Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

ADVANCING CLOUD AUDIT PRIVACY: INNOVATIVE PROTOTYPE WITH ENHANCED PRIVACY MEASURES

Dr.K.Shekhar, *Assistant professor CSE, Vaagdevi College of Engineering(Autonomous),India*
Geetendra Kumar Gutti ,*UG Student ,CSE, Vaagdevi College of Engineering(Autonomous),India*
Gutam Nikhil ,*UG Student ,CSE, Vaagdevi College of Engineering(Autonomous),India*
Menthula Susmitha ,*UG Student ,CSE, Vaagdevi College of Engineering(Autonomous),India*
Pagadala Mahendar,*UG Student ,CSE, Vaagdevi College of Engineering(Autonomous),India*

ABSTRACT

This paper encompasses an architecture that allows processing of larger voluminous data and restricting the confidential data from being revealed to unreliable sources. The system is a modular and enables segmentation into components of varying importance, depending on the credibility of information. Clouds architecture following this set up will have an internet connected add-on segments of spaces for individual users. This segmentation will limit the option of public auditors to access certain data which belongs to user carefully categorized by themselves into protected segments. Resource allocation and retrieval of user data from Cloud Service provider (CSP) will also be efficient. From the obtained result, it is evident that communication overhead will be reduced as resource allocation will be having less latency in a modular architecture. Secondly, a data owner will be having the rights in selecting and providing the content for auditing to the Public Auditing tool. This enhances the security implementation of a modular architecture. Restrictive ambiguity is to ensure that the auditing tool does not gather any information from user or cloud. Without complete information of data owners, the available segments, credibility of information, it is impossible to hold their info or track them for later misuse.

1. INTRODUCTION

The data owners may decide to store information in a variety of formats, being text, images, videos, and much more. The data belongs to user and should not be revealed to users of unauthorized access. A cloud environment is ensured to be secured by a set of protocols which have various mechanisms to login, access and maintains a log of records of users' information. Having the access con-trolling mechanism is challenging issues [1] in vast cloudenvironment.9When a data owner occupies a space in the cloud, the space is actually a virtual space allotted. That virtual space will be having limitations for other users to access data which belongs to others. Conventional access methods will have techniques to protect the device holding the memory. Whereas in a cloud, the data is much farther than the owner's control. A cloud infrastructure is a completely different domain where no single user has a control on. Not only security, a cloud has also number of other features to concern about namely, concurrency, ease of use, integrity and confidentiality. This paper concentrates on the infrastructure of the cloud with specific access control mechanisms which limit third party auditors to affect the production of data owners. The information of data owners is as important as their information[2]. These challenges will be answered in this paper.

The add-on architecture has a modular architecture which segments the data based on their origin, importance and type. Either the user/data owners or cloud service provider will limit the concealment of data segments to third party auditor. A user will create a space as a module in the overall space and stores certain information over the cloud. There will be a necessity when either the cloud service provider or the user should check the contents in the module for integrity. When it arises, the cloud service provider will prompt the owner for the right module to be subjected to integrity verification. The third party auditors are independent bodies, which will have a log and type of access obtained by records of Cloud Service Provider[3]. They have to be reliable and should not render any sup-port to the benefits of either side. Time taken for integrity verification should not be overlapped with the utilization of data by the owner.

When there are many conventional methods5to restrict access to unwanted and unauthorized usage data many models are implemented. UCON approach of park andSandhee1011which targeted on providing authority over all sequential modules of cloud, adaptability of attributeswhich focuses on how the data is concealed from usersunknown. The model proposed in this paper will be intro-ducing architecture for add-on modules of space within auser's cloud space and a security model, which assesses the level of trust embedded on the third party auditor either by cloud service provider and user. This enables a user to restrict and avail access to a third party employed by CSP. It becomes an absolute requirement for a cloud ser-vice provider to inspect, examine and report the functionalities of its infrastructure. The proposed architecture is embedded with a tool to ensure that everything is operated as it's designated to. Data owners those are registered should be delivered with a reliable space, quality, security and additional resources for efficient handling[4].1Manymonitoring tools available in the market are capable of identifying anomalies in user's data but not in the architectures. Proposed monitoring tool will identify the problems faced by users end and overhead cost in the providers end. Add mostly, the available product is designed as software, which risks the chance of data leakage. The ultimate aim of this proposal is to eliminate all possible risk factors and ensure the integrity of data.

