RESEARCH ARTICLE OPEN ACCESS

A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage

Mrs Jhansi Rani [1], Pallpu Ganesh [2]

[1] Asst.Professor, Department of Computer Applications
[2] Student, Department of Computer Applications
[1], [2] Chadalawada Ramanamma Engineering College (Autonomous)

ABSTRACT

Cloud computing is an evolving technology that provides data storage and highly fast computing services at a very low cost. All data stored in the cloud is handled by their cloud service providers or the caretaker of the cloud. The data owner is concerned about the authenticity and reliability of the data stored in the cloud as the data owners. Data can be misappropriated or altered by any unauthorized user or person. This project desire to suggest a secure public auditing scheme applying third party auditors to authenticate the privacy, reliability, and integrity of data stored in the cloud. This proposed auditing scheme composes the use of the AES-256 algorithm for encryption, SHA-512 for integrity check and RSA-15360 for publickey encryption. And perform data dynamics operation which deals with mostly insertion, deletion, and, modification.

Keywords: - Cloud Computing, Cloud Storage, Auditing Scheme, Data Owner, Cloud Service Provider.

I. INTRODUCTION

This project desire to suggest a secure public auditing scheme applying third party auditors to authenticate the privacy, reliability, and integrity of data stored in the cloud and perform data dynamics operation which deals with mostly insertion, deletion, and, modification. In Existing approaches, have prospective a way to support public auditing and privacy- preserving, in their approach, HLA and BLS signature along with MHT are used in this proposed work. In their approach support data dynamic by the Merkle hash tree. They have also maintained integrity. In their approach, confidentiality is not maintained and batch auditing is supported. In Other Existing Approach, have prospective a way for securing the cloud data. In their approach, they have used the AES for data confidentiality and TPA for data auditing. They have used the SHA-2 for generating the message digest. They have not mentioned which version of the AES(128,192,256)algorithm applied. They also not mentioned which version of SHA2(224,256,512) applied. They did not mention how data are split and how these are encrypted due to there, we do not say their approach is secured.because all versions of AES and SHA that secure.

II. RELATEDWORKS

Qian Wang, Cong Wang proposed Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing**.** Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance.

Kan Yang,Xiaohua Jia. Proposed An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.

Kan Yang,Xiaohua Jia. Proposed Privacy Preserving Public Auditing for Secure Cloud Storage. Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

.

III. PROPOSED SYSTEM ARCHITECTURE

It requires to grow a robust auditing method and do data dynamics operation. It's no passed data on third-party auditor about auditing method. It performs a communication model. It uses AES256, RSA-15360, and SHA512 algorithm. AES256 is a standard and most acceptable algorithm for encryption and decryption processes. It works on the input block size of 128 bits having a key size of 256 bit. Therefore, it has 2256 possible a key combination which is 78 digits number. It exponentially generates the number of astronomically in the observable universe. In this prospective method, DO encrypt the data and store CS. Although data is encrypted only by the symmetric key that DO can only see the data. CS can not knowledge about data. TPA requests for encrypted data to CS to check integrity. After that CS sends encrypted data to TPA. To protected data from an external attacker then CS has again encrypted the encrypted data to the public key. Because the key size is very increased then not affect the external attack.In this prospective method, No knowledge about the whole key. They know only about what they are authorized.

In this data owner module, the data owner uploads their data with its File Blocks block in the cloud server. For the security purpose the data owner encrypts the data File Blocks and then store in the cloud. The data owner can change the policy over data File Blocks by updating the expiration time. The Data owner can have capable of manipulating the encrypted data File Blocks. And the data owner can set the access privilege to the encrypted data File Blocks. The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data File Blocks and store them in the cloud for sharing with data consumers. To access the shared data File Blocks, data consumers download encrypted data File Blocks of their interest from the cloud and then decrypt them. Third party auditor (TPA), who has capabilities to manage or monitor the outsourced data under the delegation of data owner, who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and credibility in clouds and setting time period to update the old secret keys to new secret keys. The Cloud User who has a large amount of data to be stored in cloud and have the permissions to access and manipulate stored data and performs the following operations such as Searches for File Blocks based on Content's keyword, Requests for File Blocks, Request File Blocks for downloading with current sec key for the corresponding File Blocks from the cloud and dec, download.

