|| Volume 5 || Issue 11 || November 2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

# A SOPHISTICATED DATA AUDITING SCHEME OVER SENSITIVE DATA ON PUBLIC CLOUDS EMPOWERING EFFECTIVE PRIVACY PRESERVATION

**Sabah Tasleem [1], Abdul Rasool MD [2]**

*Research Scholar, Dept. of Computer Science & Engineering, LIET, Hyderabad[1]*
*Associate Professor, Dept. of Computer Science & Engineering, LIET, Hyderabad[2]*
*AcademicStudent@gmail.com[1]*
*AcademicGuide101@gmail.com[2]*

---

**Abstract:- In the present-day, emerging demand over cloud computing architectures especially in data as a service platform there is a huge incremental necessity over the quantity of data that is being kept for service as it is been outsourced from data outsource on to the cloud data server. This leads to a great increase in the quantity of user data that will get accumulated into the cloud server. We may need to focus on enhancing data access capability with a focus on maintaining data integrity auditing and there is a chance of data duplication that has to be addressed effectively. So we adopt a secure data retrieval access policy of tag evaluation strategy over duplicate data. Most of the data that is been outsourced for service is sensitive personal information so we may need to facilitate confidentiality in such matters and privacy preservation can be initiated to acquire the reliability of sensitive information of data users.**

**In general, in cloud computing, effective and efficient data retrieval processes and policies are been empowered on a high scale wherein we need to adopt high secure confidentiality preservation of sensitive formats of data and not letting the huge volume of data that get duplicated by anyway. So data user attempts to retrieve the desired data as a unique copy that should get retrieved along with the consideration of time in the factor so that the data retrieval time should get reduced to increase the performance of the system. So this optimal mechanism helps us to deal with a huge volume of data as well flexible retrieval process in the most secure way of the auditing process. Data integrity over data access of sharable data could be done by syndicate verification of a collection for their data users with segment-based security keys. All the segmented data are been mapped with a variety of security keys in connection to the corresponding users even over the data modifications entertained over a variety of data users.**

**Keywords:-** *Cloud storage, public cloud auditing, secure deduplication, batch verification*

---

## I INTRODUCTION

In the cloud computing domain, we focus primarily on two crucial factors that are associated with data users. They are: administrative data use in connection to data access strategies and liberalizing data access policies within authorized data user segments to facilitate high privacy preservation standards towards the user data that got shared in the Cloud Service in larger volumes [1]. In the conventional security policies file independent block security key will be maintained in such that segment-wise privacy-preserving could be implemented successfully. In the present-day circumstances, the cloud Computing platform needs to get associated with a huge volume of data users whereas they could be categorized into unidentified divisions in which inter access file access strategies are been associated with the group identity which suits today's practical work environments [3].

Secure auditing policies to acquire high-level data security for the encrypted data sophisticated evaluation protocols are to be adopted to facilitate services in a wider range [2]. These days an emerging demand over cloud services towards infrastructural allocation in inter-cloud architectures makes us emphasize the optimal contribution of service requests with cost-effective resource access strategies[4]. In the conventional mechanism of inter-cloud resource accessing policy in contributing service switching by specific cloud Service Provider to optimize commercial factors without

disturbing the flexibility and accessibility in the desired modes [5]. A Trustable infrastructure access control leverages wide access ability over resources under service effectively and efficiently. This inter-cloud communication mechanism that collaborates resource availability and access ability among them in a heterogeneous server mode enables users to opt for services flexible to approach that meets Ad-Hoc, active, and remote distribution platforms [7]. Flexible decision-making will be provided if we adopt this infrastructure protocol facilitates the trustworthiness of cloud infrastructure services. With these trust attributes, boundaries of infrastructural access to the users will be enhanced will be delivered satisfactorily [8]. And Secure user feedback mechanism to the user is an added advantageous factor that enables reliability and trustworthiness over the transactional operations in inter Cloud Service systems [6].

With this privacy preserved feedback system we could eliminate negative opinions over the services provided by Cloud Service with appropriate administration activities taken over by cloud servers [9]. Infrastructural resources are totally under the control of cloud service providers facilitates encapsulated services with appropriate cost-effective and service-oriented measures into consideration frameless distributed computational sharable infrastructure resources. Primary users are facilitated with a less expensive access model and with a low maintenance cost with an effective and efficient decision making methodology in cloud service providers end [10].