The users as well as providers cannot afford to expose their contents to a number of third party applications. The tools available today have been designed to test the quality of resources based on IP address, assuming that they are constant, but a cloud will be accessed by dynamically changing IP addresses which proves this theory wrong. A monitoring system should not operate on this base as the system might end up deducing the resources of a same user with different IPs to belong to different origins.

The prototype in this paper will compose both control and data plans along with a monitoring tool to identify how the modules of cloud space are being utilized by the data owners. These monitoring applications will determine a new logic in Utilization Pattern and helps to identify if any unauthorized access has been made when auditing is done. This approach will provide feedback to the service provider, data owners and third party auditing tools[5], which is completely new tan previous monitoring tools avail-able. Unlike other tools, transparency is promised in the approach, which deals with modular space of data owners that has been segregated, usage of them, trusted entries, service provider and resources that need to be verified by auditors. With a number of imperative qualities, monitoring tools should possess in a cloud environment, the following list is presented.

•Transparency in monitoring and reporting the operation of cloud.

•Knowledge of resource allocation and utilization.

•Maintaining the identity and access.

•Establish a relationship between all the devices a data owner uses to access his/her content (mobile/laptops/tabs etc).

•Up to data information on changes mode to resources (copies made through unauthorized access).

•Scalable and Quick mechanisms for analyzing huge volume of data.

The current techniques manage to fulfill all these requirements but not simultaneously. Having such a tool will be achievement for any cloud service provider and a data owner. This proposal is tested and successfully achieved all these feats simultaneously.

2. PROBLEM STATEMENT

The add-on architecture has a modular architecture which segments the data based on their origin, importance and type. Either the user/data owners or cloud service provider will limit the concealment of data segments to third party auditor[6]. A user will create a space as a module in the overall space and stores certain information over the cloud. There will be a necessity when either the cloud service provider or the user should check the contents in the module for integrity. When it arises, the cloud service provider will prompt the owner for the right module to be subjected to integrity

verification. The third party auditors are independent bodies, which will have a log and type of access obtained by records of Cloud Service Provider. They have to be reliable and should not render any support to the benefits of either side. Time taken for integrity verification should not be overlapped with the utilization of data by the owner. When there are many conventional methods to restrict access to unwanted and unauthorized usage data many models are implemented. UCON approach of park and Sandhee [7] which targeted on providing authority over all sequential modules of cloud, adaptability of attributes which focuses on how the data is concealed from users unknown.

2.1 LIMITATION OF PROBLEM STATEMENT

Complex Setup: The add-on architecture's modular approach might make the setup complex. Dividing data into different [14] segments based on origin, importance, and type could require careful planning and management, which might be challenging for users to set up correctly.

Dependency on Third Parties: Relying on third party auditors for data integrity verification introduces a dependency on external entities. Users and cloud service providers might not always have control over the actions and decisions of these auditors, potentially affecting the reliability of the verification process.

