# STRENGTHENING CLOUD SECURITY AND DATA INTEGRITY WITH INNOVATIVE ENCRYPTION METHODS

MR. SHIVAM KUMAR
Research Scholar, CSE Department, Sandip University, Madhubani, BIHAR, INDIA
Email: shivammishra121.sm@gmail.com

DR. SHAMBHU KUMAR SINGH
Assistant Professor & Head, CSE Department, Sandip University, Madhubani, BIHAR, INDIA
Email: shambhu.singh@sandipuniversity.edu.in

***Abstract* - Cloud computing has transformed the IT industry by offering storage, computing power, network, and software services on demand over the internet. This allows clients to access these services remotely from anywhere, at any time, using any device. With this shift from personal computer storage to massive data centers, data security has become a major concern for cloud developers.**

***In this paper, we propose a security model implemented in Cloud Analyst to enhance cloud storage security. This model uses various encryption algorithms and an integrity verification scheme to protect data. The storage selection phase is divided into three sections: Private, Public, and Hybrid. Each section employs different encryption techniques based on factors such as authentication, confidentiality, security, privacy, nonrepudiation, and integrity. In the Private section, a unique token generation mechanism ensures user authenticity. The Hybrid section offers an On Demand Two Tier security architecture, while the Public section focuses on faster data encryption and decryption.***

***Overall, data is secured with two layers of encryption and integrity verification across all three sections. Users must enter their login and password to access the encrypted data in any section, making it challenging for hackers to penetrate the secure environment.***

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

## I. INTRODUCTION

Cloud computing allows clients to store their data on remote databases via the internet and use various service models such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Clients are charged for the services they use based on a metering mechanism set by the cloud service provider. The main advantage of cloud computing is that clients don’t have to pay for the infrastructure, its deployment, or the expertise needed to manage and maintain it. Since clients store their important data externally on cloud storage, it’s the service provider’s responsibility to ensure this data is protected and remains intact. Security is a major concern in the cloud computing environment.

Despite the cloud service provider’s efforts to protect data from intruders, hackers, and unauthorized access, security remains an ongoing research topic. There’s a strong need for stringent security measures to ensure that neither intruders nor even the cloud service provider can access or alter users’ data.

The proposed security model offers a highly secure cloud environment using various encryption techniques at different levels. It also notifies clients if there’s any malicious activity involving their data. This model acts as a robust defense against many security breaches that could impact the cloud's performance and functionality. Encryption is the primary security method used in this model. It converts data into a cipher form to protect it from unauthorized access, and only authorized individuals with a valid decryption key can convert it back.

Data is stored in encrypted form in one of three sections—Private, Public, or Hybrid—selected by the user based on their needs. Different encryption algorithms are used in each section. This model provides a comprehensive security architecture by implementing authentication schemes, storing data in encrypted form based on security parameters (such as confidentiality, privacy, integrity, nonrepudiation, and accessibility), generating unique tokens for double authentication, and using SHA-1 for integrity verification.

The paper is organized as follows: Section 2 summarizes related work on data security. Section 3 proposes the Cloud Storage Security Model. Section 4 provides a security analysis of the proposed model. Section 5 presents the implementation results. Section 6 concludes the paper. Section 7 describes future scope.

## II. RELATED WORK

A lot of research has been done to ensure the security and privacy of cloud storage. Maintaining data integrity is crucial for ensuring the reliability and truthfulness of data. Several techniques and models have been proposed in this area, and some notable ones include:

### A. Liming Fang et al., (2013) [1]

This paper presents the PEKS model, which offers security against chosen ciphertext attacks, chosen keyword attacks, and keyword guessing attacks. It introduces two important security concepts: IND-SCF-CKCA (protecting against internal threats) and IND-KGA (protecting against external threats).

### B. Nirmala et al., (2013) [2]

The authors propose a scheme called "user authenticator." Here, the data owner divides the data file into equal blocks, encrypts each block with AES, and generates a hash code for each block. The encrypted file is then stored in the cloud. When downloading, the user requests the cloud to generate a hash code for the requested file and matches it with the original hash code to verify data integrity. This process occurs on the user side, with the cloud used only for generating hashes and storing encrypted data.