## II LITERATURE SURVEY

### SecSVA: Secure Storage, Verification, and Auditing of Big Data in the Cloud Environment

This research paper primarily focuses on internet dependent electronic gadgets in which drastic hype in the shareable resource of private information identified by smart devices. These interactive devices may not be of a similar operational behavior but with the diversified one with a variety of intercommunication strategies to facilitate sensitive information in between the authorized devices. These interactive devices will share sensitive information without entertaining any leakage of data with the proper intercommunication operations as these devices had been driven with internet-based application programming. So the whole system user evaluation process identifies authorized user devices and even their communication is being monitored with a central administrative system that is a third party access control mechanism which effectively audits the data transactions.

### Cloud storage auditing with deduplication supporting different security levels according to data popularity

To fulfill the present-day necessity of cloud computing power huge volumes of user data the guard stored in the data store should be organized with appropriate utility app to facilitate wide accessibility as well l not violating the factors to consider on reliability or trustworthiness. An optimal solution is being adopted that clubs both infrastructural datastore capability with sophisticated data auditing operational behavior which is being driven by a third party public auditor. This adoption is an effective and efficient mechanism and we could also meet the commercial factors to optimize economic dependencies. In this approach, methodologies are been framed with more data instructiveness generalizing the 3rd operations over the data store as well as preserving the crucial data from hazardous attacks.

### Cloud storage auditing with deduplication supporting different security levels according to data popularity

Here is a primitive research effort that is being driven on third party data auditing strategies and data access policies power huge volume of data with deduplication approach data needs to get outsource in between the organized parties. Apart from the effective auditing policies driven you should also emphasize little more on systematic privacy policies that enhance is semantic security e over shareable data by adopting high-level encryption strategies and height the plane data formats replaced with complex data formats. So privacy preservation is achieved by converting the original data into a cipher-text based encrypted data in addition to the logical calculations to perform data retrieval operations effectively.

## III SYSTEM ANALYSIS

### Existing system:

In existing mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing. This public verifier could

be a client who would like to utilize cloud data for particular purposes or a third party auditor (TPA) who can provide verification services on data integrity to users. With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block. Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only.

Disadvantages of the existing system:

- By introducing a data-oriented block key to the data of shareable file empower privacy only to a specific user level and fails to address a huge volume of data users in public clouds.
- The auditing process lacks security standards as they are unable to revoke malicious users unable to protect the shared data from illegal attacks.

**Proposed system:**

In the present-day emerging demand over cloud computing architectures especially in data as a service platform, there is a huge incremental necessity over the quantity of data that is been kept for service most effective as it is been outsourced from data outsource on to the cloud data server. This leads to a great increase in the quantity of user data that will get accumulated into the cloud server, we may need to focus on enhancing data access capability with a focus on maintaining Data integrity auditing and there is a chance of data duplication that has to get addressed effectively.

So we adopt a secure data retrieval access policy of tag evaluation strategy over duplicate data. Most of the data that is been outsourced for service is sensitive personal information so we may need to facilitate confidentiality in such that privacy preservation can be initiated to acquire the reliability of sensitive information of data users. The total auditing process will be driven with a public auditor verifier who can flexibility administer data user request with an associated map security group key. Every same public auditor verifier could also be in a situation to revoke a data user that initiates malicious attacks.

Disadvantages of the proposed system:

- Data access policies that got adopted don't disturb the Data integrity of the shareable data of a specific data user which Got associated with the security group key.
- Ongoing demand over Cloud Computing data access scenarios, the system should be in a situation to address a huge volume of user requests more effectively and efficiently with the sophisticated public data auditing facilities is been implemented here.

## IV IMPLEMENTATION

**Modules:**

In this project, we made four segments based on the operational nature of domain expectations considering their roles and responsibilities as a deciding factor.

- **Data user module:**
- **Public verifier auditor module**
- **Group signature generation and evaluation module:**

**Data user module:**

On this page data user related to a specific group is been facilitated with their corresponding privilege services were in a group-oriented user categorization is been done at the point of better user account creation and registration page. Every data user will be identified only with their corresponding group identity along with their login credentials. Buy this methodology we are successful in adopting an optimal auditing technique.