3. PROPOSED SYSTEM

The proposed architecture comprises of users like data originators, to those the data belong to, utilizer and monitoring. The utilizer will be user allowed by originator to access their private data on special request. Monitors are the component which makes records of all usage inform of logs to be submitted for public auditing purposes. Once the originator receives [8]-[12] requests from other users, base onthe security policies, originators provide rights or revoke them. The attributes of such data will be manipulated and be altered every time a utilizer accesses it. The data might get modified and the utilizer becomes the originator of new form of data, and the user location may not be stable in cloud environments which also make changes in the initial form when stored. These are certain attributes which are immutable, where id, originators information might not be changed at all times. Whereas mutable attributes will lead to dynamic changes and no value could be promised to be unchanged at anytime. Hence this architecture directs to cloud users and originators to determine the categorization based on the mutable features and hence protect the information within secure add on modules. These policies determine whether a utilizer is authorized by the cloud and the originator to utilize the data. These policies also ensure that the originators should not possess information that is deemed to be credible cannot be present in more than one add-on modules. Replication of data will also affect the integrity of data and owners. Data which are having mutual attributes may be present in various modules, with the understanding of having original contents at least in one place. The access control policy states that once credible information is found in more than one add-on module, and it is subjected to changes, the originator will be changed to the new user after revoking the access rights to the older originator.

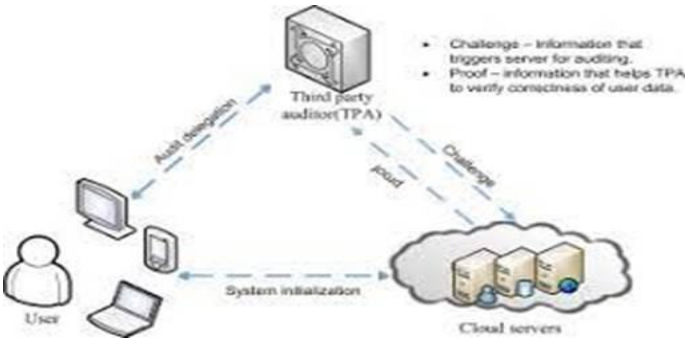
This will facilitate the leakage of information to be identified immediately.

3. FEATURE OF PROPOSED SYSTEM

Controlled Data Access: The proposed architecture allows data originators to maintain control over who can access their private data. This controlled access ensures that only authorized users are allowed to use the data, enhancing data privacy and security[13]. Improved Data Integrity: By recording all data usage through monitors and logs, the architecture enhances data integrity. The records submitted for public auditing purposes help in maintaining the accuracy and reliability of data usage, reducing the risk of unauthorized modifications[15].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

