ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 1-7

Effective Outsourcing Multiparty Computation Supporting Heterogeneous Keys

[1] VAKITI PULLAMRAJU, [2] M. SRI LAKSHMI, [3]Dr.S.PREM KUMAR

[1] M.Tech Research Scholar, G.Pullaiah College of Engineering and Technology, Kurnool
[2] Assistant Professor, G.Pullaiah College of Engineering and Technology, Kurnool
[3] HOD Department of Computer Science and Engineering,GPCET,Kurnool.

Abstract: These days, numerous associations outsource information storing to the cloud such that a part of an association (data owner) can share information or data easily among other members (clients). Because of the presence of security concerns in the cloud, both managers and clients are recommended to check the integrity of cloud information with Provable Information Ownership (PIO) before further use of information. Nonetheless, past strategy outsourcing the information and application to a gathering part causes the security and protection issues to turn into a discriminating concern. In that framework security and protection properties are not completely dissected.. We have recognized five most illustrative security and protection qualities (i.e. confidentiality, integrity, availability, accountability, and privacy-preservability). Starting with these characteristics, we exhibit the connections among them, the vulnerabilities that may be misused by aggressors, the hazard models, and in addition existing protection techniques in a cloud situation. Security investigations demonstrate that our scheme is secure

Keywords: Attack, Cloud Computing, Data Sharing, Revocation, Tracing.

1. INTRODUCTION

Cloud computing is transforming business by offering new options for businesses to increase efficiencies while reducing costs [2]. It lets user can access all applications and documents from anywhere in the world, freeing from the confines of the desktop and making it easier for group members in different locations to collaborate. It is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction. Cloud computing provides computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing infrastructure.

Some of the sourcing models used in the cloud computing are Private cloud, Public cloud, Hybrid cloud [2]. A private cloud is entirely dedicated to the needs of a single organization. It can be on or off premises. A public cloud is a multitenant cloud that is owned by a company that typically sells the services it provides to the general public. Where as in Hybrid cloud the customer uses a combination of private and public clouds to meet the specific needs of their business. In this approach, some of the organization's IT services run on-premises

while other services are hosted in the cloud to save costs, simplify scalability, and increase agility.
First, identity privacy[1] is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

Second, it is highly recommended that any member in a group[1] should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company.

Last issue is that efficient membership revocation mechanism [1] should be achieved without updating their secret keys of the remaining users and it is also desired to reduce the complexity of the key management Some of the issues related to the existing system are1. Propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. 2. Our existing scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. 3. It provides secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. 4. It provides rigorous security analysis, and performs extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.
The main disadvantage associated with the existing system is that:

1. Less security and privacy
2. Attack Prevention is not considered.

The drawback of the existing system can be overcome using this proposed system. The main contribution of this paper is that Proposed system to identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, we present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. We consider the cloud environment as a new computing platform to which the classic methodology of security research can be applied as well [3]. Therefore, we determine to employ an attribute-driven methodology to conduct our review. We employ the ecosystem of cloud security and privacy in view of five security/privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability) that are

the most representative ones in current research advances. Some researchers regard privacy as one component of security, while in this paper, we separate privacy from security due to its importance and specialty in cloud environments. Privacy is considered as highly relevant to security, as well as other security attributes that have positive or negative influences on privacy. The security ecosystem is generic and is applicable to any computer and networked systems. The main advantage of the proposed system is that:

1. Proposed system is more secure and privacy, its concentrate on all attributes of security and privacy prevents information leakage;
2. It uses the present three-tier data protection architecture to offer different levels of privacy to cloud customers.

2. GROUP SIGNATURE

Chaum and Van Heyst introduced the concept called group signature [6].In this paper we present a new type of signature for a group of person called a group signature which has the following properties: Any members of the group can sign messages. Keeps the identity secret from the verifiers. Only the group manager can reveal the real identity, when the dispute occurs which is called as traceability.

