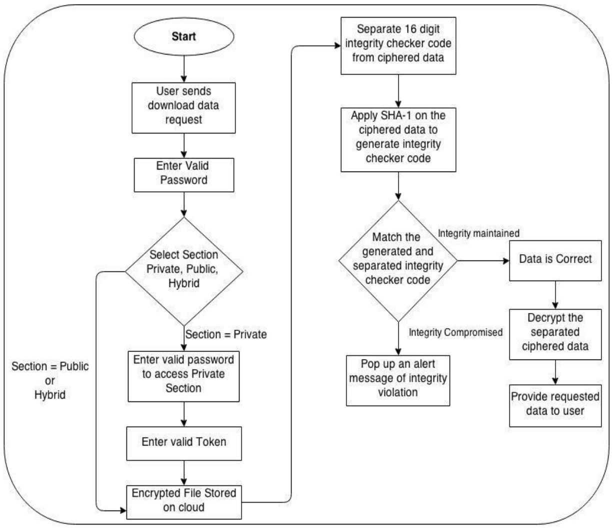

Start
User sends download data request
Enter Valid Password
Select Section Private, Public, Hybrid
Section = Private
Section = Public or Hybrid
Enter valid password to access Private Section
Enter valid Token
Encrypted File Stored on cloud
Separate 16 digit integrity checker code from ciphered data
Apply SHA-1 on the ciphered data to generate integrity checker code
Match the generated and separated integrity checker code
Integrity maintained
Data is Correct
Integrity Compromised
Pop up an alert message of integrity violation
Decrypt the separated ciphered data
Provide requested data to user

Fig 7: Data Retrieval Process

The process of data retrieval concludes that this model has implemented all the measures and techniques to safeguard data from unauthorized access, data leakage, and tampering of data etc.

IV. SECURITY ANALYSIS

The proposed model provides security and protection against a no. of security breaches, data leakage, modification etc. The designed model helps ensure the security against following issues in an efficient and effective manner.

a) Confidentiality

Data stored in a ciphered form on cloud storage by implementing different encryption techniques, makes it confidential from unauthorized users.

b) Security and Privacy

User required to first login to cloud with a valid username and password, ensures the security and privacy. Also the mechanism of token implemented in Private Section makes it highly secure by enabling double authentication of user.

c) Brute Force Attack

The encryption schemes are used in such a combination that makes it near to impossible for a hacker to apply brute force attack. The use of private key of length 16 characters in all the three sections makes it impossible for the hacker to know about the type of encryption technique used.

d) Data Tampering

Use of encryption, 16 characters key, token, username, and password provides protection against data tampering but still the data integrity needs to be verified. Use of SHA-1 ensures the data integrity by generating integrity checker code at the upload time and comparing it with the code generated at download time. If the code matches then the data has not tampered with. If code does not match then it signifies that the integrity of data has been sacrificed.

e) Loss of user identity and password

The design of private section provides protection eve if the user identity and password has been leaked. The mechanism of unique token protects against such type of situation. Since the user is required to enter the valid 16 digit unique token of alphanumeric form, generated at the time of uploading the file by cloud server provides highly secure and protected environment.

f) Non- Repudiation

Non- repudiation provides a proof of the data integrity and it guarantees that sender of data cannot deny that he/she has sent the same data and same is applicable at the receiver side also. The use of SHA-1 protect from such issues. Since SHA-1 code is irreversible which means one cannot create data from hash, so this ensures the integrity of data and provides non-repudiation scheme.

g) Masquerade Attack

The proposed model provides protection against masquerade attack. Since the user is required to first login with a username and password on cloud environment and after that further password is required to download data, which can be different from the first one. Also the use of token enforces double authentication checks. In case if an attacker gets password even then that will be of no use because of double authentication process.

h) Enhanced Level of Confusion

The key size used to encrypt the user data is same for all the encryption algorithms used in this research work, which enhanced the level of confusion for the attacker to guess the encryption technique applied in particular section. Also the integrity verification key generated by SHA-1 has been cut down to 16 digits instead of 40 digits which will prevent the attacker to know whether there is any integrity key is attached at the front of encrypted file (as implemented in this work) or not, by using this approach it will be near to impossible to get user data in its exact form.

V. IMPLEMENTATION RESULTS

The proposed security model is implemented on Cloud Analyst, tool for simulating and analyzing the huge cloud environments. Cloud Analyst is positioned on top of CloudSim. It provides all the features of CloudSim along with some extensions. It provides GUI that enables the users to configure and run the simulation experiments more easily and repeatedly.

Cloud Analyst also modified during this research work by adding one extra tab named ‘File Configuration’, to develop GUI for user for storing data on cloud as shown in fig 8.