### C. Eman M. Mohamed et al., (2012) [8]

This paper provides on-demand security software that lets users choose from eight encryption algorithms (RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish). These algorithms are evaluated using NIST statistical testing and implemented as Pseudo Random Number Generators (PRNG). Their performance is measured by encryption speed, and comparisons are made based on P-value and rejection rate.

### D. Sherif El-etriby et al., (2012) [7]

The authors compare eight encryption algorithms (AES, DES, 3DES, RC4, RC6, Two-Fish, and Blowfish) on a desktop computer and in the Amazon EC2 cloud environment. The algorithms are assessed for randomness using NIST statistical testing in the cloud environment, with PRNG used to determine the most suitable method.

### E. Pradeep Bhosale et al., (2012) [6]

To create a more secure cloud computing environment, this paper uses a 3D framework and digital signature with the RSA algorithm. Clients first select parameters among CIA (Confidentiality, Integrity, Availability), create a digital signature using the MD5 algorithm, encrypt the data with RSA, and then store the ciphered data in the cloud.

**F. Jai Arul Jose et al., (2011) [12]**

This paper proposes a security system that provides authentication, confidentiality, and integrity of user data by combining cloud computing with cluster load balancing, SSL over AES, and secure sessions. The security model is divided into different layers.

**G. Qin Liu et al., (2011) [14]**

The authors propose the R3 technique, a time and attribute-based re-encryption method. This allows the cloud server to automatically re-encrypt user data based on its internal clock, ensuring correct access control management.

**H. Dimitrios Zissis et al., (2010)**

A Trusted Third-Party Solution is proposed to maintain the integrity, confidentiality, privacy, and authenticity of data and communications in the cloud environment.

Cloud computing architecture is divided into four layers: hardware, infrastructure, platform, and application. Data must pass through all four layers, so an effective security model needs to provide protection at each level. Our proposed model is designed with these considerations in mind, offering 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".

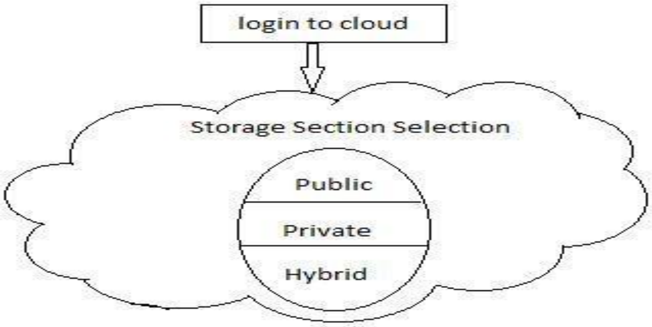


Fig 1: Storage Section Selection

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.

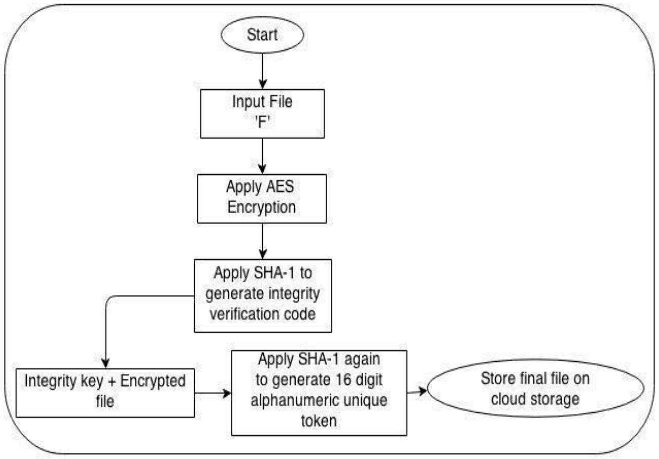

Start
Input File 'F'
Apply AES Encryption
Apply SHA-1 to generate integrity verification code
Integrity key + Encrypted file
Apply SHA-1 again to generate 16 digit alphanumeric unique token
Store final file on cloud storage

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.

