File Integrity Maintenance Tool for Secure Information Storage in Cloud

Shweta Sharma
Department of Computer Engineering,
Delhi Technological University,
India

Manoj Kumar
Associate Professor
Department of Computer Engineering,
Delhi Technological University,
India

ABSTRACT
In current scenario, modern technologies have completely changed the lives of the people. Every facility is available online through internet. People do their business through online services by being at home. This changing trend brought the concept of Cloud Computing where various physical servers(may be at different locations) are collaborated together and cloud services are provided to the users in the same fashion. When millions of people access business applications to perform their transactions, there arises a susceptibility for personal information security to get leaked through hackers/intruders etc. [1] [2] [3]. To avoid certain circumstances, data security becomes prime essential component as building block for the development of a safer and convenient system. The users require a prominent and secure portal. The risk levels get enhanced in case of access of highly confidential information through their accounts within the portal such as Banking websites, Defense or brokerage related applications. Safeguard of security through internet becomes streamlined concern for the service providers. A lot of research work has been pursued in order to ensure higher safety levels [4][5][6].

General Terms
Cloud Computing, Data Integrity.

Keywords
Security, Client-Server, Integrity Maintenance, Hash.

1. CLOUD COMPUTING & ITS CHARACTERISTICS
Cloud Computing signifies a collaboration of distributed systems with configuration based network resources to perform distinctive tasks. As per our research study [7] [8], following table describes the features provided by Cloud Computing to its users:

1.1 Various Cloud Models Categorization Based on Usage
The cloud computing platform has been categorized based on its usefulness characteristics. Different kinds of services have been designed and implemented to serve the need of business processes. Using such variety of platforms, many application/software based services have been improved.

Table 1. Cloud Models Categorization

S. No.	Types of Cloud Models	Specification & Usage
1	IaaS (Infrastructure as a Service)	Availability of virtual servers to clients for configuration and management.
2	PaaS (Platform as a Service)	Supply of servers to customers for development related purposes.
3	SaaS (Software as a Service)	Software/Application based services are provided
4	SaaS (Security as a Service)	Facility of security solutions.
5	IDaaS (Identity as a Service)	Management of identities in the cloud.
6	CaaS (Communication as a Service)	The consumer can utilize Enterprise level VoIP, VPNs in economic scales.
7	MaaS (Monitoring as a Service)	Application /server status are to be checked through monitoring tools during downtime.

1.2 Security Issues Present in Cloud Computing
In cloud computing, due to many prevalent kinds of attacks, various security concerns have been raised and identified. These issues have been the major concern of cloud in terms of data security. Following table shortlists the prevalent security related concerns in Cloud Computing [9] [10]:

Table 2. Security issues in Cloud

S. No.	Security Issues in Cloud	Definition
1	Data Privacy & Confidentiality	Safeguard of sensitive information between clients and cloud service providers.
2	Backup	Maintenance of originality of data through data replication over cloud server.
3	Authentication	Identification of client/server as trusted entities among themselves.
4	Integrity	Preservation of intact original information.
5	Interception of Data	Data modifications may occur on cloud server through security breaches.
6	Intermediary	Intermediate parties legal rights must be protected to ensure proper transactions among third parties involved in cloud system.
7	Data Storage Location	Customer ensures the data storage location within cloud and liabilities in case of data exposure

		must be decided beforehand.
8	Governing Laws and Jurisdiction	Legal procedures to be followed while performing transactions among different companies with distinct countries involved.
9	Vendor Contracts	Organizations providing cloud services may not warranty security constraints to users.
10	Willingness to Cloud	Weak internet facility does not lead to data migration on cloud.
11	Standardization	Clash of policies over cloud computing agreements among organizations.