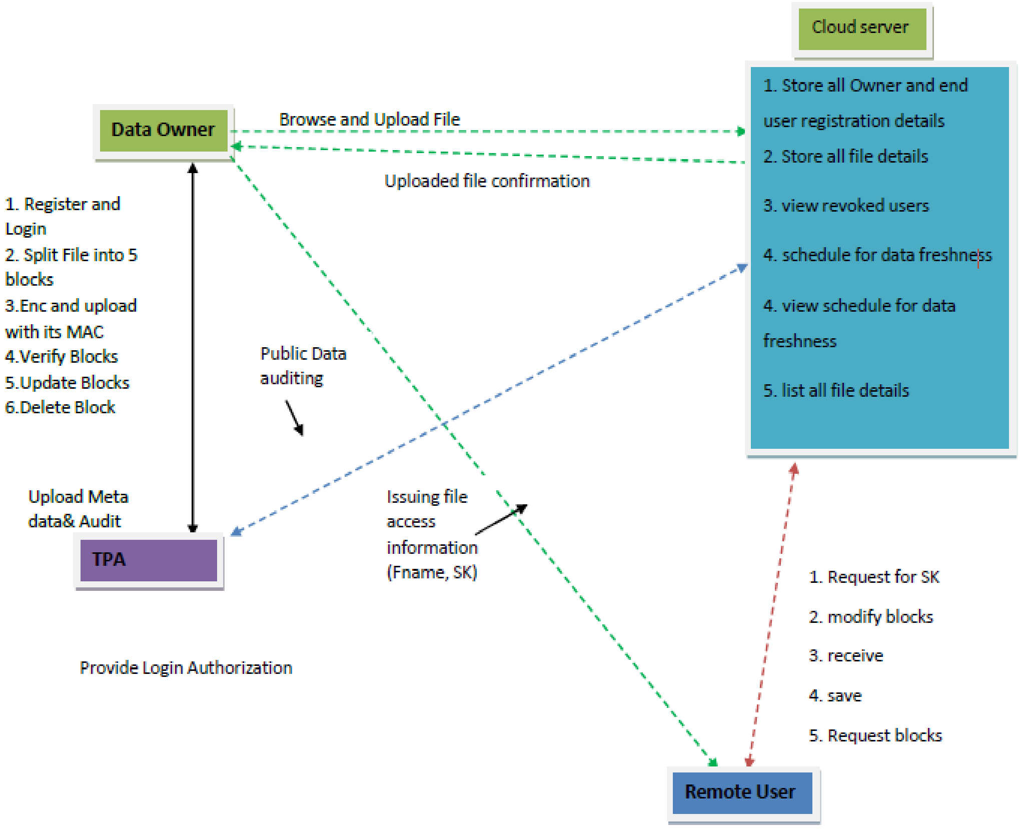
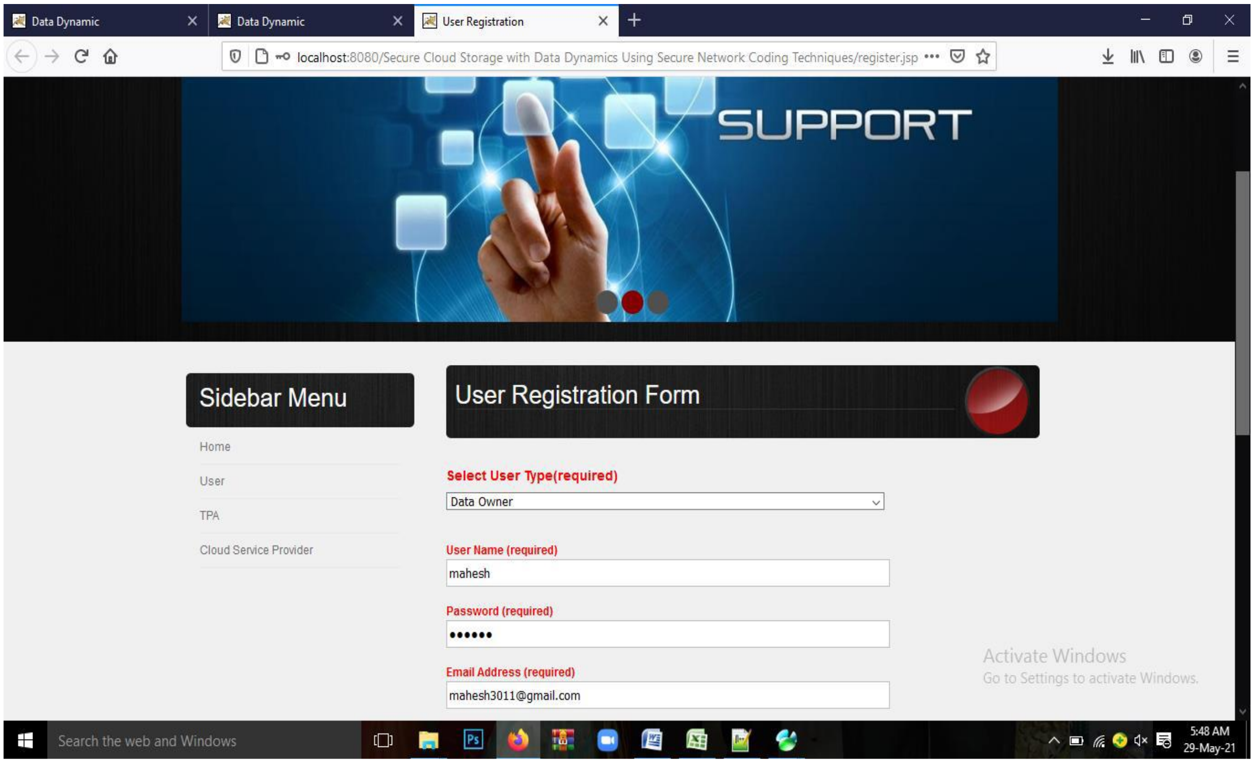

