RESEARCH ARTICLE OPEN ACCESS

# Authentication Schemes for Session Passwords for Data Sharing in the Cloud

T.N.Sandya[1], J.Shanthini[2],
M.E[1], Assisatant Professor[2], Dept of Computer Science and Engineering,
Info Institute of Engineering,Coimbatore-India
Anna University
sandyanithy@gmail.com[1],
shanthinisampath@gmail.com[2],

**ABSTRACT**
Cloud computing is sharing of resources as needed basis which is consumed over the internet. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. Users' fear is mainly concerned of loss of control. To address this problem, in this paper, we propose a highly decentralized information accountability framework to keep track of the actual usage of the user's data in the cloud. The LOG file is created which keeps track of the actual usage of the user once authentication is triggered. Auditing mechanism which is done distributed strengthens users' control. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.
***Keywords***-Cloud computing, data sharing, accountability.

## I. INTRODUCTION

### *A. Cloud Computing*

Cloud computing is heavily based on a more traditional technology: grid computing, which has been researched for more than 20 years. Cloud computing focuses on the sharing of information and computation in a large network of nodes, which are quite likely to be owned by different vendors/companies. It is believed that cloud computing has been one of the sources for success in several major companies such as Google and Amazon. Cloud computing is expected to be the platform for next generation computing, in which users carry thin clients such as smart phones while storing most of their data in the cloud and submitting computing tasks to the cloud. A browser serves as the interface between clients and the cloud.

The data processed on clouds are outsourced, that leads to many issues: accountability. Such problem becomes a barrier to adopt cloud. To avoid this problem owner should be able to track their usage in the cloud. For example, user's data are handled by Service Level Agreement (SLA) which is made at the time of registration in the cloud. Conventional access control approaches were developed for closed domains which are not apt for certain environment due the features: First, data handling is outsourced by the Cloud Service Provider (CSP) to other members in the cloud and theses members can also delegate the tasks to others, and so on. Second, members are allowed to join and leave the cloud in their need basis. Finally, data handling in the cloud creates a complex and dynamic hierarchical service chain which does is absent in conventional environments. To overcome the above problems, we propose an approach called Cloud Information Accountability (CIA), which is based on the notion of information accountability. CIA keeps track of actual usage of the user which purely done on a distributed fashion. CIA, does not check the service-level agreements. Along with the CIA two modes were created for auditing purpose: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder While the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed.

## II. LITERATURE SURVEY

### *A. Provable Data Possession at Untrusted Stores*

G. Ateniese et al [1]. Focused retaining a file from the outsourced storage data. As part of pre-processing, the client may be stored at the server side. The client may expand the file or add data which is stored in the server side. Before deleting a local copy of file data possession makes sure whether that file is stored in the server. Clients encrypt a file prior to out-sourcing the storage. The client may ask proof for all the file blocks, making the data possession guarantee deterministic. Interestingly, when the server deletes a fraction of the file, the client can detect server misbehaviour with high probability by asking proof for a constant amount of blocks, independently of the total number of file blocks.

### *B. Provenance Management in Curated Databases*

P. Buneman et al [3]. Investigates general-purpose techniques for recording provenance for data that is copied among databases. Describes an approach in which they track the user's actions while browsing source databases and copying data into a curated database, in order to record the user's actions in a convenient, query able form. They present an implementation of this technique and use it to evaluate the feasibility of database support for provenance management. These databases are highly valued and have in some cases, replaced paper publication as the medium of communication. Specifically they consider the problem of tracking and managing provenance describing the user actions involved in constructing a curated database. This includes recording both

local modifications to the database (inserting, deleting, and updating data) and global operations such as copying data from external sources. Unfortunately, they cannot remember where the anomalous data came from, so cannot trace it to the source to resolve the conflict.

### *C. Cloud Computing and Information Policy: Computing in a Policy Cloud*

P.T. Jaeger et al [6]. Presented on paper that explores the nature and potential of cloud computing, the policy issues raised, and research questions related to cloud computing and policy. Ultimately, the policy issues raised by cloud computing are examined as a part of larger issues of public policy attempting to respond to rapid technological evolution. The objective is to introduce the policy concerns, research areas, and potential solutions related to cloud computing that will likely be the focus of discussion and deliberation in coming years. If these problems are considered during the developmental stages of cloud computing, perhaps they can be addressed before the consequences of non action are too significant. It focuses on a range of policy aspects of cloud computing specific issues raised by gaps in current laws and regulations. In the case of cloud computing, technological innovation, commercial interest, and consumer interest are all fast outpacing current information policy.

### *D .Cloud Security and Privacy: an Enterprise Perspective on Risks and Compliance*

T. Mather et al [8]. Discusses on Information Security and Cloud Computing, Providing a Secure Cloud, Cloud-delivered Security Services, and finally prove it on area of research. It explores the issues of the risks in cloud security and rises the solution for their risks. Main concentration is on variable Thread Trends, link determines overall risk, sources of insecurity, Cloud threads, Specific Customer Concerns Related to Security, Top Security Threats and Risks, Information Security Process and Management System, and provides the various technique of the solution for solving the above problems.