1.3 Significant Security Attacks on Cloud

In order to protect information over cloud platform, we are required to analyze different sorts of already prevalent security attacks. Various security attacks have arisen due to the popularity of cloud computing platform in the corporate industries in recent days. The below table represents and defines the collection of cloud security attacks [11] [12] [15]:

Table 3. Security attacks on Cloud

S. No.	Security Issues in Cloud	Definition
1	Distributed Denial of Service Attack(DDoS)	Indefinite suspension of services of clients connected through internet. Leads to loss of personal information of users in specified conditions.
2	Masquerading	Attacker impersonates another person.
3	Replaying	Attacker obtains an original copy of message from sender and tries to retaliate later.
4	Repudiation	Message sender/receiver may deny being the same for a given exchanged message.
5	Insider Threats	Super user privileges may get misused through cloud service provider's database administrators.
6	Software & Security Management Risks	Dormant virtual machines aggravate the possibility of worms, viruses & malwares in cloud.
7	Side Channel Attacks	Inherent cache monitoring techniques to check for information flow among clients and cloud service providers.
8	Cloud Dependency Stack	Impact on security levels of business domains due to issues present in lower levels of cloud stack such as SaaS.
9	Geographical Implications	The mobilization of virtual instances leads to loss of company's sensitive information through government agencies.
10	Phishing	Act of acquiring confidential information from user by pretending as a trusted entity in cloud.

2. PROPOSED ARCHITECTURE

In a server-client environment, there occurs substantial data exchange between both entities. Client may require information storage in certain shared files/folders at remote server location for easy access and information retrieval.In those scenarios, the file data integrity becomes the topmost priority for the server. Certain schemes have been suggested with its regards [13][14].

Here, we would like to propose a new design to protect information integrity among client –server process exchanges. Following diagram represents the principle idea for proposed design scheme.

Through the proposed design, we can achieve following functionalities:-

- Integrity Maintenance: - It leads to establishment of information integrity within a given file.
- Detection of Modified Data:-If attacked through outside intruders, it will be identified through proposed design scheme.
- Replacement through Backup replica: - Modified data will be replaced through original copy of information (stored at server end in case of emergency).
- Client Verification Process:-Valid client verification would happen using proposed design.
- Alleviated Trust level Mechanism:-This scheme involves both client and server in order to finalize the contents to be stored within the file as final output of proposed cryptography design. This feature greatly enhances the quality of design .Here, no entity can be the intruder in worst case scenario and thus, certain level of quality trust establishes between both entities in a cloud computing environment.

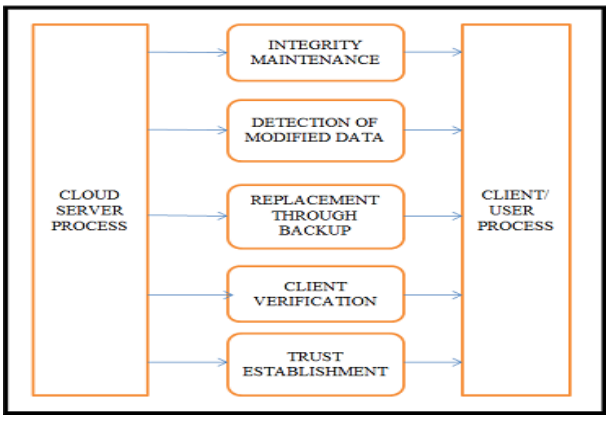

Fig 1: Proposed Architecture for File Integrity Tool in Cloud Environment

3. PROPOSED MODEL FOR LIGHT WEIGHT FILE INTEGRITY MAINTENANCE TOOL DURING CLIENT-SERVER INTERACTON IN CLOUD

This tool has been designed and proposed based on the integrity establishment and monitoring of the client's information already stored over cloud. It is beneficial in terms of protecting any confidential information leakage through

cloud. It could hamper business structures. Thus, we focused on safe data storage over cloud with minimum server overhead. This tool performs functions as per following algorithm:

- Initialize server process SP and client process CP respectively.
- The server process listens to client port and establishes connection.
- Initialize the input file F's location on server hard disk.
- Integrity Establishment function
- {
- The Server process SP applies SHA-2 algorithm on F.
- Add Nonce N and apply AES (Advanced Encryption Standard) algorithm to produce intermediate result.
- The intermediate result stream is sent to client process.
- The client process CP applies AES decryption algorithm.
- Adds Nonce N'.
- Apply SHA-2 on intermediate result to produce H(X).
- Apply RSA digital Signature scheme (signing process).
- CP transfers output stream to server process.
- The Server process SP stores the final output X in <secure> tags within F.
- }
- Integrity monitoring function (Invoked by SP/CP)
- {
- Call Integrity Establishment Function to produce output X'.
- Compare X and X'.
- If (X equals X') then print- File intact. Monitoring Completed.
- Else Replace F' with originally stored F.
- Call Integrity Establishment function
- }
- Client Verification Process
- {
- Initialize SP and CP.
- SP applies RSA Digital Signature scheme (verifying process) on X.
- Output is stored as Y.
- If (Y equals H(X)), then Client verified.
- Exit }