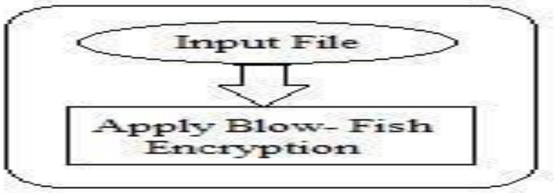


Fig 3: Public Section

**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.

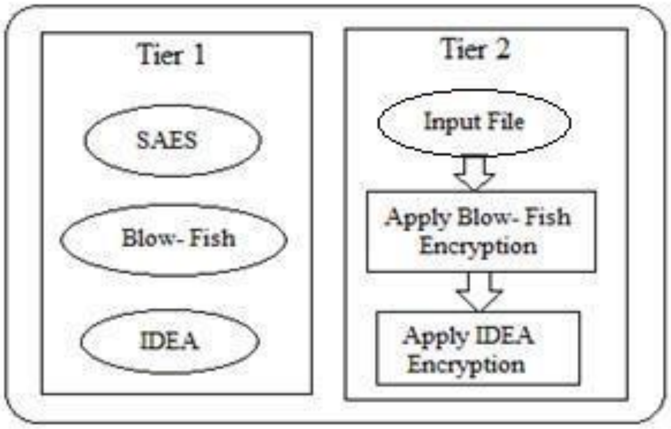


Fig 4: Hybrid Section (Two Tier Security Architecture)

**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.

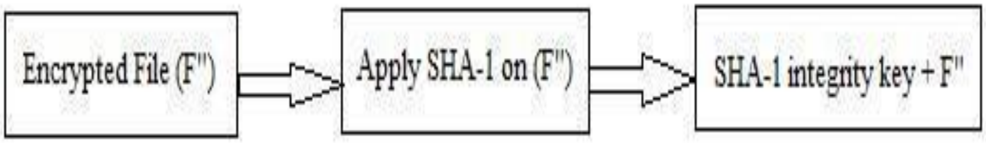


Fig 5: SHA-1 Integrity Key

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.

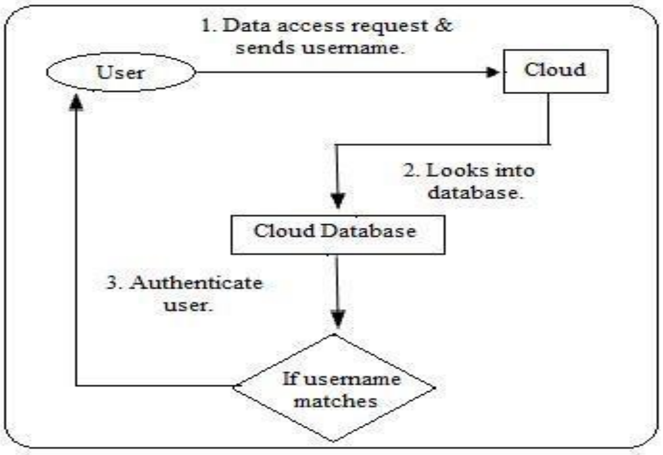


Fig 6: Data Access Request

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.