**Public verifier auditor module:**

In this public verifier auditor module primarily emphasizes administration activities to facilitate reliable and Secure auditing in a more sophisticated way. In this module, the auditor could also have a look at the overall files that got associated with the user and group identity which could be audited with appropriate secure auditing policies. The auditing process will be typically driven to maintain the Data integrity of the user-specific share data so that it that are retrieval operations are been administered properly. Upon identification of malicious data attacks over the shared data so that the supposed data

user should get blocked to fulfill the empowered security policies over the auditing process in a most sophisticated way.

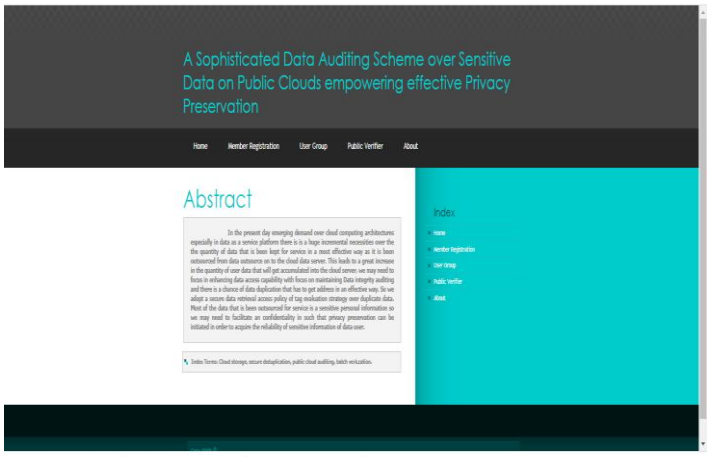
**Group signature generation and evaluation module:**

In this group signature generation module user-specific associated group related security key has to be mapped with the corresponding data user and could be reused upon the data access operations in evaluating the process of sophisticated auditing mechanism driven by public auditing verifier in such that system is been enhanced with a more reliable and trusted manner. This group signature generation module generates an automated hashcode which will be stored in the cloud data store and be verified for the users who attempt to request for specific file access upon successful mapping performs the file operations or violation leads to uh blocking of the user by the group auditor administration roles. All the users under a single group are been mapped with an identical security key so that team integrity could be maintained effectively.

## V PROJECT EXECUTION AND TESTING

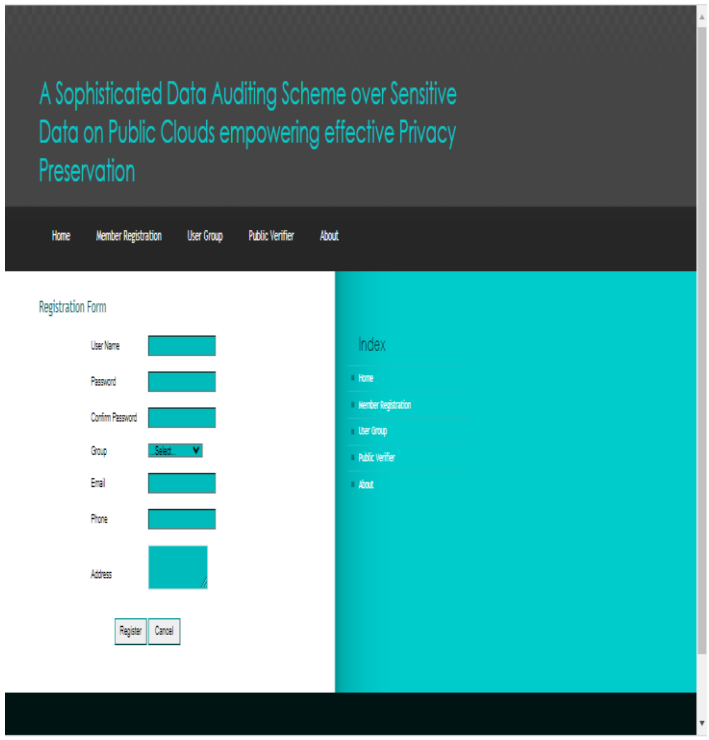
**Welcome screen:**

This is a welcome page of the project that is A Sophisticated Data Auditing Scheme over Sensitive Data on Public Clouds empowering effective Privacy Preservation.



