OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

APPLICATION SECURITY SERVICES FOR CLOUD COMPUTING

Manojkumar Mahajan [1], Suhas Kothavle[2], Nutan Sarode[3]
Asst. Professor, *Computer, G.V.A.I.E.T, Shelu, India*[1]
Asst. Professor, *Computer, G.V.A.I.E.T, Shelu, India*[2]
Asst. Professor, *IT, P.G.M.C.O.E., Wagholi,Pune, India*[3]
manojkumar.mahajan@gmail.com [1], *kothavle.suhas@rediffmail.com* [2], *nutansarode310@ gmail.com* [3]

Abstract: **Application security is a Major problem facing by many organizations. In which application security is relatively easy to maintain. By knowing which type of application is used and how to use this application in efficient manner by providing application security. In many cases this application is secure and harder to corrupt than in other site specific storage situation. For better Security purpose Temporal attribute based encryption method and multi keyword search encryption algorithm methods are analyzed In this paper, We also discuss the different new techniques which are suitable for privacy aware application intensive computing. And also how to improve the quality of services by providing efficient techniques that are observed.**

Keywords: *LSK, PSK, LOG.*

---∴∴∴---

I INTRODUCTION

Cloud computing is any hosted service that is delivered over a network, typically the Internet. Integrated cloud computing is a whole dynamic.

1.1 Cloud computing Service models

Computing system and has its advantages Cloud Services are divided into basically three parts. IaaS (includes the entire infrastructure stack), PaaS (sits on top of IaaS and adds an additional layer with application development capabilities and programming languages and tools), and SaaS (builds upon IaaS and PaaS and provides a self contained operating environment delivering presentation, application, and management capabilities) [3]. The advantages to the cloud computing service model will be discussed further in this section.

1.1.1 Infrastructure as a Service (IaaS)

This is the base layer of the cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization. Amazon EC2 is a good example of an IaaS. In Amazon EC2 (Elastic Compute Cloud) application will be executed on a virtual computer (also known as an instance).

1.1.2. Platform as a Service (PaaS)

Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service. Along with SaaS and IaaS, it is a service model of cloud computing. In this model, the consumer creates the software using tools and/or libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers, storage and other services. PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities [2]. There are various types of PaaS vendor; however, all offer application hosting and a deployment environment, along with various integrated services. Services offer varying levels of scalability and maintenance. PaaS offerings may also include facilities for application design, application

1.1.3. Software as a Service (SaaS)

Software as a Service is a method of providing users with software through the Internet [2, 3]. The combination of using the Internet together with software services have occurred for some time, although the term describing this sensation have been relatively diffuse until recent years. Several of the most common uses of these services include e-mail clients (e.g., Hotmail and Gmail), anti-virus scans (e.g., Symantec, McAfee, and Kaspersky) and word processors (e.g., Google Docs and Adobe Buzzword). These applications are not directly a collection of SaaSs, but the services they offer are. SaaS should not be seen upon as a way of creating

software or its underlying architecture. SaaS is more of a business model, which institutes a new way of distributing software. It is about delivering web-based software over the Internet, where the user runs the application in a browser and only pays for the use of the software instead of owning it.

1.2 Security Issues

There are many security problems occurred in cloud computing. Due to this type of security issues which affects the clients and there providers.

1.2.1 Service Level agreement

Cloud is applications delivered as services. Service-Oriented Architecture, the quality and reliability of the services become important aspects. However the demands of the service consumers vary significantly. It is not possible to full all consumer expectations from the service provider perspective and hence a balance needs to be made via a negotiation process. At the end of the negotiation process, provider and consumer commit to an agreement. In SOA terms, this agreement is referred to as a SLA. This SLA serves as the foundation for the expected Level of service between the consumer and the provider.