Cloud server
1. Store all Owner and end user registration details
2. Store all file details
3. view revoked users
4. schedule for data freshness
4. view schedule for data freshness
5. list all file details
Data Owner
Browse and Upload File
Uploaded file confirmation
1. Register and Login
2. Split File into 5 blocks
3.Enc and upload with its MAC
4.Verify Blocks
5.Update Blocks
6.Delete Block
Public Data auditing
Upload Meta data& Audit
TPA
Issuing file access information (Fname, SK)
Provide Login Authorization
1. Request for SK
2. modify blocks
3. receive
4. save
5. Request blocks
Remote User

Fig.1 Proposed architecture

IV. RESULTS AND DISCUSSION

The output screens obtained after executing and running the system are shown from Fig.2 to Fig.9



localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/register.jsp

User Registration Form

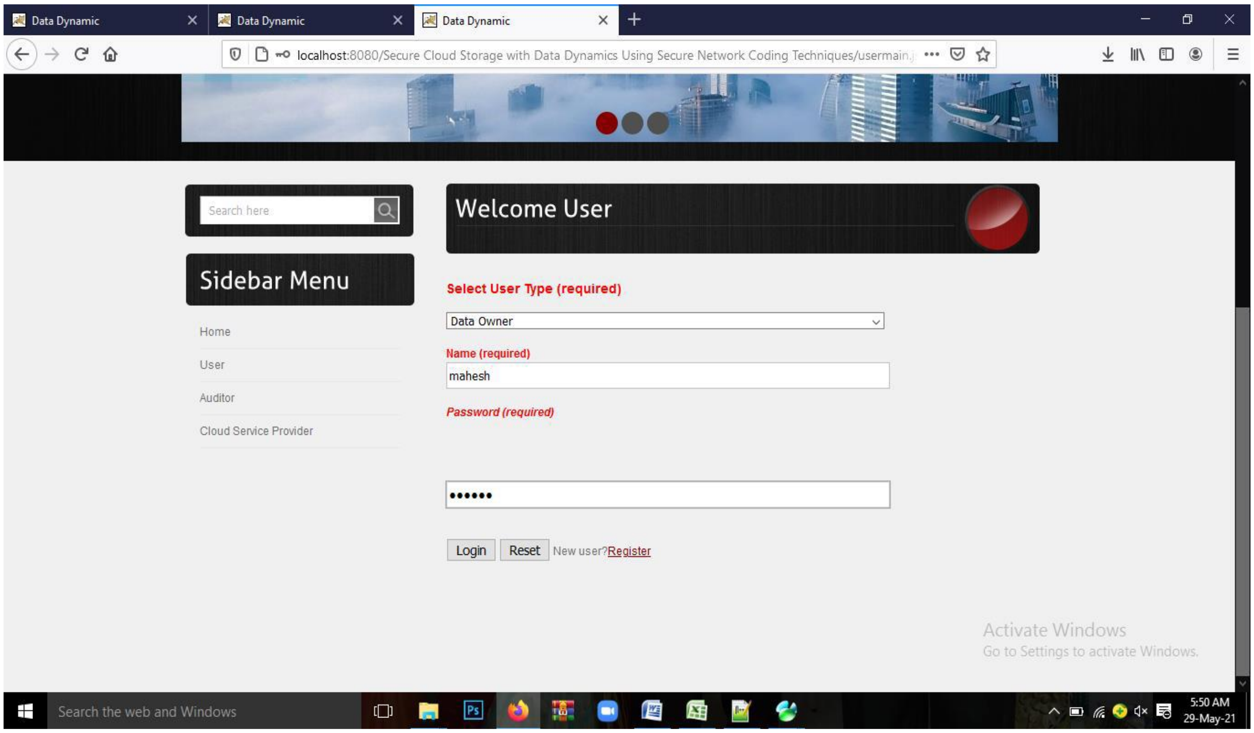
Select User Type(required): Data Owner

User Name (required): mahesh

Password (required): ••••••

Email Address (required): mahesh3011@gmail.com

Fig.2 Data Owner registration



localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/usermain.j

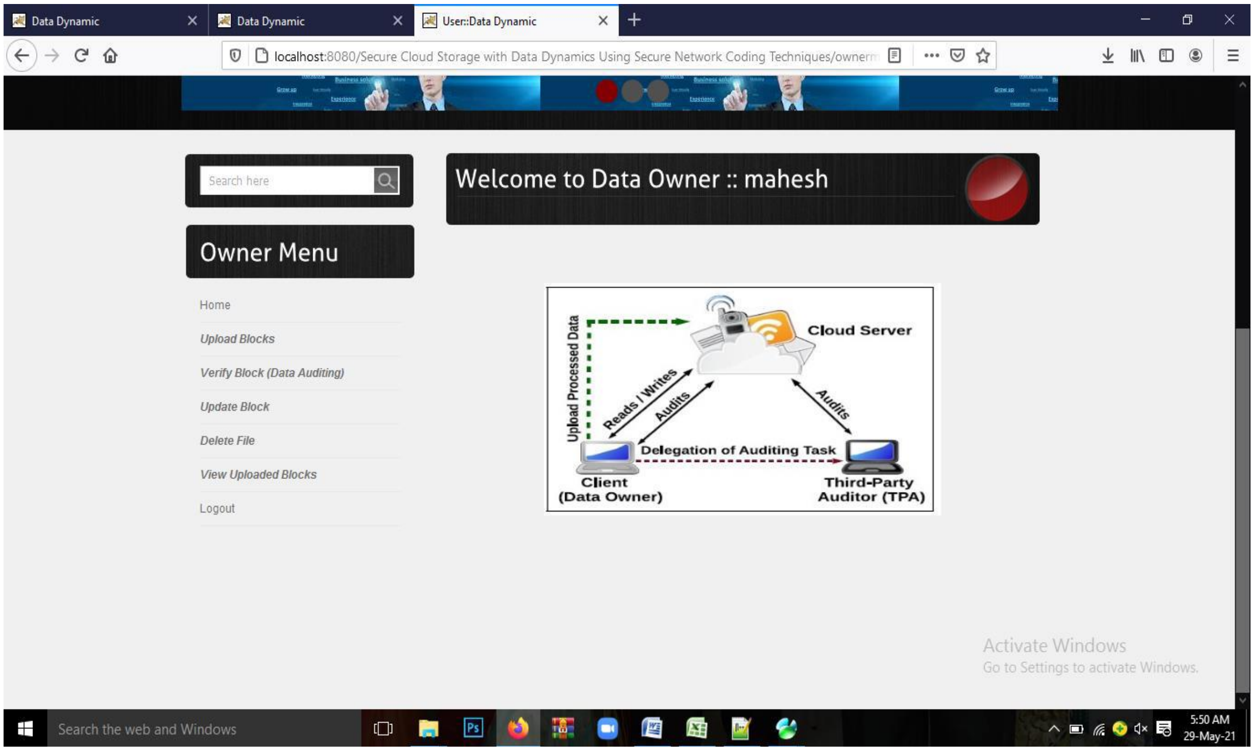
Welcome User

Select User Type (required): Data Owner

Name (required): mahesh

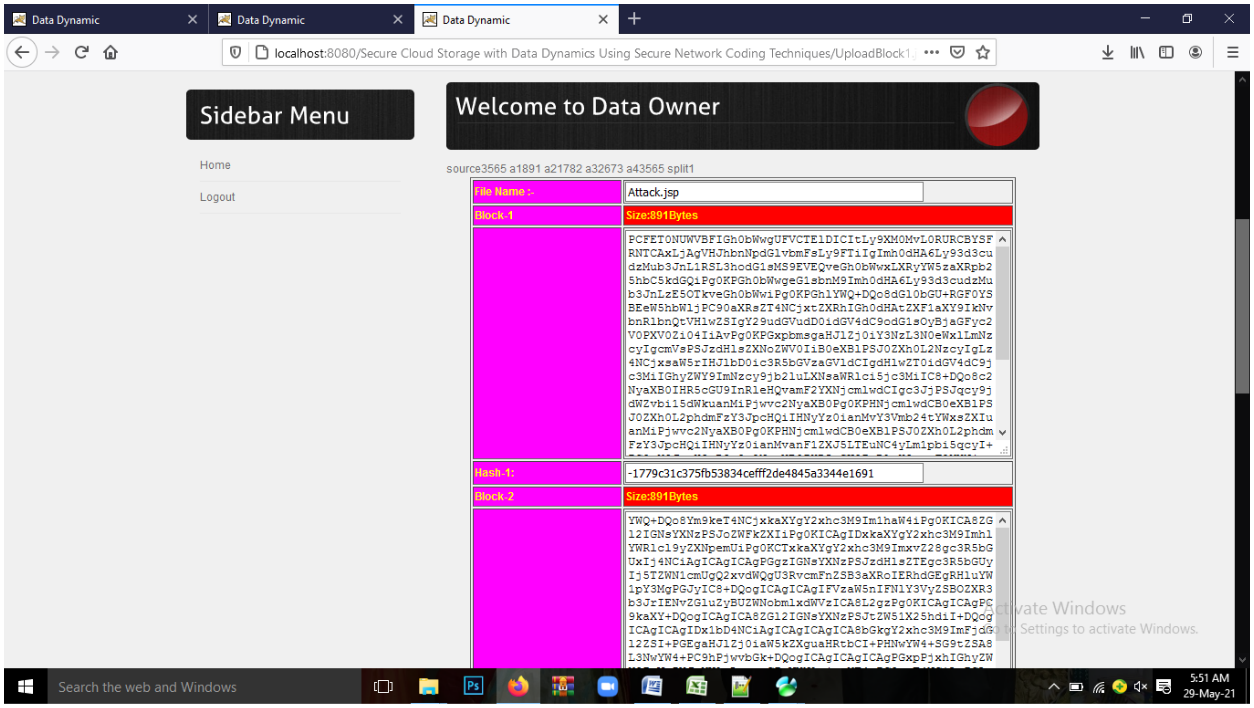
Password (required): ••••••

Fig.3 Data owner login page



Welcome to Data Owner :: mahesh

Fig.4 data owner home page


Data Dynamic
Data Dynamic
Data Dynamic
localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/UploadBlock1.
Sidebar Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
5:51 AM
29-May-21