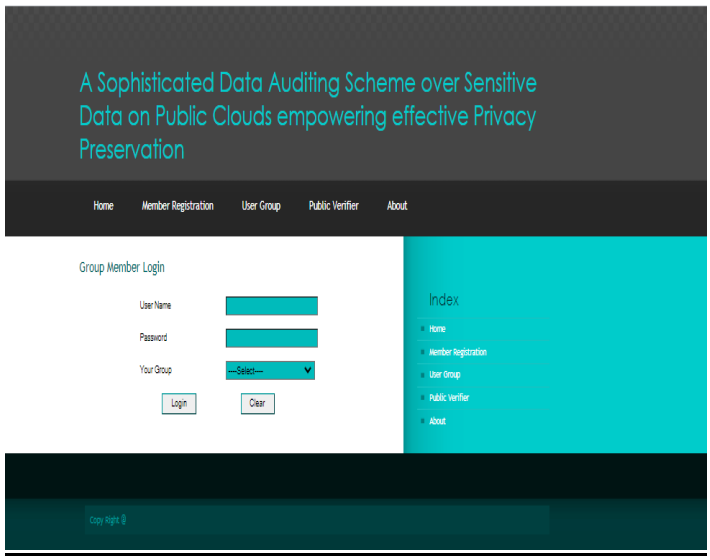

**Registration page :**

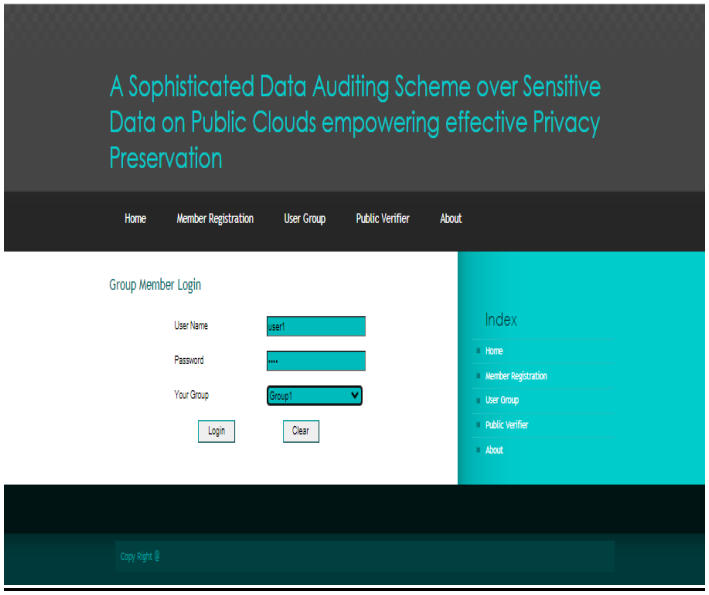
Using this registration page the person could be able to create his cloud user registration with his personal information which could be reused in logging into his account it with the credentials entered on this page. This is the page where are all users have to use to create the account in the database and while the service is provided by the cloud server.




**User Login page :**

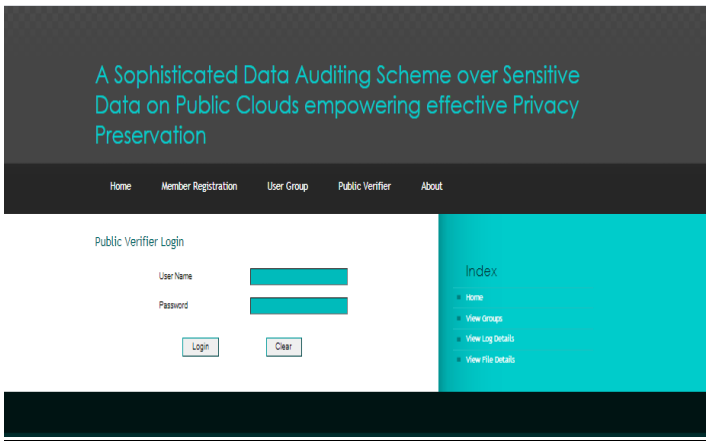
This is a user login page through which users can able to use his services by entering their credentials like user mail ID and password as well there is an option to make a new registration to create a new user account. If the entered credentials are not correct it will be redirected to the very same page. If the user enters the right credentials will get migrated to the user home page successfully and can utilize specified services provided by the server.