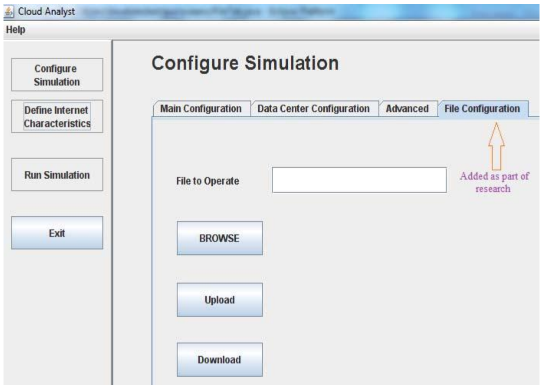


Fig 7: Proposed GUI with ‘File Configuration’ tab

The file uploaded by user in hybrid section stored in the encrypted manner as showed in figure 11 along with the integrity checker code and an alphabet (I, B, S, or C) attached at the front of ciphered data.

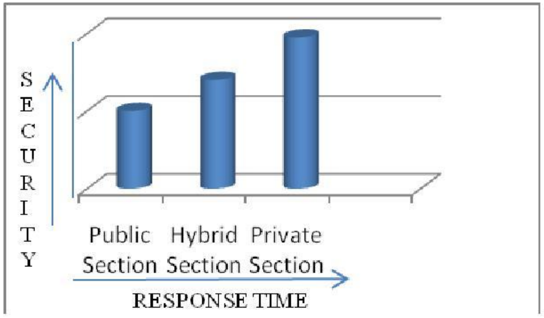
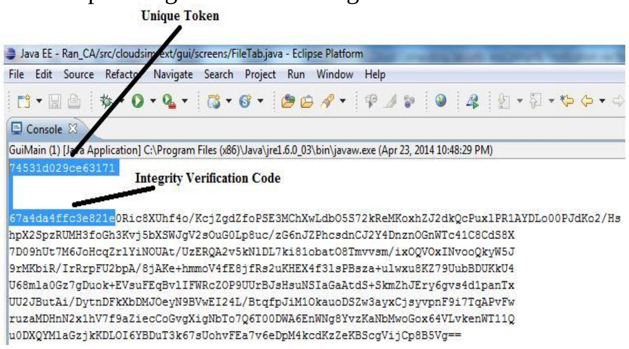


Fig 8: Security Evaluation

This graph shows the level of security provided by each section. It is clear that the private section is highly secure and protected. Also as the level of security increases the response time for uploading and downloading data also increases.


Unique Token
Integrity Verification Code
Java EE - Ran_CA/src/cloudsim/ext/gui/screens/FileTab.java - Eclipse Platform
File
Edit
Source
Refactor
Navigate
Search
Project
Run
Window
Help
Console

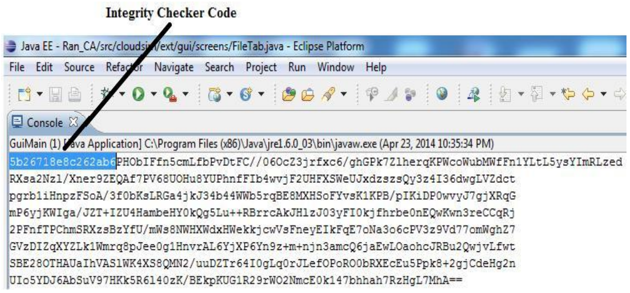
```
GuiMain (1) [Java Application] C:\Program Files (x86)\Java\jre1.6.0_03\bin\javaw.exe (Apr 23, 2014 10:48:29 PM)
74531d029ce63171


67a4da4ffc3e821e0Ric8XUhf4o/KcjZgdZfoPSE3MChXwLdb05S72kReMKoxhZJ2dkQcPux1PR1AYDLo00PJdKo2/Hs
hpX2SpzRUMH3foGh3Kvj5bXSWJgV2sOuG0Lp8uc/zG6nJZPhcsdnCJ2Y4DnznOGnWTc41C8CdS8X
7D09hUt7M6JoHcqZrlYiNOUAt/UzERQA2v5kN1DL7ki81obat08Tmvvsm/ixOQVOxINvooQkyW5J
9rMKbiR/IrRrpFU2bpA/8jAKe+hmmoV4fE8jfRs2uKHEX4f31sPBsza+ulwxu8KZ79UubBDUKkU4
U68mla0Gz7gDuok+EVsuFEqBvlIFWRcZOP9UUrBJsHsuNSIaGaAtdS+SkmZhJEry6gvs4d1panTx
UU2JButAi/DytnDFkXbDMJOeyN9BVwEI24L/BtqfpJiM1OkauoDSZw3ayxCjsyvpnF9i7TqAPvFw
ruzaMDHnN2x1hV7f9aZiecCoGvgXigNbTo7Q6T00DWA6EnWNg8YvzKaNbMwoGox64VLvkenWT11Q
u0DXQYMlaGzjkKDLOI6YBDuT3k67sUohvFEa7v6eDpM4kcdKzZeKBScgVijCp8B5Vg==
```