### *F. Accountability as a Way Forward for Privacy Protection in the Cloud*

S. Pearson et al [10]. Privacy in the sense of data protection, as defined by Directive Issues. The corporate entity seeking to contract for services in the cloud, the issue of how to provide appropriate privacy protection for cloud computing is important, and as yet unresolved. An approach is proposed in which procedural and technical solutions are co-designed to demonstrate accountability as a path forward to resolving jurisdictional privacy. It gives a concentration to outsourcing, offshoring, virtualization and Autonomic Technology.

### *G .Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services*

M.C. Mont et al [9]. Describes an innovative approach and related mechanisms to enforce users' privacy by putting users in control and making organizations more accountable. A technical solution based on sticky policies and tracing services that leverages Identifier-based Encryption (IBE) and TCPA technologies were introduced. Work is in progress to build a full working Prototype. Identity and privacy management solutions plays a key role in protecting identities and profiles, enforcing good management practices and helping to detect criminal activities and support forensic analysis. Enforced tracing and auditing of disclosures of confidential data, to increase data receivers' accountability. Disclosure of data subject to the fulfillment of the sticky policies 'constraints.

### *H. A Privacy Manager for Cloud Computing*

S. Pearson et al [11]. focus on a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. The different possible architectures for privacy management in cloud computing; give an algebraic description of obfuscation, one of the features of the privacy manager; and describe how the privacy manager might be used to protect private metadata of online photos.

### *I. Information Accountability*

D.J. Theyitzner et al[15]. describes with the access control and encryption no longer capable of protecting privacy, laws and systems are needed that hold people accountable for the misuse of personal information, whether public or secret. Important values have been over-whelmed by the increasingly open information environment in which they live. These threats follow from the ease of information storage, transportation, aggregation, and analysis. Their approach to information-protection policy has been to seek ways to prevent information from "escaping" beyond appropriate boundaries, then wring our hands when it inevitably does. This hide-it-or-lose-it perspective dominates technical and public-policy approaches to fundamental social questions of online privacy, copyright, and surveillance.

### *J. Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing*

Q. Wang et al [14]. Has envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data canters, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, they 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 client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing.

### *K. Towards a Vmm –Based Usage Control Framework for Os Kernel Integrity Protection*

M. Xu et al [16]. Focus on protecting kernel integrity is one of the fundamental security objectives in building a trustworthy operating system (OS). For this end, a variety of approaches and systems have been proposed and developed.

However access control models used in most of these systems are not expressive enough to capture important security requirements such as continuous policy enforcement and mutable process and object attributes. The increasing number of kernel-level root kit attacks clearly demonstrates this threat. In this paper they present a simple but effective usage control model UCONKI with unique properties of decision continuity and attribute mutability for OS kernel integrity protection. Further to enforce UCONKI security policies, they propose a virtual machine monitor (VMM) based architecture that is isolated and protected from attacks from other untrusted processes inside a virtual ma-chine (VM).They have implemented a proof-of-concept prototype in Linux to demonstrate the feasibility of our approach. The experiments is done with 18 real-world kernel root kits show that their approach is able to successfully detect and prevent all kernel integrity violations from them.

### *L. Decentralized Trust Management and Accountability in Federated Systems*

B. Chun et al [4]. Focus on three key problems for trust management in federated systems and present a layered architecture for addressing them. The three problems they address include how to express and verify trust in a flexible and scalable manner, how to monitor the use of trust relationships over time, and how to manage and re evaluate trust relationships based on historical traces of past behaviour. Existing work provides the basis for expressing and verifying trust, it does not address the concurrent problems of how to continuously monitor and manage trust relationships over time. These problems close the loop on trust management and are especially relevant in the context of federated systems where remote resources can be acquired across multiple administrative domains and used in potentially undesirable ways (e.g., to launch denial-of-service attacks).

### *M. Towards a Theory of Accountability and Audit*

R. Jagadeesan et al [7]. Describes accountability mechanisms, which rely on after-the-fact verification, are an attractive means to enforce authorization policies. Describes an operational model of accountability-based distributed systems. The analyses which support both the design of accountability systems and the validation of auditors for finitely accountability systems. The study provides formal foundations to explore the tradeoffs underlying the design of accountability systems including: the power of the auditor, the efficiency of the audit protocol, the requirements placed on the agents, and the requirements placed on the communication infrastructure.

### *N. Lineage Retrieval for Scientific Data Processing*

R. Bose et al [2]. Focus on dissemination and exchange of data sets as on the publication of conclusions. Accurately tracking the lineage of scientific data sets is thus imperative for the complete documentation of scientific work. Researchers are effectively prevented from determining, preserving, or providing the lineage of the computational data products they use and create, however, because of the lack of a definitive model for lineage retrieval and a poor fit between current data management tools and scientific software. Based on a comprehensive survey of lineage research and previous prototypes, presents a meta model to help identify and assess the basic components of systems that provide lineage retrieval for scientific data products.

### *O. Promoting Distributed Accountability in the Cloud*

S. Sundareswaran et al [13]. Focus on users' data that is usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly financial and health data) can become a significant barrier to the wide adoption of cloud services. Highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, they leverage the programmable capability of Java JAR files to enclose our logging mechanism together with users' data and policies. Ensuring that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, they also provide distributed auditing mechanisms.