II METHODOLOGY

2.1 Accountability of abstraction Layer in Cloud

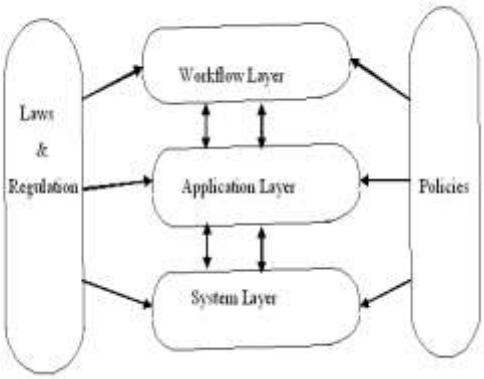

Figure 1. Abstraction Layers of Accountability in Cloud Computing

Figure 1 shows the abstraction layers for the type of logs needed for an accountable cloud which stipulated three basic layers: workflow, Application and system layers. It is important to note that the focus is on the abstraction layers of logs and not on architectural layers. Hence, the Trust Cloud framework is independent of virtual or physical environments, and consequently, the current cloud layers of IaaS, PaaS and SaaS. Such explicit definition of layers allows us to efficiently identify the areas of their application and their focus areas. At a glance, the five layers look deceptively simple, but the problem is more complex than it looks. Each layer has a slightly different focus, and different set of sub-components for each context. Our model simplifies the problem and makes accountability more achievable. The usefulness of abstraction layers is also analogous to OSI and TCP/IP networking layers. Let us now discuss the research issues, scope and scale of each Trust Cloud framework layer:

2.1.1 System Layer

Various Components working under the system layer are as follows.

- Operating Systems (OS)

OS system and event logs are the most common type of logs associated with cloud computing at the moment. However, these logs are not the main contributing factor to accountability of Application in the cloud, but a supporting factor. This is because in traditional physical server environments housed within companies, the emphasis was on server health, system status and ensuring uptime, as server resources are limited and expensive to maintain. In cloud computing, resources are relatively inexpensive and appear to end-users as though they were unlimited. OS logs, while important, are no longer the top concern of customers.

- File Systems

Even though the file system is technically part of the OS, we explicitly include it as a major component in a file-centric system layer. This is because, in order to know, trace and record the exact file life cycles, we often have to track system read/write calls to the file system. From the system read/write calls, we can also extract the files' virtual and physical memory locations, providing more information for further forensics.

2.1.2 Application Layer

- Provenance Logger

To enable reasoning about the origins, collection or creation, evolution, and use of Application, it is essential to track the history of Application, i.e., its provenance. Provenance information is often viewed as the foundation for any reasonable model of privacy and trust. It enables validation of processes involved in generating/obtaining the Application and the detection of unusual behavior. We also need to detect attempts to falsify provenance Application; to protect Application owners as well as Application providers from exposing sensitive, important information indirectly through provenance logs; and to enable efficient querying of provenance Application. Cloud computing-based provenance logging must fulfill the following criteria: (1) be secure and privacy-aware (to ensure that the logs themselves cannot be tempered with or be a source for knowledge inference); (2) be (eventually) consistent and complete (3) be transparent/non-invasive; (4) be scalable, e.g. avoid exponential explosion of provenance Application through application of summarization techniques; (5) be persistent over the long term; (6) allow for multiple tailored views (to permit access based on roles with different access Privileges); and (7) be efficiently accessible.

- Consistency Logger

While current cloud providers typically support a weaker notion of consistency, i.e., eventual consistency, it is important to have mechanisms to allow for rollback, recovery, replay, backup, and restoring of Application. Such functionality is usually enabled by using operational and/or transactional logs, which assist with ensuring atomicity, consistency, and durability properties. Logs have also been proven useful for monitoring operational anomalies. While these concepts are well established in the domain, cloud computing characteristics such as eventual Consistency, "unlimited" scale, and multi-tenancy pose new challenges. In addition, secure, privacy-aware mechanisms must be devised not only for consistency logs but also for their backups.

2.1.3 Workflow Layer

The workflow layer focuses on audit trails and audit related Application found in the software services in the cloud.

2.1.4 Automated Continuous Auditing

With the promise of high performance computing power from cloud architectures, we foresee automated auditing of financial and business process transactions in the cloud. Auditability is a prerequisite for such a step. However, achieving auditability via methods such as continuous auditing [4] within a highly virtualized environment is a very difficult and complex task. There needs to be consideration not only of the auditing of business logic and control flows, but also of the applications.