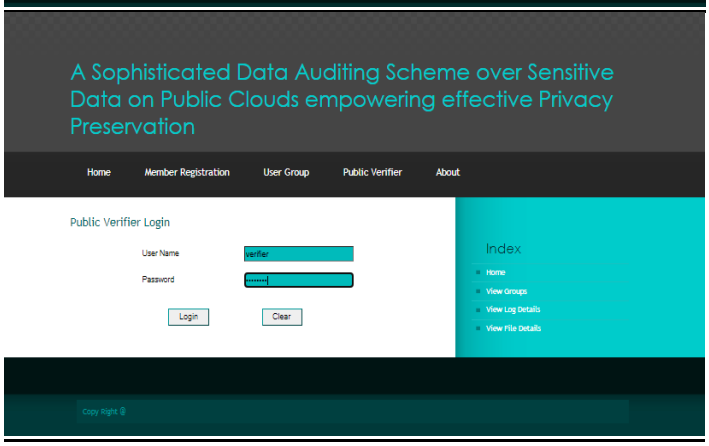





**Public Verifier Login page :**

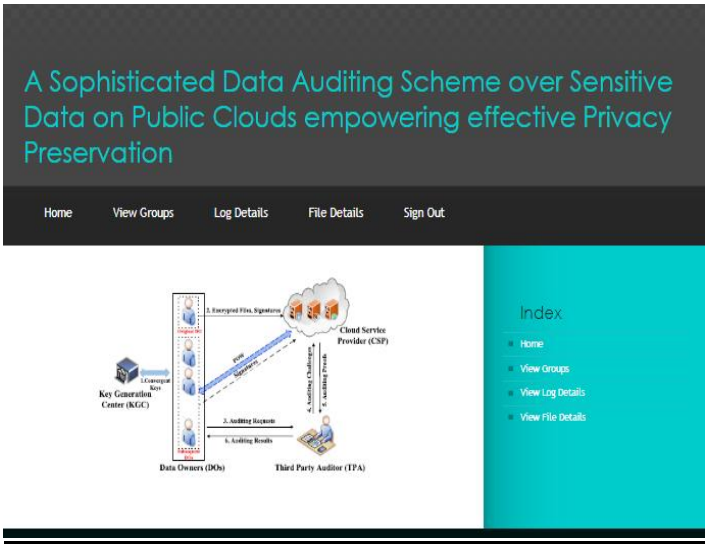
This is the Public Verifier login page through which the user can able to use his services by entering their credentials like user mail ID and password. If the entered credentials are not correct it will be redirected to the very same page. If the Public Verifier enters the right credentials will get migrated to the Public Verifier home page successfully and can utilize specified services provided by the server.



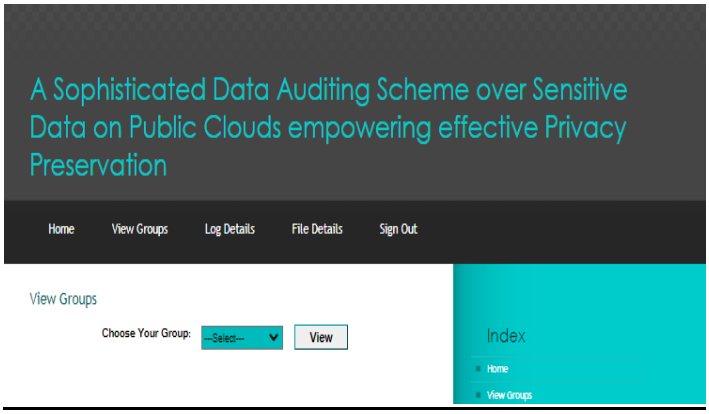

**Public Verifier homepage:**

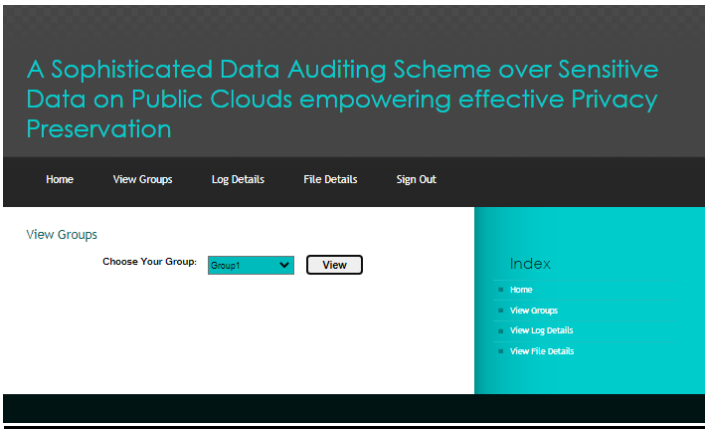
Public Verifier will enter into this page upon successful entry of credentials in the Public Verifier login page. This page enables all the services provided by the server like ViewGroups, LogDetails, and File Details options are facilitated.