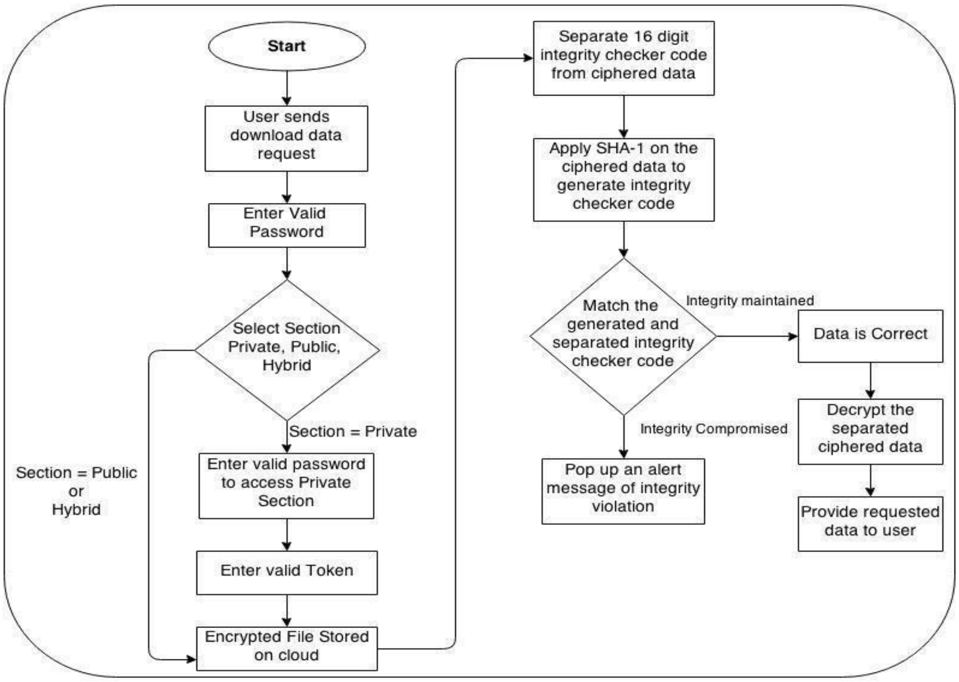

Start
User sends download data request
Enter Valid Password
Select Section Private, Public, Hybrid
Section = Private
Section = Public or Hybrid
Enter valid password to access Private Section
Enter valid Token
Encrypted File Stored on cloud
Separate 16 digit integrity checker code from ciphered data
Apply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

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

Our proposed model offers robust security against numerous threats, including security breaches, data leaks, and modifications. Here's how it tackles various security issues effectively:

a) **Confidentiality**
Data stored on cloud storage is encrypted using various techniques, ensuring it remains confidential and inaccessible to unauthorized users.

b) **Security and Privacy**
Users must log in with a valid username and password, ensuring security and privacy. Additionally, the token mechanism in the Private Section provides double authentication, making it even more secure.

c) **Brute Force Attack**
The encryption schemes are combined in a way that makes brute force attacks nearly impossible. Using a private key of 16 characters in all sections further protects against hackers by obscuring the encryption techniques used.

d) **Data Tampering**
Encryption, a 16-character key, token, username, and password work together to protect against data tampering. Data integrity is verified using SHA-1, which generates an integrity checker code at upload and compares it at download. Matching codes confirm data integrity, while mismatches indicate tampering.

e) **Loss of User Identity and Password**
The Private Section's design safeguards even if user identity and password are leaked. The unique 16-digit alphanumeric token required at the time of file upload ensures a secure environment.

f) **Non-Repudiation**
Non-repudiation ensures that the sender cannot deny sending data, and the receiver cannot deny receiving it. SHA-1, which produces irreversible hash codes, guarantees data integrity and supports non-repudiation.

g) **Masquerade Attack**
The model defends against masquerade attacks. Users must log in with a username and password, and a second password is required to download data. The token adds another layer of double authentication, making it useless for attackers even if they obtain a password.

h) **Enhanced Level of Confusion**
The uniform key size for all encryption algorithms increases the difficulty for attackers to guess which technique was used. Additionally, reducing the SHA-1 integrity verification key from 40 to 16 digits obscures whether an integrity key is attached to the encrypted file, making it nearly impossible for attackers to access the data in its original 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.

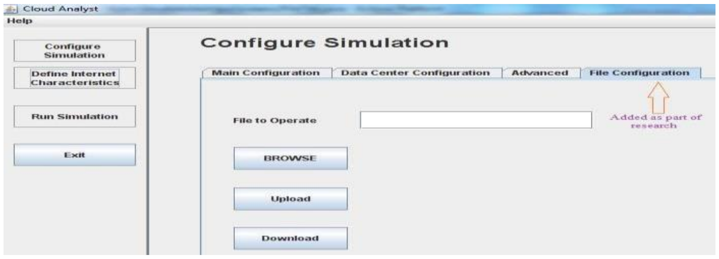


Fig 7: Proposed GUI with „File Configuration" tab

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.