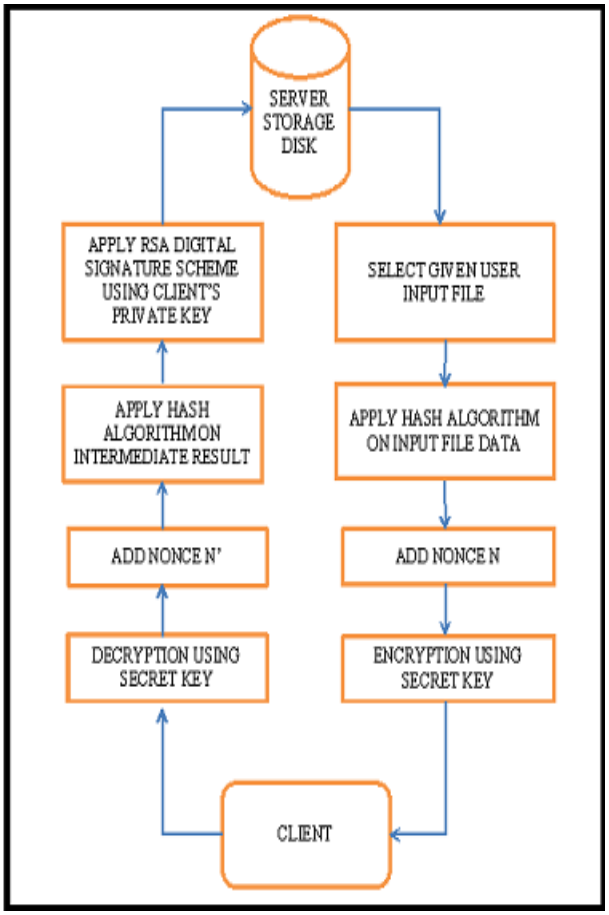

Fig2: Proposed File Integrity Secure Storage based Tool.

4. MODEL IMPLEMENTATION

- During client–server interaction, to establish and monitor integrity of the stored client data. We have designed this model.
- Initially, the client stores its data in server specified directory.
- For integrity establishment, server accesses the file and applies a hash algorithm (sha-2) to generate message digest (MD).
- It appends (already shared random numbers called as Nonce N and N') N along with MD and encrypts using client- server shared secret key.
- The encrypted data gets transferred to client.
- Client receives the file and decrypts it using secret key and appends another nonce N' to the data. And applies hash algorithm (sha2) to generate H(X).
- Now, client implements RSA digital Signature Scheme to encode and transfers the final string to server for storage.
- At the same time, server may also verify the H(X) using client's public key.
- This way, client's involvement in integrity establishment gets achieved and server may also verify the client's authenticity using Digital Signature verification process.

- It enhances the trust level among server and client as they act as peers in determining integrity of stored data.
- And thus, more secure designed model for storage and maintenance of server data at server location.

5. RESULTS & DISCUSSIONS

This model has been implemented in windows7 platform using Linux based Oracle VM virtual box. This tool provides the facility of client- server environment on existing machine only. There have been various processes including client and server processes. The server process executes and establishes connection with client process using specified socket address structures. There are two types of processes which gets generated i.e. client and server processes. Firstly, the server process executes and allows the client process to perform following functionalities-

a. Integrity Calculation:-This functionality calculates the final checksum value for the original file content and stores it in safe tags within the original file only.

b. Integrity Maintenance: This function may be scheduled to perform integrity checks regularly for the stored confidential client files (already stored by client on the server).