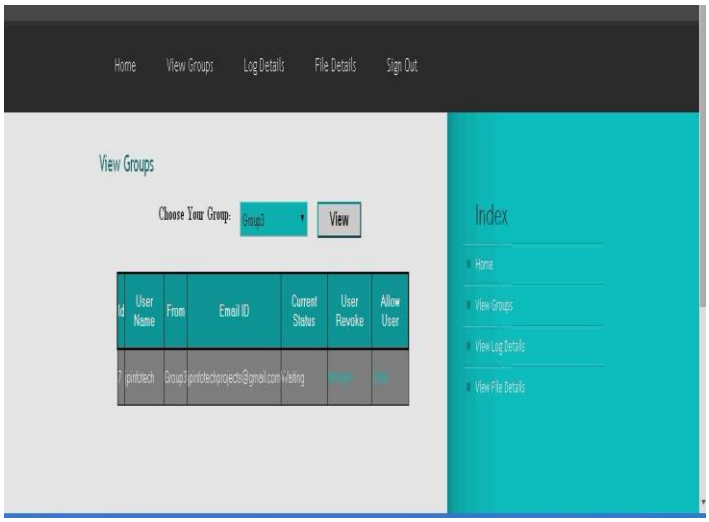



**View group details page:**

On this page, we could be able to check the user details that belong to a specific group selected by using a dropdown list and click on the view button.

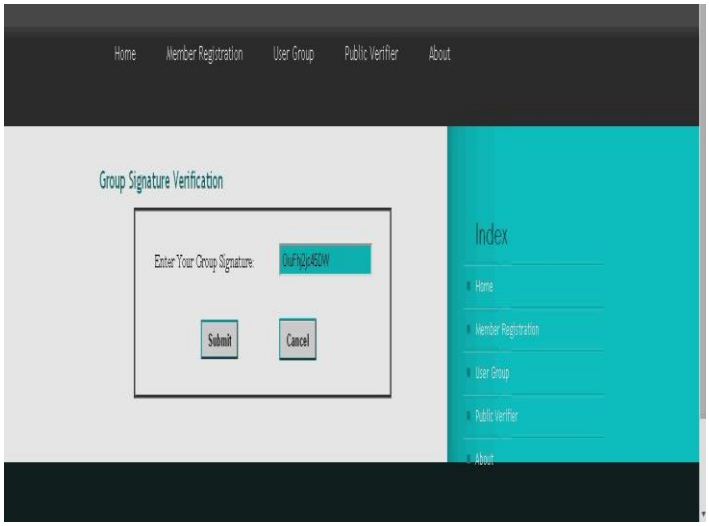




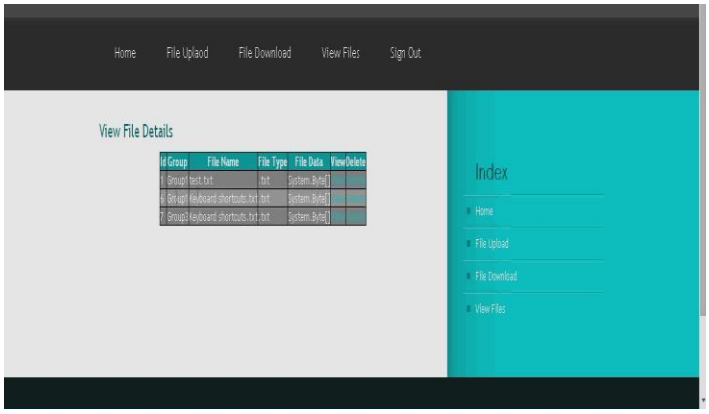

**Group signature verification page:**

On this page to fetch the data of the file of a group we may need to enter the group signature and click on the submit button.