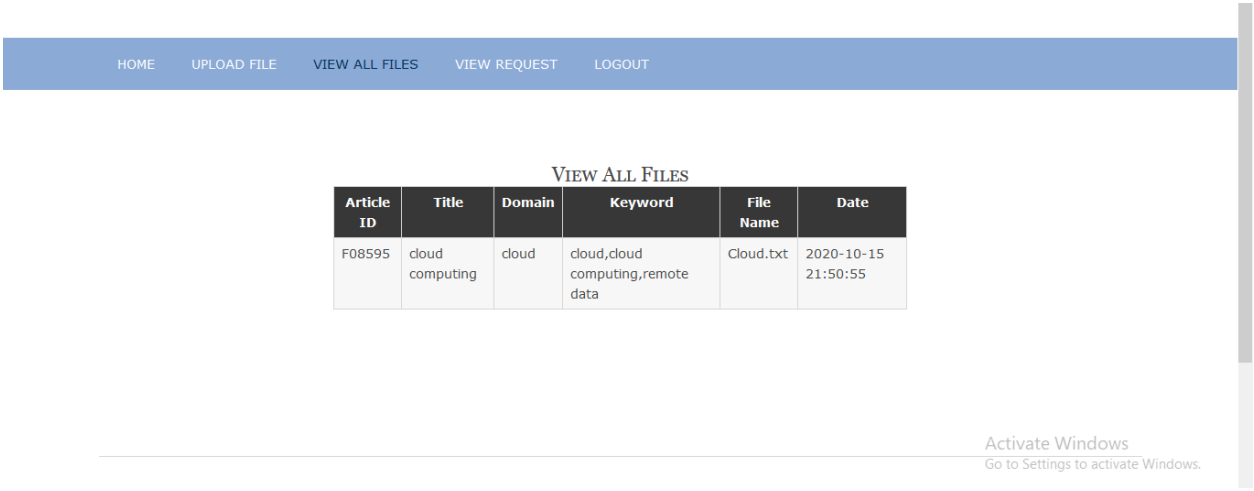
4. SYSTEM ARCHITECTURE



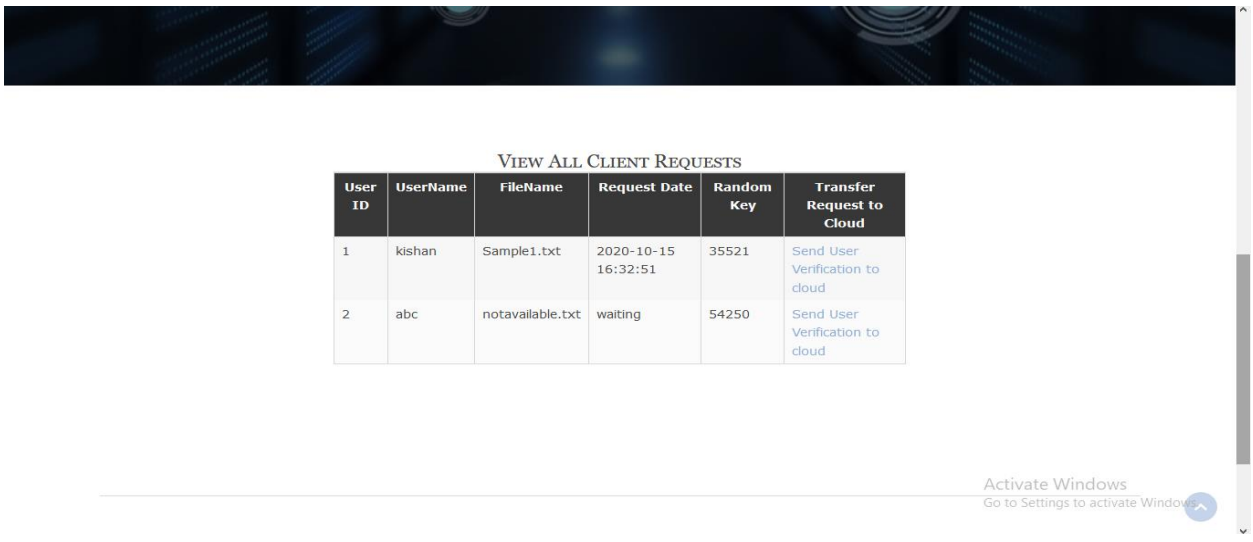
5. METHODOLOGY USED

- OWNER
- USER
- CLOUD

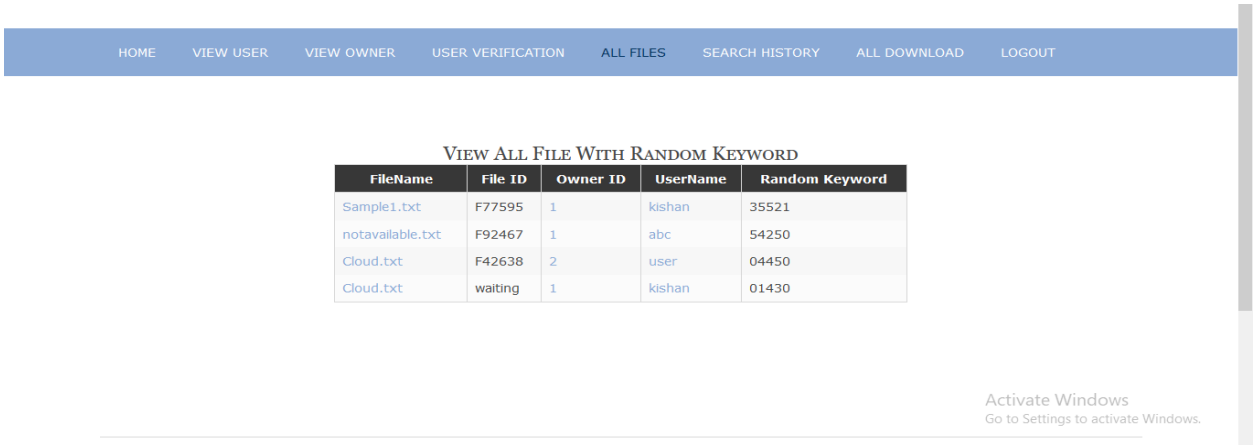