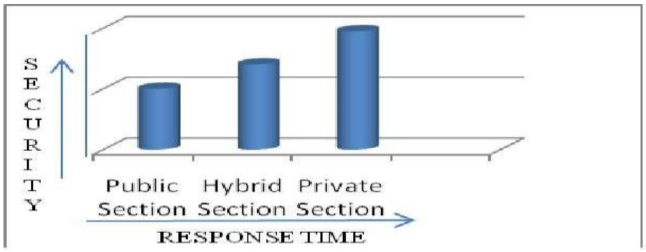
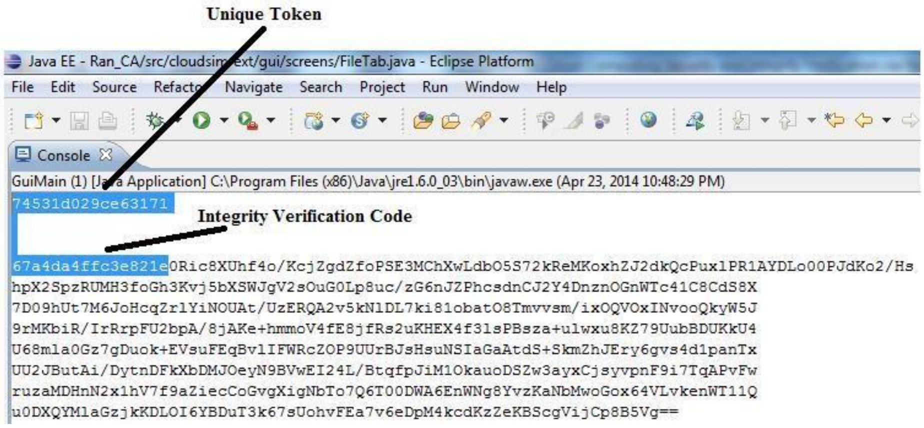


Fig 8: Security Evaluation

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.

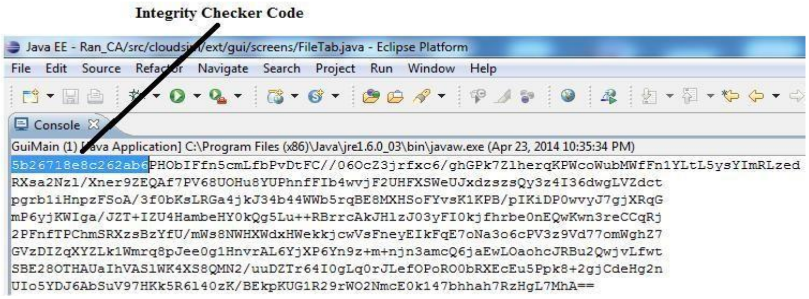

Unique Token
Integrity Verification Code
Java EE - Ran_CA/src/cloudsim/ext/gui/screens/FileTab.java - Eclipse Platform
File Edit Source Refactor Navigate Search Project Run Window Help
Console

```
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/KcjZgdZfoPSE3MChXwLdbO5S72kReMKoxhZJ2dkQcPux1PR1AYDLo00PJdKo2/Hs
hpX2SpzRUMH3foGh3Kvj5bXSWJgV2sOuG0Lp8uc/zG6nJZPhcsdnCJ2Y4DnznOGnWTc41C8CdS8X
7D09hUt7M6JoHcqZrlYiNOUAt/UzERQA2v5kNlDL7ki81obatO8Tmvvsm/ixOQVOxINvooQkyW5J
9rMKbiR/IrRrpFU2bpA/8jAKe+hmmoV4fE8jfRs2uKHEX4f31sPBsza+ulwxu8KZ79UubBDUKkU4
U68mla0Gz7gDuok+EVsuFEqBvlIFWRcZOP9UUrBJsHsuNSIaGaAtdS+SkmZhJEry6gvs4d1panTx
UU2JButAi/DytnDFkXbDMJOeyN9BVwEI24L/BtqfpJiM1OkauoDSZw3ayxCjsyvpnF9i7TqAPvFw
ruzaMDHnN2x1hV7f9aZiecCoGvgXigNbTo7Q6T00DWA6EnWNg8YvzKaNbMwoGox64VLvkenWT11Q
u0DXQYMlaGzjkKDLOI6YBDuT3k67sUohvFEa7v6eDpM4kcdKzZeKBScgVijCp8B5Vg==
```