3. DYNAMIC BROADCAST ENCRYPTION

Broadcast encryption allows a user to distribute message securely to a set/group of users in an in secure environment so that only a privileged subset of users can decrypt the data. Apart from this Dynamic broadcast encryption [7] also allows the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of cipher texts are unchanged and the group encryption key requires no modification? The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique, which will be used as the basis for file sharing in dynamic groups

4. SYSTEM FUNCTIONING

A. Data Confidentiality:

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. New users should decrypt the data stored in the cloud before their participation, and revoked users is unable to decrypt the data moved into the cloud after the revocation

B. Threats in cloud confidentiality:

Malicious SysAdmin: The Cross-VM attack [5] discusses how others may violate confidentiality cloud customers that co-residing with the victim, although it is not the only threat. Privileged sysadmin of the cloud provider can perform attacks by accessing the memory of a customer's VMs. For instance, enables a sys admin to directly access the VM memory at run time by running a user level process in Domain.

1) Defense Strategies:

Co Trusted Cloud Computing Platform: It present a trusted cloud-computing platform (TCCP), which offers a closed box execution environment for IaaS services. TCCP guarantees confidential execution of guest virtual machines. It also enables customers to attest to the IaaS provider and to determine if the service is secure before their VMs are launched into the cloud. The design goals of TCCP are: 1) to confine the VM execution inside the secure perimeter; 2) that a sysadmin with root privileges is unable to access the memory of a VM hosted in a physical node. TCCP leverages existing techniques to build trusted cloud computing platforms. This focuses on solving confidentiality problems for clients' data and for computation outsourced to the cloud. With TCCP, the sysadmin is unable to inspect or tamper with the content of running VMs

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 1-7

C.Data Integrity:

Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

1) Threats to Cloud Integrity

Data Loss/Manipulation: In cloud storage, applications deliver storage as a service. Servers keep large amounts of data that have the capability of being accessed on rare occasions [5] . The cloud servers are distrusted in terms of both security and reliability, which means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss (e.g., backup and restore, data migration, and changing