6. RESULTS / EXPERMENTALS



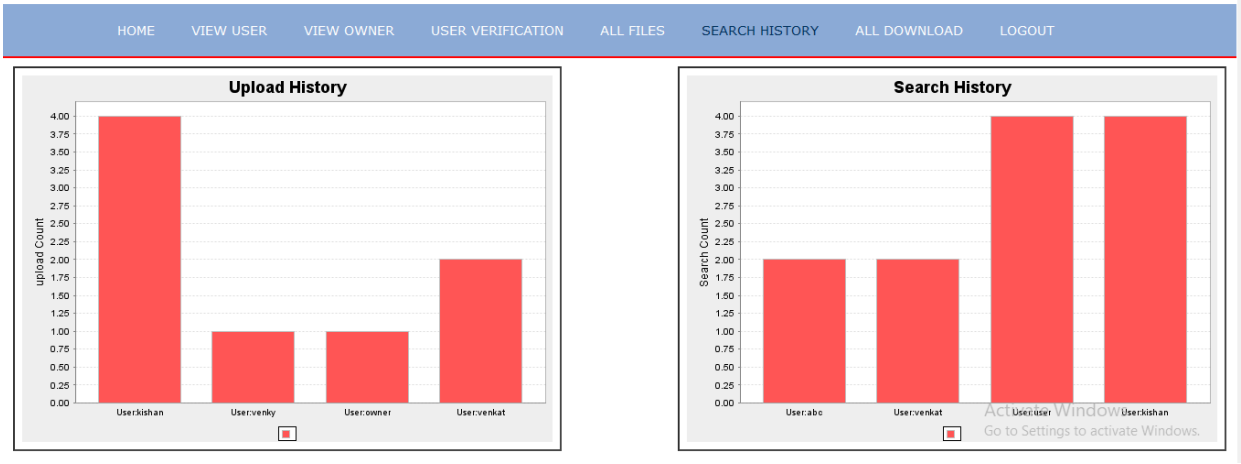
Client request



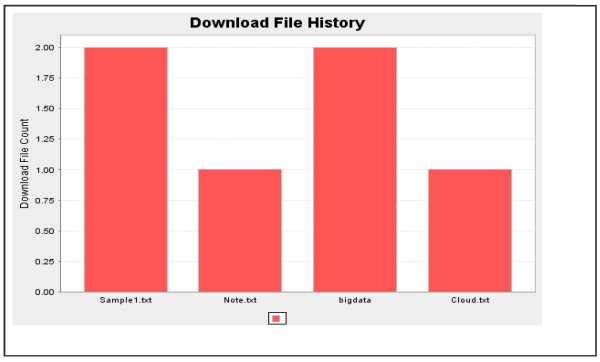
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024