Welcome to Data Owner

source3565 a1891 a21782 a32673 a43565 split1

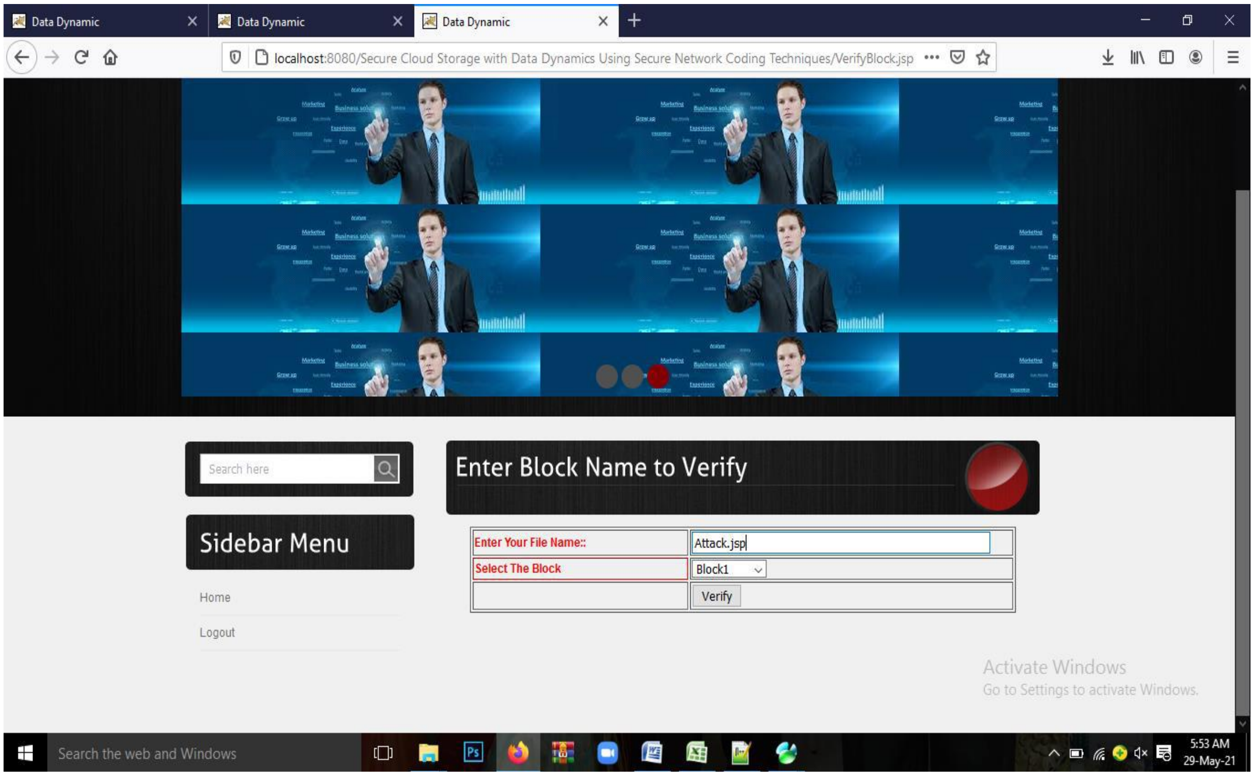
File Name :-	Attack.jsp
Block-1	Size:891Bytes

PCFETONUWVBFIGh0bWwgUFVCTElDICItLy9XM0MvL0RURCBYSF
RNTCAxLjAgVHJhbnNpdGlvbmFsLy9FTiIgImh0dHA6Ly93d3cu
dzMub3JnL1RSL3hodG1sMS9EVEQveGh0bWwxLXRyYW5zaXRpb2
5hbC5kdGQiPg0KPGh0bWwgeG1sbnM9Imh0dHA6Ly93d3cudzMu
b3JnLzE5OTkveGh0bWwiPg0KPGhlYWQ+DQo8dGl0bGU+RGF0YS
BEeW5hbWljPC90aXRsZT4NCjxtZXRhIGh0dHAtZXF1aXY9IkNv
bnRlbnQtVHlwZSIgY29udGVudD0idGV4dC9odG1sOyBjaGFyc2
V0PXV0Zi04IiAvPg0KPGxpbmsgaHJlZj0iY3NzL3N0eWxlLmNz
cyIgcmVsPSJzdHlsZXNoZWV0IiB0eXBlPSJ0ZXh0L2NzcyIgLz
4NCjxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZT0idGV4dC9j
c3MiIGhyZWY9ImNzcy9jb2luLXNsaWRlci5jc3MiIC8+DQo8c2
NyaXB0IHR5cGU9InRleHQvamF2YXNjcmlwdCIgc3JjPSJqcy9j
dWZvbi15dWkuanMiPjwvc2NyaXB0Pg0KPHNjcmlwdCB0eXBlPS
J0ZXh0L2phdmFzY3JpcHQiIHNyYz0ianMvY3Vmb24tYWxsZXIu
anMiPjwvc2NyaXB0Pg0KPHNjcmlwdCB0eXBlPSJ0ZXh0L2phdm
FzY3JpcHQiIHNyYz0ianMvanF1ZXJ5LTEuNC4yLm1pbi5qcyI+