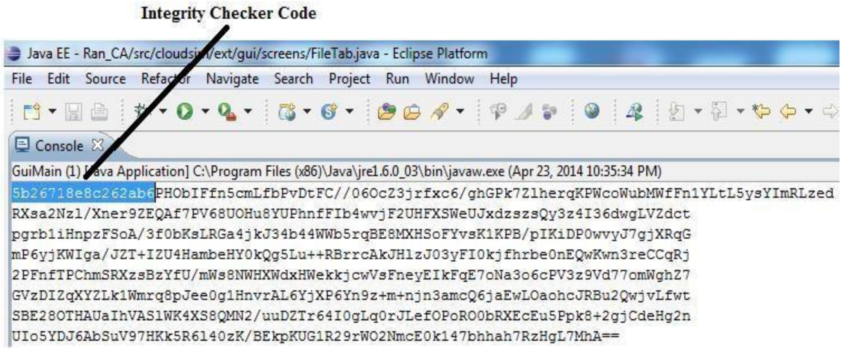
Fig 9: Encrypted File Stored on Cloud Storage Private Section

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.


Integrity Checker 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 10:35:34 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 Checker 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 10:35:34 PM)
5b26718e8c262ab6PHObIFfn5cmLfbPvDtFC//06OcZ3jrfxc6/ghGPk7ZlherqKPWcoWubMWfFn1YLtL5ysYImRLzed
RXsa2Nzl/Xner9ZEQAf7PV68UOHu8YUPhnfFIb4wvjF2UHFXSWeUJxdzszsQy3z4I36dwgLVZdct
pgrb1iHnpzFSoA/3f0bKsLRGa4jkJ34b44WWb5rqBE8MXHSoFYvsK1KPB/pIKiDP0wvyJ7gjXRqG
mP6yjKWIga/JZT+IZU4HambeHY0kQg5Lu++RBrrcAkJHlzJ03yFI0kjfhrbe0nEQwKwn3reCCqRj
2PFnfTPChmSRXzsBzYfU/mWs8NWHXWdxHWekkjcwVsFneyEIkFqE7oNa3o6cPV3z9Vd77omWghZ7
GVzDIZqXYZLk1Wmrq8pJee0g1HnvrAL6YjXP6Yn9z+m+njn3amcQ6jaEwLOaohcJRBu2QwjvLfwt
SBE28OTHAUaIhVASlWK4XS8QMN2/uuDZTr64I0gLq0rJLefOPoRO0bRXEcEu5Ppk8+2gjCdeHg2n
UIo5YDJ6AbSuV97HKk5R6l40zK/BEkpKUG1R29rWO2NmcE0k147bhhah7RzHgL7MhA==
```

Fig 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

Our proposed cloud storage security model creates a highly secure environment by dividing user data into three sections based on key security parameters: authentication, confidentiality, integrity, availability, nonrepudiation, security, and privacy. By implementing double authentication mechanisms, it effectively prevents unauthorized access to user data. The model also guards against various security threats, including brute force attacks, masquerade attacks, data tampering, and cryptanalysis of the integrity key. Additionally, it allows users to choose encryption techniques in the hybrid section based on factors like cost and security needs.

## VII. FUTURE SCOPE

We can further enhance this model by incorporating an encrypted data searching scheme using index building for encrypted data. Confidentiality can be improved by introducing various combinations of encryption techniques across all three sections. Additionally, we can develop a procedure that automatically classifies data into the three sections based on factors such as 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 Reencryption 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.