Search and upload history with bar chart



Download history with bar chart



7. CONCLUSION

The prototype presented an architecture which enables thedata originator to identify the importance of their informa-tion, identify the impact upon losing them once the vastcloud infrastructure and thus segregating them into mean-ingful modules. These modules will be predefined with aset of policies to regulate the utilizer and cloud admin-istrators to transfer, modify and perform other operationsover original content. The data is handled in such a wayto avoid deadlocks and be produced to authorized utilizer.The architecture had another security enforcement that is,the cloud provider will also impose a monitoring modelwhich will analyze and repeat the connected devices beingoriginators and utilizer, the rendered service and perfor-mance of this architecture was documented. The modelhas been tested on the presence of trusted data origina-tors and utilizer. The future work will include the

privacypreserving algorithm over the data which will materializeadditional security parameters by both the ends. The ulti-mate aim of this architecture is to ensure that the usershave full features to protect their information in this vir-tual space. When it comes to public auditing, the indepen-dent body is made accountable to address protection ofdata in a cloud environment. The same may lead to leak-age of data. To some extent, this has been achieved by amonitoring prototype by cloud service provider and policystatements defined by the data originators over the add-onmodules presented by the model. These two advancementshave been proven better than previous models from the obtained results. The same results will be expected whenthe model is implemented in real time.

8. REFERENCES

1.F. M. Lazouski and P. Mori,Computer Science Review4, 81(2010).
2.G. M. Lazouski, F. Martinelli, and P. Mori, Usage control in cloudsystems,Proc. of ICITST-12(2012), pp. 202–207.
3.J. Park, D. Nguyen, and R. Sandhu, A provenance-based accesscontrol model,Proceedings of the 2012 Tenth Annual InternationalConference on Privacy, Security and Trust (PST) (PST'12), IEEEComputer Society(2012), pp. 137–144.
4.OASIS XACML TC.eXtensible Access Control Markup Language(XACML) Version 3.0, OASIS Standard(2013).
5.M. Colombo, A. Lazouski, F. Martinelli, and P. Mori, A proposalon enhancing XACML with continuous usage control features,Pro-ceedings of CoreGRID ERCIM Working Group Workshop on Grids,P2P and Services Computing, Springer(2010), pp. 133–146.
6.G. Aceto, A. Botta, W. de Donato, and A. Pescap,Comput. Netw.:Int. J. Comput. Telecommun. Netw.57, 2093(2011).
7.A. Cuomo, G. D. Modica, S. Distefano, A. Puliafito, M. Rak,O. Tomarchio, S. Venticinque, and U. Villano,J. Grid Comput.11, 1(2013).
8.M. Dhingra, J. Lakshmi, and S. K. Nandy, Resource usage monitor-ing in clouds,De ACM/IEEE 13th International Conference on GridComputing(2012).
9.P. Massonet, S. Naqvi, C. Ponsard, J.Latanicki, B. Rochwerger, andM. Villari, A monitoring and audit logging architecture for data loca-tion compliance in federated cloud infrastructures,IEEE Interna-tional Parallel and Distributed Processing Symposium, Anchorage,Alaska(2011).
10.D. Petcu,J. Grid Comput.12, 321(2014).
11.J. Povedano-Molina, J. M. Lopez-Vega, J. M. Lopez-Soler,A. Corradi, and L. F. Dargos,Futur. Gener. Comput. Syst.29, 2041(2013).
12.A. Kertesz, G. Kecskemeti, A. Marosi, M. Oriol, X. Franch, andJ. Marco, Integrated monitoring approach for seamless service pro-visioning in federated clouds,20th Euromicro International Con-ference on Parallel, Distributed and Network-based Processing,Munich, Germany(2012).
13.S. A. de Chaves, R. B. Uriarte, and C. B. Westphall,IEEE Commun.Mag.49, 130(2009).
14.J. Moses, R. Iyer, R. Illikkal, S. Srinivasan, and K. Aisopos,Shared resource monitoring and throughput optimization incloud-computing datacenters,IEEE International Parallel and DistributedProcessing Symposium, Anchorage, Alaska(2011).
15.L. Romano, D. De Mari, Z. Jerzak, and C. Fetzer, A novel approachto QoS monitoring in the cloud,First International Conference onData Compression, Communications and Processing, Palinuro, Italy(2011).