Fig 9: Encrypted File Stored on Cloud Storage Private Section

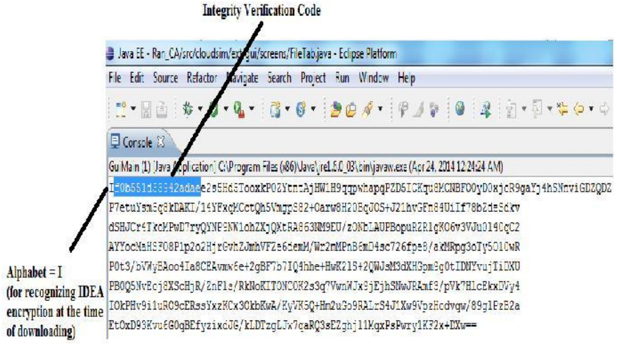
The file uploaded by user in private section stored in the encrypted manner as shown in figure 4.8 along with the integrity checker code attached at the front of ciphered data and also the unique token generated is being displayed in the figure.

The file uploaded by user in public section stored in the encrypted manner as shown in the figure 10 along with the integrity checker code attached at the front of ciphered data.



```
GuiMain (1) [Java Application] C:\Program Files (x86)\Java\jre1.6.0_03\bin\javaw.exe (Apr 23, 2014 10:35:34 PM)
5b26718e8c262ab6PHObIFfn5cmLfbPvDtFC//06OcZ3jrfxc6/ghGPk7ZlherqKPWcoWubMWfFn1YLtL5ysYImRLzed
RXsa2Nzl/Xner9ZEQAf7PV68UOHu8YUPhnfFIb4wvjF2UHFXSWeUJxdzszsQy3z4I36dwgLVZdct
pgrb1iHnpzFSoA/3f0bKsLRGa4jkJ34b44WWb5rqBE8MXHSoFYvsK1KPB/pIKiDP0wvyJ7gjXRqG
mP6yjKWIga/JZT+IZU4HambeHY0kQg5Lu++RBrrcAkJHlzJ03yFI0kjfhrbe0nEQwKwn3reCCqRj
2PFnfTPChmSRXzsBzYfU/mWs8NWHXWdxHWekkjcwVsFneyEIkFqE7oNa3o6cPV3z9Vd77omWghZ7
GVzDIZqXYZLk1Wmrq8pJee0g1HnvrAL6YjXP6Yn9z+m+njn3amcQ6jaEwLOaohcJRBu2QwjvLfwt
SBE28OTHAUaIhVASlWK4XS8QMN2/uuDZTr64I0gLq0rJLefOPoRO0bRXEcEu5Ppk8+2gjCdeHg2n
UIo5YDJ6AbSuV97HKk5R6l40zK/BEkpKUG1R29rWO2NmcE0k147bhhah7RzHgL7MhA==
```

Fig 10: Encrypted File Stored on Cloud Storage Public Section


Integrity Verification Code
Alphabet = I
(for recognizing IDEA encryption at the time of downloading)
Java EE - Ran_CA/src/cloudsim/ext/gui/screens/FileTab.java - Eclipse Platform
File
Edit
Source
Refactor
Navigate
Search
Project
Run
Window
Help
Console

```
GuiMain (1) [Java Application] C:\Program Files (x86)\Java\jre1.6.0_03\bin\javaw.exe (Apr 24, 2014 12:24:24 AM)
I50b551d33342adaee2s5Hd5TooxkP0ZYtntAjHW1H9qqpwhapqPZD5ICKqu8KCNBFOOyD0xjcR9gaYj4hSNnviGDZQDZ
P7etuYsm5q8kDAKI/14YFxqKCctQh5Vmgp382+Oarw8H20BqJOS+J21hvGFn84UiIf78b2de5ckv
dSHJCr4TkcMPwD7ryQYNP9NW1ohZXjQXtRA863NM9EU/zONbLAUPBopuRZR1gKO6v3VJu0140qC2
AYYocMaHSF08P1p2o2HjrGvhZJmhVFZe6demM/Wr2mMPnB6mD4sc726fpe8/aKMRpg3oTy5O10wR
P0t3/bVWyBAoo4Ia8CEAvmw6e+2gBF7b7IQ4hhe+HwK215+2QWJsM3dXHGpm9g0tIDNYvujTiDXU
PB0Q5NvEcj8XScHjR/2nFls/RkNoKITONCOK2s3q7VwnWJx9jEjhSNwJRAmf3/pVk7HlcEkxDVy4
IOkPHv9i1uRO9cERssYxzKCx3OkbKwA/KyVK5Q+Hm2uGo9RALrS4J1Xw9VpzHcdvqw/89g1PzB2a
EtOxD93Kvu6G0qBEfyzixcJG/kLDTzgLJx7qaRQ3sEZghj11KqxPsPwry1KF2x+DXw==
```