### *P. Provenance in Cloud Computing*

Many applications which require provenance are now moving to cloud infrastructures. However, it is not widely realised that clouds have their own need for provenance due to their dynamic nature and the burden this places on their administrators. Analyse the structure of cloud computing to identify the unique challenges facing provenance collection and the scenarios in which additional provenance data could be useful. Another important point which indirectly depends on cloud provenance is trust establishment. Trust establishment in cloud computing requires collaborative efforts from industry and academia. Establishing trust in cloud systems requires two mutually dependent elements: (a.) support infrastructures with trustworthy mechanisms and tools to help cloud providers automate the process of managing, maintaining, and securing their systems and (b.) developing methods to help cloud users and providers establish trust in the operation of the infrastructure by continually assessing its operational status.

### *Q. Trusted Computing and Provenance*

Provenance systems can benefit from greater awareness of security principles and the use of security technology. Trusted Computing, a hardware-based method for establishing platform integrity, is not only useful, but immediately applicable. Demonstrating how existing Trusted Computing mechanisms can be used for provenance, and identify the remarkable similarity and overlap between the two research areas. This is accomplished through presenting architectural ideas for a trusted provenance system, and by comparing the respective requirements and capabilities of trusted systems and provenance systems.

### *R. Designing a Verification Protocol for Data Integrity*

An effective and flexible distribution verification protocol to address data storage security in cloud computing. In this protocol, is relied on erasure code for the availability, reliability of data and utilize token pre computation using Sobol Sequence to verify the integrity of erasure coded data rather than Pseudorandom Data in existing system. The

scheme provides more security to user data stored in cloud computing. The performance analysis shows that our scheme is more secure than existing system against Byzantine failure, unauthorized data modification attacks, and even cloud server colluding attacks.

## III. Proposed System

We propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and track able. Our proposed CIA framework provides end-to end accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honoured, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed. In proposed system to track the actual usage of the data, I aim to develop auditing and session key techniques which satisfy the requirement.

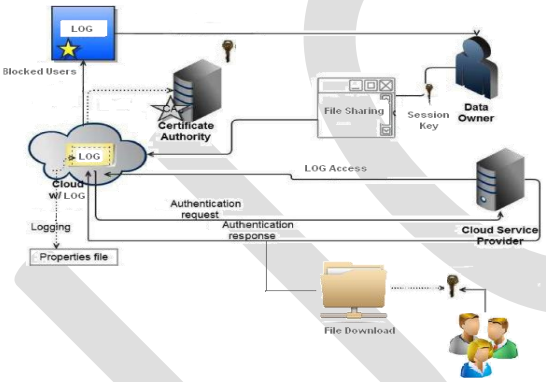


Fig. 1. System model.

## IV. Discussion

Data security and privacy is one of the biggest challenges in Cloud Computing. Cloud data must be protected not only against external attackers, but also corrupt insiders. Our Proposed system follows the information-centric approach which aims to make cloud data self-intelligent. In this approach, cloud data are encrypted and packaged with a usage policy using session key. The data when accessed will consult its policy, create a virtualization environment, and attempt to assess the trustworthiness of the data environment (using Trusted Computing).

## V. Conclusion

We propose an innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. This approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge. During the authentication, during of a log record, and during the merging of the logs. Also, with respect to storage overhead, we notice that our architecture is very lightweight, in that the only data to be stored are given by the actual files and the associated logs. Further, LOG act as a compressor of the files that it handles. In particular, as introduced in multiple files can be handled by the same logger component. To this extent, we investigate whether a single logger component, used to handle more than one file, results in storage overhead.

## VI. References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D.Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[2] R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," ACM Computing Surveys, vol. 37, pp. 1-28, Mar. 2005.

[3] P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf.Management of Data (SIGMOD '06), pp. 539-550, 2006.

[4] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf.System Sciences (HICSS), 2004.

[5] B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.

[6] P.T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?," J. Information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009.

[7] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of Accountability and Audit," Proc. 14th European Conf.Research in Computer Security (ESORICS), pp. 152-167, 2009.

[8] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), first ed. O' Reilly, 2009.

[9] M.C. Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," Proc. Int'l Workshop Database and Expert Systems Applications (DEXA), pp. 377-382, 2003.

[10] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Proc. First Int'l Conf. Cloud Computing, 2009.

[11] S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.

[12] A. Pretschner, M. Hilty, and D. Basin, "Distributed Usage Control," Comm. ACM, vol. 49, no. 9, pp. 39-44, Sept. 2006.

[13] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. European Conf. Research in Computer Security (ESORICS), pp. 355-370, 2009.

[15] D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen-baum, J. Hendler, and G.J. Sussman, "Information Accountability," Comm.ACM, vol. 51, no. 6, pp. 82-87, 2008. .

[16] M. Xu, X. Jiang, R. Sandhu, and X. Zhang, "Towards a VMMBased Usage Control Framework for OS Kernel Integrity Protection," SACMAT '07: Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 71-80, 2007.