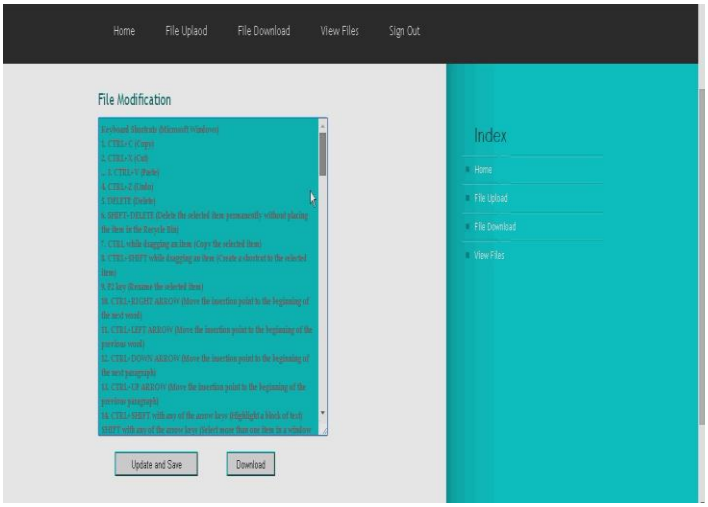

**View file details page:**

All files that got uploaded onto the cloud server are being listed here with facilities like to view and delete the specified file




**File data update page:**

The content of the specific file that got selected will be displayed with a facility of update and save.




## VI CONCLUSION

Data-to-day demand over cloud computing architectures especially in data as a service platform we adopted a scheme to address huge incremental necessities over the quantity of data that is been kept for service in the most effective way as it is been outsourced from data outsource on to the cloud data server. With a great increase in the quantity of user data that will get accumulated into the cloud server, we may need to focus on enhancing data access capability with a focus on maintaining Data integrity auditing and there is a chance of data duplication that has to get addressed effectively is employed successfully. So we adopt a secure data retrieval access policy of tag evaluation strategy over duplicate data. Most of the data that is been outsourced for service is sensitive personal information so we may need to facilitate confidentiality in such that privacy preservation can be initiated to acquire the reliability of sensitive information of data users. Effective and efficient data retrieval processes and policies are been empowered on a high scale wherein we need to adopt high secure confidentiality preservation over sensitive formats of data and not letting a huge volume of data that get duplicated in any way. So data user attempts to retrieve the desired data as a unique copy that should get retrieved along with the consideration of time in the factor so that the data retrieval time should get reduced to increase the performance of the system. So this optimal mechanism helps us to deal with a huge volume of data as well flexible retrieval process in the most secure way of the

auditing process. We achieved Data integrity over data access of sharable data that could be done by syndicate verification of a collection for their data users with segment-based security keys.

## REFERENCES

[1] G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues, ‘‘SecSVA: Secure storage, verification, and auditing of big data in the cloud environment,’’ IEEE Commun. Mag., vol. 56, no. 1, pp. 78–85, Jan. 2018, doi: 10.1109/MCOM.2018.1700379.

[2] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ‘‘Enabling public auditability and data dynamics for storage security in cloud computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011, doi: 10.1109/TPDS.2010.183.

[3] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, ‘‘Authentication in cloud-driven IoT-based big data environment: Survey and outlook,’’ J. Syst. Architect., vol. 97, pp. 185–196, Aug. 2019, doi: 10.1016/j.sysarc.2018.12.005.

[4] H. Hou, J. Yu, and R. Hao, ‘‘Cloud storage auditing with deduplication supporting different security levels according to data popularity,’’ J. Netw. Comput. Appl., vol. 134, pp. 26–39, May 2019, doi: 10.1016/j.jnca.2019.02.015.

[5] J. Gants and D. Reinsel. Digital Universe Decade—Are You Ready?’’ [Online]. Available: https://www.emc.com/collateral/analyst-reports/idcdigital-universe-are-you-ready.pdf

[6] X. Jia and J. Zhou, ‘‘Leakage resilient proofs of ownership in cloud storage, revisited,’’ in Applied Cryptography and Network Security. Lausanne, Switzerland: Springer, 2014, pp. 97–115, doi: 10.1007/978-3-319-07536 -5_7.

[7] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, ‘‘Dynamic-hash-table based public auditing for secure cloud storage,’’ IEEE Trans. Services Comput., vol. 10, no. 5, pp. 701–714, Sep./Oct. 2017, doi: 10.1109/TSC.2015.2512589.

[8] J. Han, Y. Li, and W. Chen, ‘‘A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities,’’ Comput. Stand. Interfaces, vol. 62, pp. 84–97, Feb. 2019, doi: 10.1016/j.csi.2018.08.004.

[9] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ‘‘Proofs of ownership in remote storage systems,’’ in Proc. CCS, Chicago, IL, USA, Oct. 2011, pp. 491–500, doi: 10.1145/2046707.2046765. [10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. CCS, Alexandria, VA, USA, 2007, pp. 598–609, doi: 10.1145/1315245.1315318