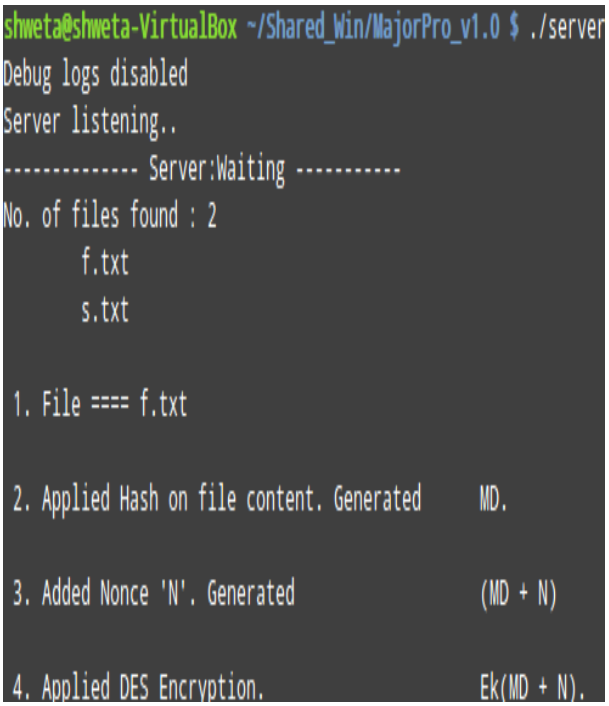

Fig 3: Screenshot for Server process Initialization Mode

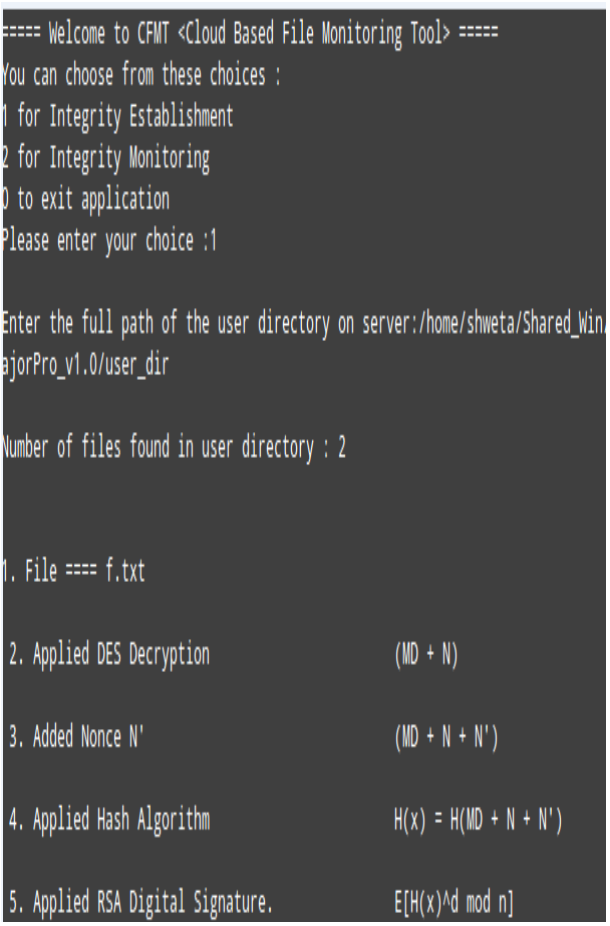

Fig 4: Screenshot of Client Process Initialization Mode

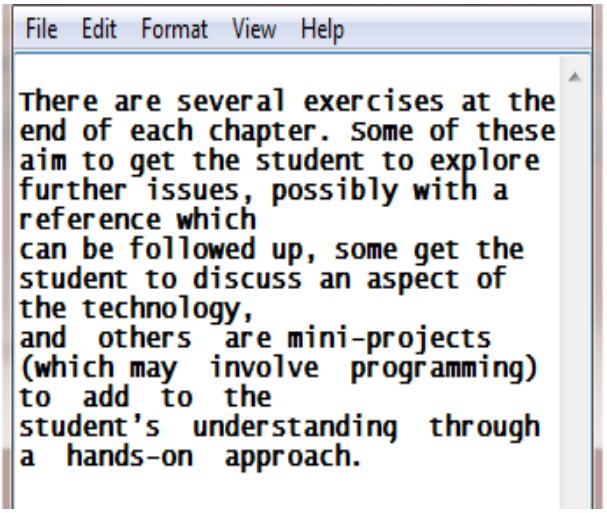

Fig 5: Original client's Data stored on server.