Hash-1:	-1779c31c375fb53834cefff2de4845a3344e1691
Block-2	Size:891Bytes

YWQ+DQo8Ym9keT4NCjxkaXYgY2xhc3M9Im1haW4iPg0KICA8ZG
l2IGNsYXNzPSJoZWFkZXIiPg0KICAgIDxkaXYgY2xhc3M9Imhl
YWRlcl9yZXNpemUiPg0KCTxkaXYgY2xhc3M9ImxvZ28gc3R5bG
UxIj4NCiAgICAgICAgPGgzIGNsYXNzPSJzdHlsZTEgc3R5bGUy
Ij5TZWN1cmUgQ2xvdWQgU3RvcmFnZSB3aXRoIERhdGEgRHluYW
1pY3MgPGJyIC8+DQogICAgICAgIFVzaW5nIFN1Y3VyZSBOZXR3
b3JrIENvZGluZyBUZWNobmlxdWVzICA8L2gzPg0KICAgICAgPC
9kaXY+DQogICAgICA8ZGl2IGNsYXNzPSJtZW51X25hdiI+DQog
ICAgICAgIDx1bD4NCiAgICAgICAgICA8bGkgY2xhc3M9ImFjdG
l2ZSI+PGEgaHJlZj0iaW5kZXguaHRtbCI+PHNwYW4+SG9tZSA8
L3NwYW4+PC9hPjwvbGk+DQogICAgICAgICAgPGxpPjxhIGhyZW

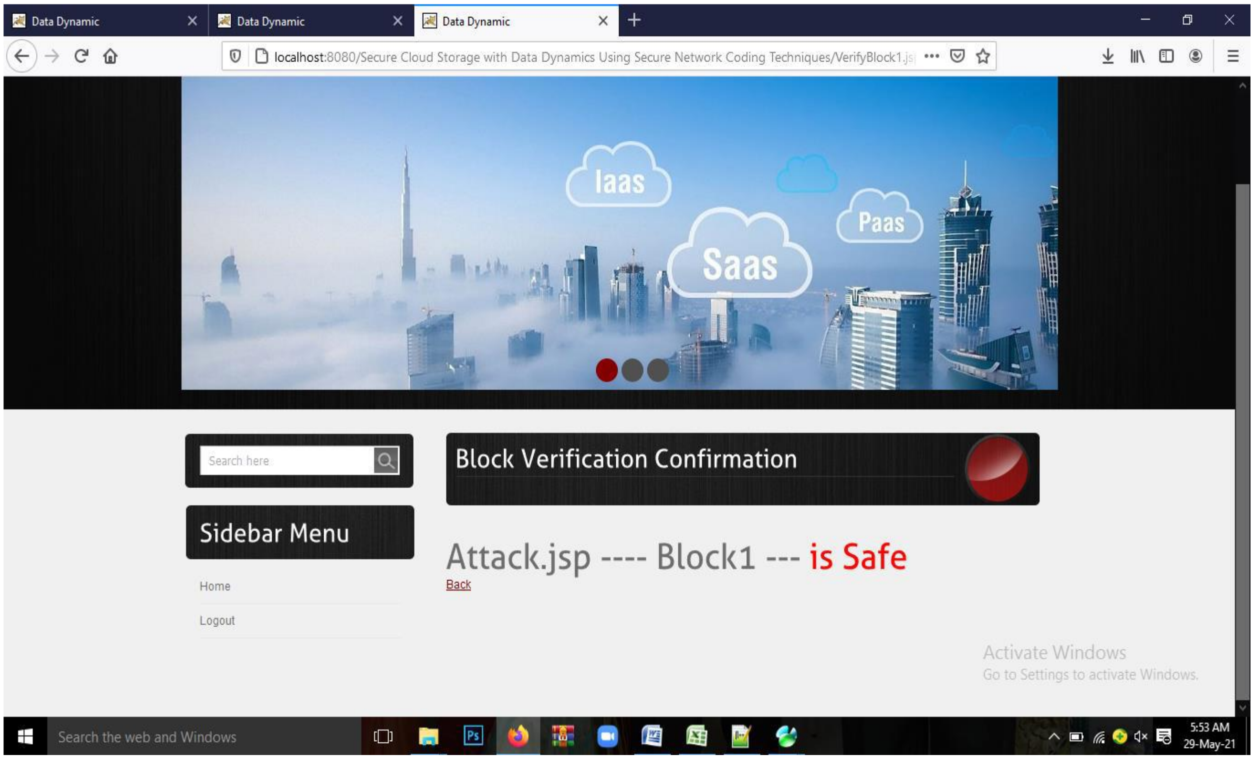
Fig.5 upload files


Data Dynamic
Data Dynamic
Data Dynamic
localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/VerifyBlock.jsp
Search here
Sidebar Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
5:53 AM
29-May-21

