ADVANCING CLOUD AUDIT PRIVACY: INNOVATIVE PROTOTYPE WITH ENHANCED PRIVACY MEASURES

[1] Mr.B.Suresh,[2] G.Usharani,[3] J.Raju,[4] J.Akash,[5] K.Sidharth,[6] K.Dinesh
[1] Assistant Professor,[23456]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

This paper encompasses an architecture that allows processing of larger voluminous data and restricting the confidential data from being revealed to unreliable sources. Thesystem 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.

I. 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 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. 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. 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.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.

Data owners those are registered should be delivered with a reliable space, quality,security and additional resources for efficient handling. Many monitoring 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 provider'send. 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 shouldnot 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 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.

•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.

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 attributes which focuses on how the data is concealed from users unknown. The model proposed in this paper will be introducing architecture for add-on modules of space withina user'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.

II. LITERATURE SURVEY

TITLE: Advancing Cloud Audit Privacy: Innovative Prototype with Enhanced Privacy Measures

AUTHOR: Bob Duncan

ABSTRACT: Many people assume that cloud audit is no more difficult than IT audit in general. We provide an outline of the evolution of cloud, providing an explanation of how it differs from conventional IT. We consider three main purposes of audit, the most widely understood of which is the statutory

requirement for financial statements to be audited by an independent external auditor, which has been a cornerstone of confidence in global financial systems since auditing was introduced. It provides assurance that company managers havepresented a "true and fair" view of a company's financial performance and position, underpinning the trust and obligation of stewardship between company management and the owners of the company, the shareholders. Traditional audit approaches often involved treating IT systems as "black box" systems, meaning trust was placed in the IT systems, and looking at the functioning of the IT system was not considered part of the statutory audit. The obvious shortcoming of this approach was addressed by conducting a specific IT based audit of the IT systems, to ensure these systems performed exactly as expected. These audits are usually conducted by IT specialists, often in conjunction with accounting audit professionals to ensure the functioning of these systems are properly understood. However, these are not mandated under statute, which presents a weakness. In addition, there is no requirement for an annual audit to be undertaken. A second purpose of audit is IT systems audit.

TITLE: Advancing Cloud Audit Privacy: Innovative Prototype with Enhanced PrivacyMeasures

AUTHOR: Yuhong Liu

ABSTRACT: While cloud computing is gaining popularity, diverse security and privacy issues are emerging that hinder the rapid adoption of this new computing paradigm. And the development of defensive solutions is lagging behind. To ensure a secure and trustworthy cloud environment it is essential to identify the limitations of existing solutions and envision directions for future research. In this paper, we have surveyed critical security and privacy challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations,and envisioned future research directions. This action is fully justified now, when the research is reaching good levels in this area and the environmental context presents risk levels which can be harmful to organizations.

TITLE: Advancing Cloud Audit Privacy: Innovative Prototype with Enhanced PrivacyMeasures

AUTHOR: Whittington

ABSTRACT: The mobile cloud computing in the cloud, providing scalability, mobility and reduced maintenance costs, has had a very positive role in the development of various types of business, with more organizations adopting these technologies as an integral part of the infrastructure that supports their operational activities, with a significant impact on accounting information systems. Considering that these systems are responsible for the processing and storage of sensitive and confidential information assets, the adoption of those technologiesrequires a rigorous analysis regarding the security of information assets and the use of apps.

TITLE: Advancing Cloud Audit Privacy: Innovative Prototype with Enhanced PrivacyMeasures

AUTHOR: Nafiseh Soveizi

ABSTRACT: Today, the number of data-intensive and compute-intensive applications like business and scientific workflows has dramatically increased, which made cloud computing more popular because of its ability to deliver a large number of computing resources on-demand.Security is a critical issue affecting the wide adoption of cloud technologies, especially for workflows that are mostly dealing with sensitive data and tasks.

TITLE: Advancing Cloud Audit Privacy: Innovative Prototype with Enhanced PrivacyMeasures

AUTHOR: Yousra Abdul Alsahib

ABSTRACT: In past few years, cloud computing is one of the popular paradigms to host and deliver services over Internet. It is having popularity by offering multiple computing services as cloud storage, cloud hosting and cloud servers etc., for various types of businesses as well as in academics. Though there are several benefits of cloud computing, it suffers from security and privacy challenges. Privacy of cloud system is a serious concern for the customers. Considering the privacy within the cloud there are numerous threats to the user's sensitive data on cloud storage.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

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. 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 Sandee 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.

DISADVANTAGES:

- Complex Setup: The add-on architecture's modular approach might make the setup complex. Dividing data into different segments based on origin, importance.
- Dependency on Third Parties: Relying on third party auditors for data integrity verification introduces a dependency on external entities.

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. Once the originator receives 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. . Replication of data will also affect the integrity of data and owners. Data which are having mutual attributes may be presentin 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.

ADVANTAGES

- 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.
- 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.