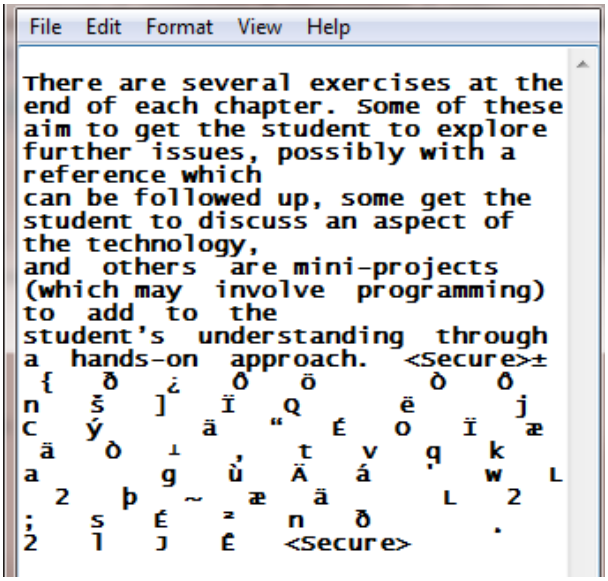

Fig 6: Original Client's Data stored after Integrity Calculation (stored within given tags).

Thus, it can be observed that this tool proves to be quite time efficient and cost effective as it performs integrity calculation in around 1000 microseconds for a given 500 byte file which is a very limited requirement as compared to the long delays(in minutes/hours) required for server to perform integrity checks on client's file. And also, there is no memory constraint in this tool. This tool works without any database requirement on the server. Thus, satisfies the light weight and secure storage tool criteria for cloud computing environment.

6. CONCLUSION

For highly confidential client data, an enhanced security model is required which can provide high level security during information storage under cloud platform. This model has been proposed which can be setup in a cloud computing environment and is very cost effective and highly secure for client's data. It ensures trust mechanism between both entities during interaction (which is a desirable advantage to promote cloud businesses).This tool cam work in form of scheduler/executable to be run on cloud server at customized time/day sequences. It benefits using regular integrity checks and thus supervises the intact integrity of the client's information over the cloud with better client-server communications.

7. REFERENCES

[1] G A Solanki: Welcome To the Future of Computing: Cloud Computing and Legal Issues: International Journal of scientific & technology research volume1, issue 9, October 2012.

[2] Nelson Gonzalez, CharlesMiers, FernandoRed´igolo1, and MarcosSimpl´icio: A quantitative analysis of current security concerns and solutions for cloud computing: Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications2012,http://www.journalofcloudcomputing.com/content/1/1/11.

[3] S.Suganya, P. Damodharan: Enhancing Security for Storage Services in Cloud Computing: International Conference on Current Trends in Engineering and Technology, ICCTET'13.

[4] Ms. T.J. Salma: A Flexible Distributed Storage Integrity Auditing Mechanism in Cloud Computing: 2013 IEEE 14th International Conference on High Performance Switching and Routing.

[5] Bhavani Thuraisingham, Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan ,The University of Texas at Dallas: Secure Data Storage and Retrieval in the Cloud.

[6] Qingni Shen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying ZhangSecDM: Securing Data Migration Between Cloud Storage Systems :2011 IEEE ninth International conference on Dependable, autonomic and Secure computing.

[7] Zhongbin Tang, Xiaoling Wang, Li Jia, Xin Zhang, and Wenhui Man: Study on data security of cloud computing: IEEE.

[8] Hu glory Tianfield: Security Issues in Cloud Computing: 2012 IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012, COEX, Seoul, Korea.

[9]Henry Kasim, Terence Hung, Xiaorong Li: Data Value Chain as a Service Framework: for Enabling Data Handling, Data Security and Data Analysis in the Cloud: 2012 IEEE 18th International Conference on Parallel and Distributed Systems

[10] Tina Francis, S.Vadivel: Cloud Computing Security: Concerns, Strategies and Best Practices: Proceedings of 20121ntemational of Cloud Computing, Technologies, Applications & Management 2012 IEEE.

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

[12] Mrs. G.Nalinipriya ME., (Phd), Mr.R.Aswin Kumar: Extensive Medical Data Storage with Prominent Symmetric Algorithms On Cloud - A Protected Framework: 2013 International Conference on Smart Structures & Systems (JCSSS-20 13), March 28 - 29, 2013, Chennai, INDIA.

[13] A light Weight Centralized File Monitoring Approach for Securing Files in Cloud Environment : The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

[14] A secure and light weight approach for critical data security in cloud: 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN).

[15] Forouzan, "Cryptography and Network Security", TMH.