Enter Block Name to Verify

Enter Your File Name::	Attack.jsp
Select The Block	Block1
	Verify

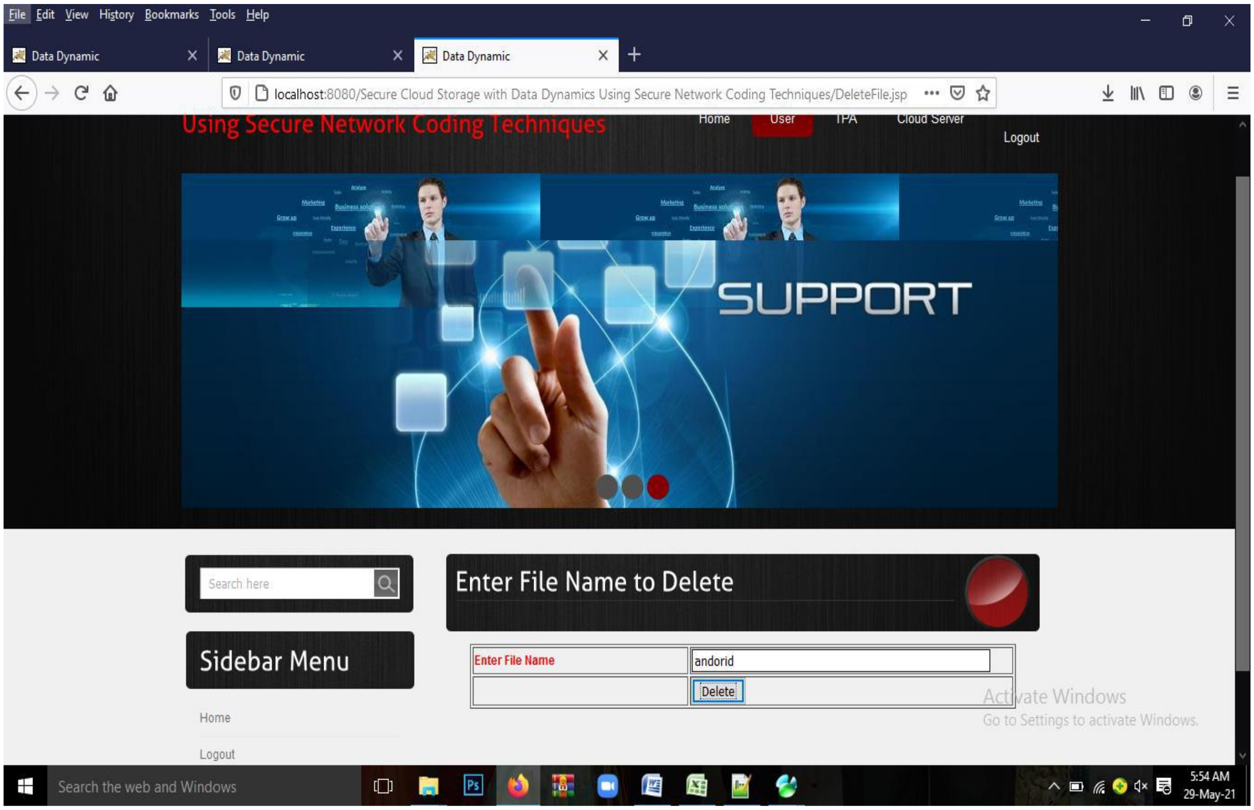
Fig.6 Verify block


Data Dynamic
Data Dynamic
Data Dynamic
localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/VerifyBlock1.js
Iaas
Saas
Paas
Search here
Sidebar Menu
Home
Logout
Back
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
5:53 AM
29-May-21