2.1.5 Patch Management Auditing

There is also a need for auditing of the management of virtual machine image bug fixes, patching and upgrades in a cloud environment. The scale of patching and deployment within the cloud environment is massive, and the associated logs need to be highly auditable for proper troubleshooting, playbacks and accountability of the technical staff performing these activities.

III PROPOSED ENHANCEMENT

3.1 Temporal attribute-based Encryption for Cloud Computing

• A: the set of attributes A = {A1, · · · ,Am};
• Ak(ti, tj): the range constraint of attribute Ak on [ti, tj], i.e., ti ≤ Ak ≤ tj ;
• P: the access control policy expressed as a Boolean function on AND/OR logical operations, generated by the grammar: P ::= Ak(ti, tj)|P AND P|P OR P;
• L: the access privilege assigned to the user's license, generated by L ::= {Ak(ta, tb)}Ak €A;
• APK: the public key over A;
• LSK: the private key with L;
• MSK: the master key presided by system managers;
• CP: the cipher text header over P;
• SK: the session key used to encrypt the Application by symmetrical encryption scheme. The definitions of P and L can meet the basic requirements of dual temporal expressions. We focus on the temporal access control and encryption process in cloud computing.

3.2 Temporal attribute based encryption algorithm

Secure information management architecture based on emerging temporal attribute-based encryption primitives. A policy system that meets the needs of complex policies by following algorithm

Step 1: Start

Step 2: Setup (1κ, A): Takes a security parameter κ as input, outputs the master key MSK and
The public-key APK;

Step 3: GenKey(MSK,uk,L): Takes the user's ID number uk as input, the access privilege L and MSK, outputs the user's private key LSK;

Step 4: Encrypt (APK, P): Takes a temporal access policy P and PK as input, outputs the cipher text header CP and a random session key SK;

Step 5: Decrypt (LSK, CP): Takes a user's private key LSK, and a cipher text header CP as input, outputs a session key SK.

Step 6: Stop method. So due to this strong encryption we justify actually what to show and what not to show are other core functionalities that will be done by this Method.

Security is one main concern for cloud-computing applications, when a user application which is owned by cloud service provider. In this paper We analyze challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud application (MRSE), and establish a set of strict privacy requirements for such a secure cloud application utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching". We first define the security requirements for the given problem of application security and then employ a secure usage of different technique for application scenarios. Where total number of keywords that can be searched is relatively limited and there are only few search terms in a query by using a trapdoor based system also to prevent the cloud server from learning additional information from the application and the index, and to meet privacy requirements.

IV CONCLUSION

Security is one main concern for cloud-computing applications, when a user application which is owned by cloud service provider. In this seminar We analyze challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud application (MRSE), and establish a set of strict privacy requirements for such a secure cloud application utilization system to become a reality.

Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching". We first define the security requirements for the given problem of application security and then employ a secure usage of different technique for application scenarios. Where total number of keywords that can be searched is relatively limited and there are only few search terms in a query by using a trapdoor based system also to prevent the cloud server from learning additional information from the application and the index, and to meet privacy requirements.

REFERENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE Transactions on Dependable and Secure computing, Vol. 9, No. 4, pp. 556 – 568, July/August 2012.

[2] Lv, H. and Y. Hu, "Analysis and Research about Cloud Computing Security Protect Policy", In proceeding of the International Conference intelligence Science and Information Engineering, pp. 214-216, 2011.

[3] Mathisen, E., "Security Chalenges and solutions in Cloud Computing", in proceeding of the IEEE International Conference and Digital Ecosystem and Technologies, pp. 208-212

[4] John C. Roberts II, and Wasim Al-Hamdani "Who Can You Trust in the Cloud? A Review of Security Issues Within Cloud Computing".

[5] 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.

[6] P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks" ACM Trans. Computer Systems, vol.11, pp. 205-225, Aug. 1993.

[7] Madhan Kumar Srinivasan, K Sarukesi , Paul Rodrigues, Sai Manoj M, and Revathy P, "State of the art Cloud Computing Security Taxonomies a classification of Security Challenges in the present Cloud Computing Environment", International Conference on Advances in Computing, Communications and Informatics.

[8] S. Yu, C. Wang, K. Ren, and W. Lou. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing". In Proceedings of IEEE INFOCOM, pp. 534-542, 2010.