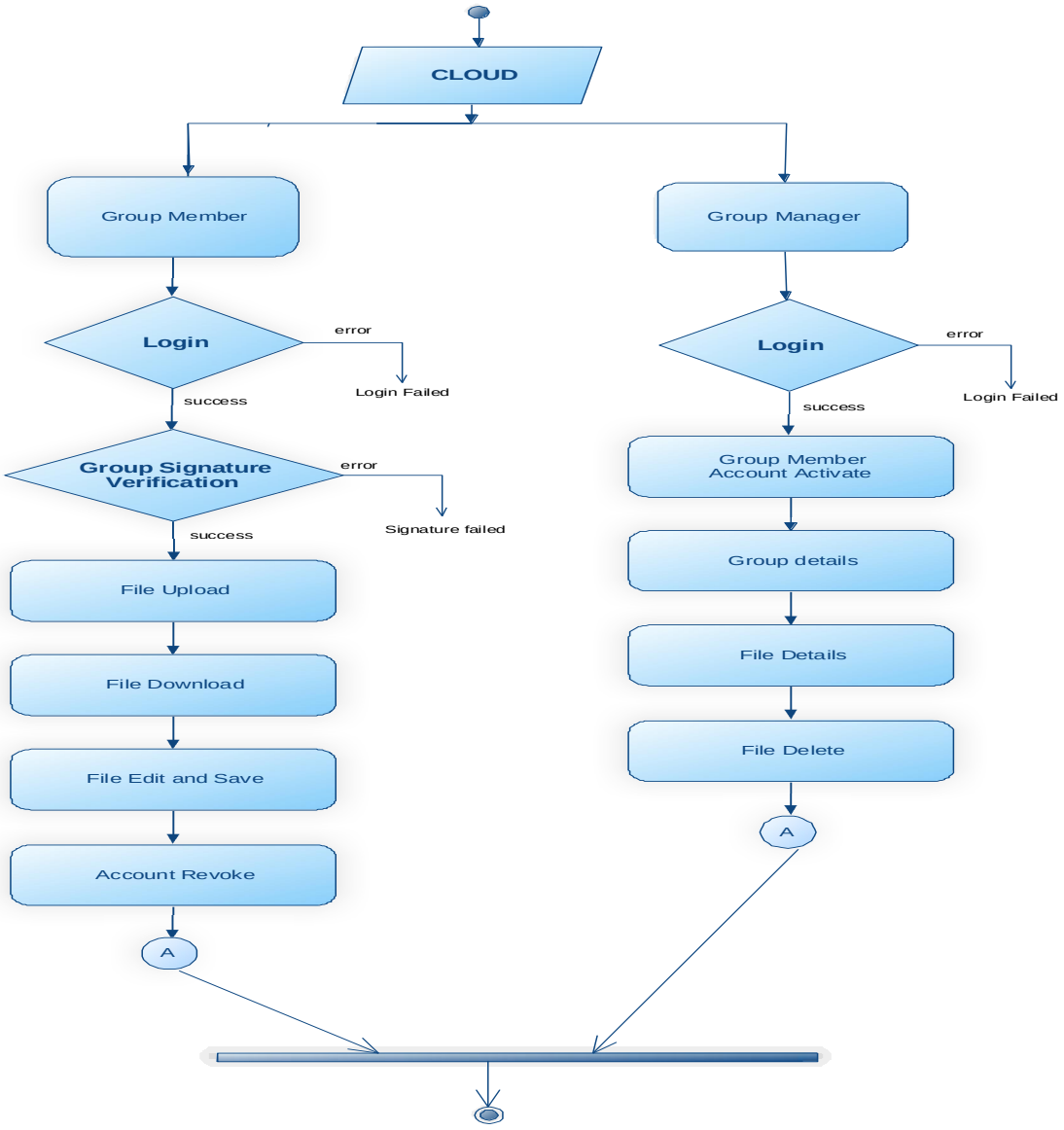

Fig 1 System Functioning

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 1-7

memberships in P2P systems). Additionally, adversaries may initiate attacks by taking advantage of data owners' loss of control over their own data.

2) Defense Strategies

The goal of Dynamic PDP (DPDP) is to support full dynamic operations (e.g., append, insert, modify, and delete). The purpose of dynamic operations is to enable authenticated insert and delete functions with rank-based authenticated directories that are built on a skip list. The experiment result shows that, although the support of dynamic updates costs certain computational complexity, DPDP is practically efficient.

D. Cloud Availability

Availability is crucial since the core function of cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system

1.Threats to Cloud Availability

Flooding Attack via Bandwidth Starvation: In a flooding attack, which can cause Deny of Service (DoS), a huge amount of nonsensical requests are sent to a particular service to hinder it from working properly. In cloud computing, there are two basic types of flooding attacks:

• Direct DOS – the attacking target is determined, and the availability of the targeting cloud service will be fully lost.

• Indirect DOS – the meaning is twofold: 1) all services hosted in the same physical machine with the target victim will be affected; 2) the attack is initiated without a specific target.

1)Defense strategy

Defending the new DOS attack: This new type of DOS attack differs from the traditional DOS or DDOS attacks in that traditional DOS sends traffic to the targeting application/host directly while the new DOS attack does not; therefore, some techniques and counter-measures for handling traditional DOSs are no longer applicable. A DOS avoidance strategy called service migration has been developed to deal with the new flooding attack. A monitoring agent located outside the cloud is set up to detect whether there may be bandwidth starvation by constantly probing the cloud applications. When bandwidth degradation is detected, the monitoring agent will perform application migration, which may stop the service temporarily, with it resuming later. The migration will move the current application to another subnet of which the attacker is unaware.

E.Cloud Accountability

Accountability implies that the capability of identifying a party, with undeniable evidence, is responsible for specific events. When dealing with cloud computing, there are multiple parties that may be involved; a cloud provider and its customers are the two basic ones, and the public clients who use applications (e.g., a web application) outsourced by cloud customers may be another party. A fine-grained identity, however, may be employed to identify a specific machine or even the faulty/ malicious program that is responsible.