Block Verification Confirmation

Attack.jsp ---- Block1 --- is Safe

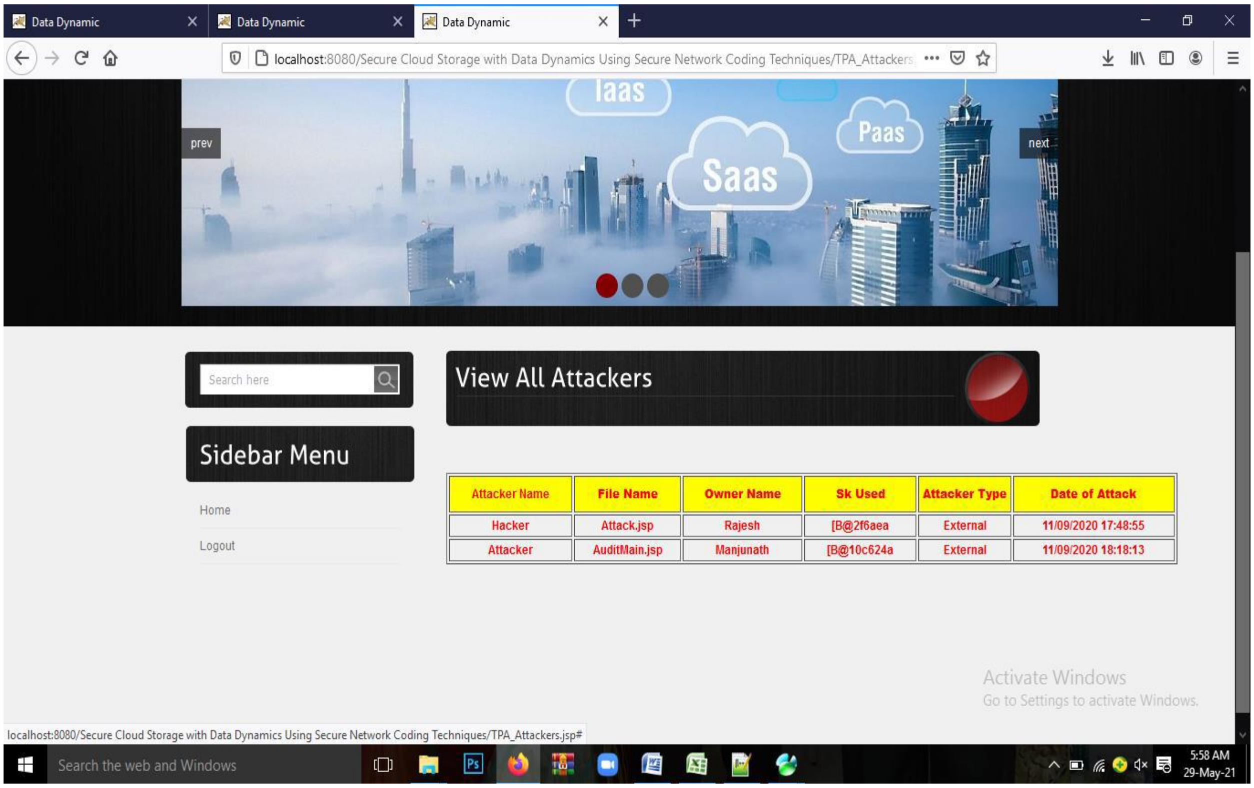
Fig.7 Block verification confirmation


File Edit View History Bookmarks Tools Help
Data Dynamic
Data Dynamic
Data Dynamic
localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/DeleteFile.jsp
Using Secure Network Coding Techniques
Home
User
TPA
Cloud Server
Logout
SUPPORT
Search here
Sidebar Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
5:54 AM
29-May-21

Enter File Name to Delete

Enter File Name	andorid
	Delete

Fig.8 Delete file


Data Dynamic
Data Dynamic
Data Dynamic
localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/TPA_Attackers
prev
next
Iaas
Saas
Paas
Search here
Sidebar Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
localhost:8080/Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques/TPA_Attackers.jsp#
Search the web and Windows
5:58 AM
29-May-21

View All Attackers

Attacker Name	File Name	Owner Name	Sk Used	Attacker Type	Date of Attack
Hacker	Attack.jsp	Rajesh	[B@2f6aea	External	11/09/2020 17:48:55
Attacker	AuditMain.jsp	Manjunath	[B@10c624a	External	11/09/2020 18:18:13

Fig. 9 View Attacker

V. FUTURE SCOPE AND CONCLUSION

Proposed a secure cloud storage protocol for dynamic data (DSCS I) based on a secure network coding (SNC) protocol. To the best of our knowledge, this is the first SNC-based DSCS protocol that is secure in the standard model and enjoys public verifiability and have discussed some challenges while constructing an efficient DSCS protocol from an SNC protocol and have also identified some limitations of an SNC-based secure cloud storage protocol for dynamic data. However, some of these limitations follow from the underlying SNC protocol used. A more efficient SNC protocol can give us a DSCS protocol with better efficiency and have also identified certain SNC protocols suitable for append-only data and constructed an efficient DSCS protocol (DSCS II) for append only data.

REFERENCES

[1] B. Sengupta and S. Ruj, “Publicly verifiable secure cloud storage for dynamic data using secure network coding,” in ACM Asia Conference on Computer and Communications Security, 2016, pp. 107–118.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner,Z. N. J. Peterson, and D. X. Song, “Provable data possession at untrusted stores,” in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, “PORs: Proofs of retrievability for large files,” in ACM Conference on Computer and Communications Security, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[5] C. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” ACM Transactions on Information and System Security, vol. 17, no. 4, pp. 15:1–15:29, 2015.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,” IEEE Transactions on Parallel and Distributed Systems,vol. 22, no. 5, pp. 847–859, 2011.

[7] D. Cash, A. K¨upc¸ ¨ u, and D. Wichs, “Dynamic proofs of retrievability via oblivious RAM,” in EUROCRYPT, 2013, pp.279–295.

[8] B Prasanalakshmi, A Kannammal "Secure credential federation for hybrid cloud environment with SAML enabled multifactor authentication using biometrics" International Journal of Computer Applications, (2012),Vol.53, Issue.18.

[9] Satish, Karuturi S R V, and M Swamy Das. "Review of Cloud Computing and Data Security." IJAEMA (The International Journal of Analytical and Experimental Modal Analysis) 10, no. 3 (2018): 1-8, 2018.