Fig 11: Encrypted File Stored on Cloud Storage Hybrid Section

Hybrid Section Decryption Algorithm Recognition Steps:

```
IF alphabet =
      I THEN
            Apply IDEA
decryption IF alphabet = B
      THEN
            Apply Blow-Fish
decryption IF alphabet = S
      THEN
            Apply SAES
decryption IF alphabet = C
      THEN
            Firstly apply IDEA decryption and then
            apply Blow-Fish decryption.
```

VI. CONCLUSION

The proposed cloud storage security model provides a highly secure cloud environment by introducing the three sections to store user data base on the security parameters namely authentication, confidentiality, integrity, availability, non-repudiation, security, and privacy. It restricts unauthorized entities to get control of the user's data by implementing double authentication mechanisms. 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 user to select the encryption techniques in hybrid section, according to the various factors associated with data such as cost, security etc.

VII. FUTURE SCOPE

This model can further be enhanced by introducing the encrypted data searching scheme by implementing the technique of index building for ciphered data. The confidentiality can also be enhanced by introducing the different combinations of encryption techniques in all the three sections. Also a procedure can be incorporated which classify data automatically in three sections based on the factors of confidentiality, integrity, and availability.

REFERENCES

[1] Liming Fang, Willy Susilo, Chunpeng Ge, and Jiandong Wang,"Public Key Encryption With Keyword Search Secure Against Keyword Guessing Attacks Without Random Oracle", Elsevier, pp. 221-241, 2013.

[2] V. Nirmala, R. K. Shivanadhan, and Dr. R. Shanmuga Lakshami, "Data Confidentiality and Integrity Verification using User Authenticator scheme in Cloud", International Conference on Green High Performance Computing, IEEE, pp. 1-5, 2013.

[3] Mr. Prashant Rewagad, and Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", International Conference on Communication Systems and Network Technologies, IEEE, 2013.

[4] 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.

[5] Afnan Ullah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, and Karim Djemame, "Security Risks and their Management in Cloud Computing", International Conference on Cloud Computing Technology and Science, IEEE, pp. 121-128, 2012.

[6] Pradeep Bhosale, Priyanka Deshmukh, Girish Dimbar, and Ashwini Deshpande, "Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption", International Journal of Engineering Research & Technology Volume: 1, Issue: 8, 2012.

[7] Sherif El-etriby, and Eman M. Mohamed, "Modern Encryption Techniques for Cloud Computing", ICCIT, pp. 800-805, 2012.

[8] Eman M. Mohamed, Hatem S.Abdelkader, and Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", International Conference on Informatics and Systems, 2012.

[9] Mark D. Ryan, "Cloud computing security: The Scientific Challenge, and A Survey of Solutions", Elsevier, pp. 1-6, 2012.

[10] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, and Yunlu Chen, "Security and Privacy for Storage and Computation in Cloud Computing", Elsevier, pp. 1-16, 2012.

[11] Miao Zhou, Yi Mu, Willy Susilo, Jun Yan, Liju Dong , "Privacy Enhanced Data Outsourcing in the Cloud", Elsevier Journal of Network and Computer Applications, pp. 1367-1373, 2012.

[12] G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology Volume: 1, Issue: 1, pp. 18-22, 2011.

[13] Amanjot Kaur, and Manisha Bhardwaj, "Hybrid Encryption for Cloud Database Security", International Journal of Engineering Science & Advanced Technology Volume: 2, Issue: 3, pp. 737-741, 2011.

[14] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, "Reliable Re-encryption in Unreliable Clouds", IEEE, pp. 1-5, 2011.

[15] Rajkumar Buyya, "Mastering Cloud Computing", Elsevier, USA, p. 469, 2013.

[16] Zaigham Mahmood, "Cloud Computing for Enterprise Architectures", Springer, UK, p. 346, 2011.

[17] Borko Furht, "Handbook of Cloud Computing", Springer, New York, p. 655, 2010.

[18] Judith Hurwitz, "Cloud Computing for Dummies", Willey Publishing, p. 339, 2010.

[19] Anthony T. Velty, "Cloud Computing A Practical Approach", McGraw Hill, New York, p. 353, 2010.

[20] William Stallings, "Cryptography and Network Security Principles and Practice", Pearson, p. 743.

[21] Chen Jia Xue Dongyue, and Lai Xuejia, "An Analysis of International Data Encryption Algorithm against Differential Cryptanalysis", The National Natural Sciences Foundation of China and PRP program of SJTU.