1) Threats to Cloud Accountability

SLA violation: A. Haeberlen addresses the importance of accountability in cloud computing, where the loss of data control is problematic when something goes awry. For instance, the following problems may possibly arise: i) The machines in the cloud can be mis-configured or defective and can consequently corrupt the customer's data or cause his computation to return incorrect results;

ii) The cloud provider can accidentally allocate insufficient resources for the customer, an act which can degrade the performance of the customer's services and then violate the SLA;

*2) **Defense Strategies***

Collaborative Monitoring: A solution that is similar to AVM was developed by maintaining an external state machine whose job is to validate the correctness of the data and the execution of business logic in a multi-tenancy environment. It defines the service endpoint as the interface through which the cloud services are delivered to its end users. It is assumed that the data may only be accessed through endpoints that are specified according to the SLA between the cloud provider and the users. The basic idea is to wrap each endpoint with an adapter that is able to capture the input/output of the endpoint and record all the operations performed through the endpoint. The log is subsequently sent to the external state machine for authentication purpose.

F.Cloud Privacy

Privacy is yet another critical concern with regards to cloud computing due to the fact that customers' data and business logic reside among distrusted cloud servers, which are owned and maintained by the cloud provider. Therefore, there are potential risks that the confidential data (e.g., financial data, health record) or personal information (e.g., personal profile) is disclosed to public or business competitors. Privacy has been an issue of the highest priority.

1) Threats to Cloud Privacy

Computation Privacy Breach: In some sense, privacy-preservability is a stricter form of confidentiality, due to the notion that they both prevent information leakage. Therefore, if cloud confidentiality is ever violated, privacy-preservability will also be violated. Similar to other security services, the meaning of cloud privacy is twofold: data privacy and computation privacy.

2) Defense Strategies

Gentry proposed Fully Homomorphic Encryption (FHE) to preserve privacy in cloud computing. FHE enables computation on encrypted data, which is stored in the distrusted servers of the cloud provider. Data may be processed without decryption. The cloud servers have little to no knowledge concerning the input data, the processing function, the result, and any intermediate result values. Therefore, the outsourced computation occurs 'under the covers' in a fully privacy-preserving way. FHE has become a powerful tool to enforce privacy preserving in cloud computing. However, all known FHE schemes are too inefficient for use in practice. While researchers are trying to reduce the complexity of FHE, it is worthwhile to consider alleviating the power of FHE to regain efficiency. It has proposed somewhat homomorphic encryption, which only supports a number of homomorphic operations, which may be much faster and more compact than FHE.

CONCLUSION

In this paper, we tend to style a secure information sharing theme, EOMCSHK, for dynamic teams in associate degree untrusted cloud. In EOMCSHK, a user is in a position to share information with others within the cluster while not revealing identity privacy to the cloud. In addition, EOMCSHK supports economical user revocation and new user connection. additional specially, economical user revocation are often achieved through a public revocation list while not change the non-public keys of the remaining users, and new users will directly rewrite files keep within the cloud before their participation. Moreover, the storage overhead and therefore the secret writing computation price are constant. Intensive analyses show that our planned theme satisfies the specified security needs and guarantees potency moreover.

REFERENCES

[1] X. Liu, Y. Zhang, B. Wang and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Group in the Cloud," IEEE Tran. On Parallel and Distributed System,vol. 24, no. 6 June 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H Katz,A. Konwinski, G. Lee, A.D. Patterson, A. Rabkin, I Stoica, and M. Zaharia, " A View of Cloud Computing," comm.ACM, vol. 53, no. 4, pp. 50-58, April 2010

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010

[5] A.M. Lonea, D.E. Popescu, H. Tianfield "Detecting DDoS Attacks in Cloud Computing Environment" INT J COMPUT COMMUN, ISSN 1841-9836 8(1):70-78, February, 2013.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003

[7] D. Chaum and E. van Heyst, "Group Signatures," Proc Int'l Conf.Theory and Applications of Cryptographic Technique (EUROCRYPT),p p. 257-265, 1991.

[8] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993

[9] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology (CRYPTO), pp. 41-62, 2001.

[10] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud Proc. 10th Int. Conf. Applied Cryptography and Network

[11] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," proc. Int'l Conf. Pratice and Theory in Public