SYSTEM ARCHITECTURE

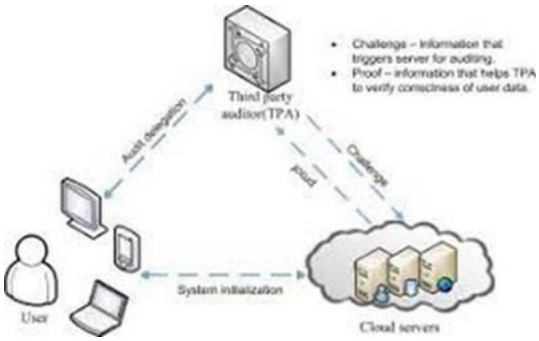


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- OWNER
- USER
- CLOUD

MODULE DESCRIPTION

OWNER: The client module typically refers to the component of the system that interacts directly with the end-user or client. It's the part of the system that is responsible for collecting data, processing requests, and communicating with the server-side components.

In the context of enhancing privacy measures in cloud audit, the client module might play a crucial role in ensuring secure communication, data encryption, access control, and user authentication. It could also involve features like secure login mechanisms, encryption of data before transmission, and implementing privacy-preserving protocols.

SERVER: The server module in this scenario refers to the part of the system that handles the processing and storage of data. It typically manages data storage, performs computations, and responds to requests from the client module.

When focusing on enhancing privacy measures in

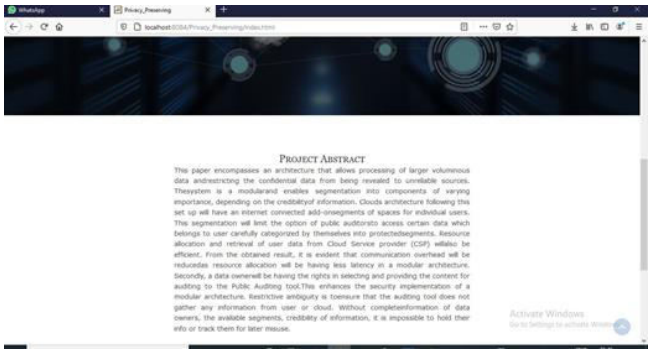
cloud audit, the server module plays a critical role in implementing secure data storage, encryption techniques, access control policies, and audit logging. It ensures that data is securely stored, processed, and accessed only by authorized entities while maintaining the integrity and confidentiality of the information.

THIRD PARTY AUDITOR: The third-party auditor module typically refers to an external entity or service that is responsible for independently verifying and auditing the privacy and security measures implemented in the cloud system. This module enhances transparency and trust by providing an unbiased assessment of the system's compliance with privacy standards and regulations.

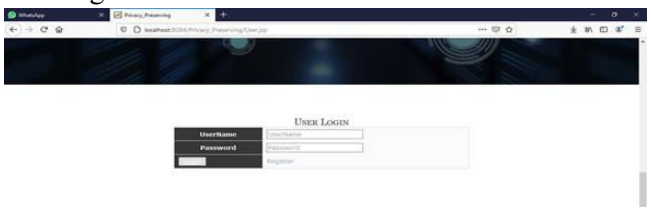
In the context of enhancing privacy measures in cloud audit, the third-party auditor module may perform tasks such as conducting security assessments, reviewing privacy policies, validating data protection mechanisms, and ensuring regulatory compliance.

V. SCREENSHOTS:

Home screen



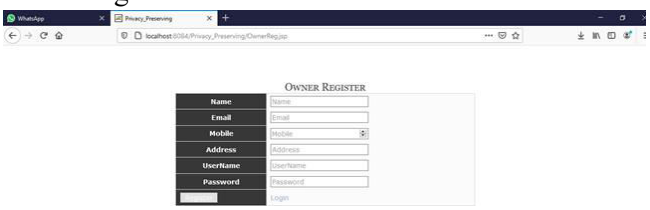
User login



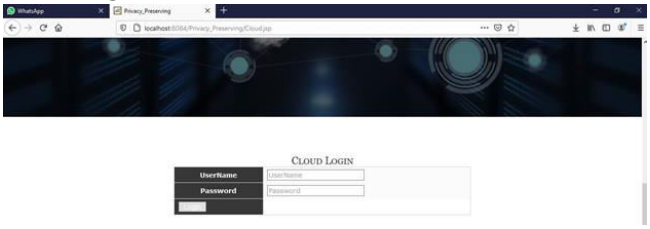
user registration

Owner login

Owner registration



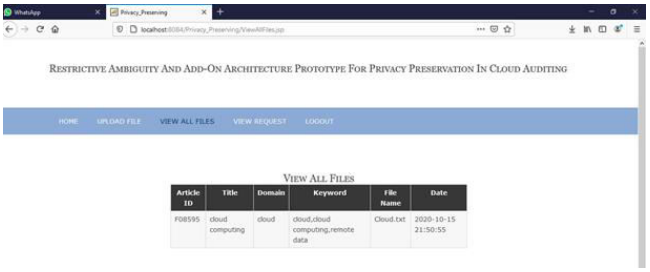
Cloud login



Owner home screen

Upload file

View all files



VI. CONCLUSION

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 vast cloud 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.

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, and J. Marco, Integratedmonitoring approach for seamless service pro-visioning in federated clouds,20th Euromicro International Conference 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 in cloud-computing datacenters, IEEE International Parallel and Distributed Processing Symposium, Anchorage, Alaska (2011).
15. L. Romano, D. De Mari, Z. Jerzak, and C. Fetzer, A novel approach to QoS monitoring inthe cloud, First International Conference on Data Compression, Communications and Processing, Palinuro, Italy (2011)