Securing Services in Networked Cloud Infrastructures

Priyadharshini.P[1], Sharadha. I [2], Gnanaselvi.S[3], Pavunrajan.D[4]
[1, 2, 3, 4] PSR Rengasamy College of Engineering for Women, Sivakasi, India.

Abstract- *Cloud storage provides a convenient, massive, and scalable storage at low value; however,information privacy may be a major concern that forestalls users from storing files on the cloud confidingly. One approach of enhancing privacy from information owner purpose of read is to encode the files before outsourcing them onto the cloud and decode the files once downloading them. However, encoding may be a serious overhead for the mobile devices, and information retrieval method incurs an advanced communication between the info user and cloud. Normally with restricted information measure capability and restricted battery life, these problems introduce serious overhead to computing and communication similarly as a better power consumption for mobile device users, that makes the encrypted search over mobile cloud terribly difficult. In this paper, we have a tendency to propose TEES (Traffic and Energy saving Encrypted Search), a information measure and energy economical encrypted search design over mobile cloud. It is incontestable that the info privacy doesn't degrade once the performance improvement strategies are applied. Our experiments show that TEES reduces the computation time in the meantime the network traffics throughout the file retrievals also are considerably reduced.*

Keywords- Networked cloud security, security architecture, security attacks, trusted virtual domains (TVD), security management.

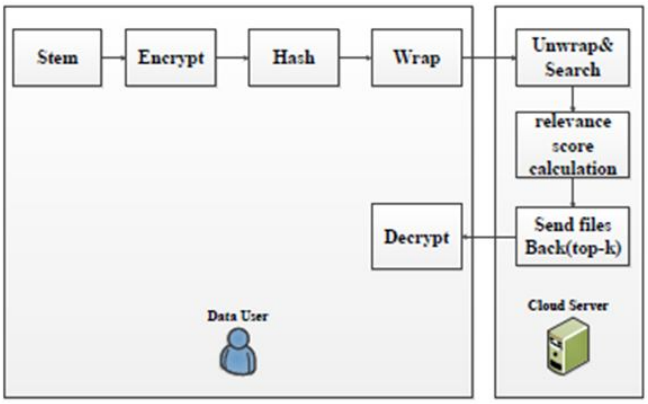
I. INTRODUCTION

Today most records offerings are hosted on-line and getting access toon-line offerings has come to be section of everyone's day by day life. For presents numerous benefits to establishments to go well with their dynamic necessities for internet hosting on-line offerings in the Internet. For example, cloud computing promotes on-demand example, customer sought to be the use of them to examine today's information with wealthy content material or doing on line banking with complicated functionalities. On the different hand, on line offerings have turn out to be a steady goal for malicious attackers trying to make the most vulnerabilities to achieve touchy facts to benefit them financially or to acquire get right of entry to structures which can then be used to crate in addition assaults on different systems. Hence it has end up a nightmare for the provider operators to make sure the security, quality and availability of their services. Cloud computing self-service. access, fast elasticity, pay for use and excessive availability. Hence unique sectors inclusive of healthcare, social networks and authorities are migrating their offerings to the cloud environment. There are distinct sorts of cloud fashions such as public cloud, non-public cloud and hybrid cloud, as properly as one of a kind sorts of deployment infrastructures such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In this paper, we will be solely involved with the IaaS cloud infrastructure.

II. LITERATURE REVIEW

A) Attack Detection- Techniques for detection of a range of attacks such as attacks in the trusted virtual domains (TVD)architecture. These include attacks between the virtual machines within a TVD, attacks between the virtual machines in different TVDs, malicious insider attacks, external attacks, and attacks against specific services such as DNS, database and web servers within a TVD.

B) Secure TVD Management-Management of virtual machines within a trusted virtual domain should satisfy well defined security policies. For instance, the addition and deletion of a virtual machine and the revocation of privileges associated



with a virtual machine in a TVD should be subjected to specified security policies.

C)Secure TVD Communications. Techniques for securing communications between VMs in different TVDs and mechanisms for enhancing the assurance of communications between the VMs in TVDs.

III. IMPLEMENTATION

A. Modules

1. Authentication Module
2. Crypto Module
3. TEES Module
4. Data detection

B. Modules Description

1. Authentication module

The Module is to register the new users and previously registered users can enter into our project. The register user only can enter into proposed process in this project.

2. Crypto Module

1. The encrypted search has expanded towards data sharing with protection of user's privacies. A scheme was proposed which encrypted each word of a document separately.
2. So, it is not adaptable with existing file encryption schemes and it does not deal with non-secure data

3. TEES Module

1. In order to achieve security enhancement with energy and traffic efficiency, we implement the modules in TEES using modified routines and new algorithms.
2. To control the statistics information loss, we enforced our one-to-many in the data owner module. We also wrapped the keywords to be search In order to get top-k important files, we achieved a ranking function to calculate the importance score on the cloud.

4. Data Detection

Every word in these files goes through stemming to retain the word stem. Next, thedata owner encrypts and hashes every term to fix its entry in the index.

The index is then created by the data owner. Finally, the data owner encrypts the index and stores it into the cloud server, together with the encrypted file set.

IV. CONCLUSION

In this paper, we have proposed techniques for securing services that are hosted in a multi-tenant networked cloud infrastructures. The proposed architecture is based on trusted virtual domains and it considers both the security policies of the tenant domains as well as specific security policies of the virtual machines in the tenant domains. We also discuss security management policies such as secure addition and deletion of a virtual machine and the revocation of privileges associated with a virtual machine in a trusted virtual domain. We describe techniques for detecting a range of attacks such as attacks between the virtual machines within a TVD, attacks between the virtual machines in different TVDs, malicious insider attacks and attacks against specific services within a TVD.

V. ACKNOWLEDGEMENT

I take his chance to precise my hearty due to my guide faculty member. **Pavunrajan.D** for his steering and sharing his findings for technical steering and direction. Suggestion given by his were forever useful during this work to succeed. His leadership has been greatly valuable on behalf of me to figure on this project and is available with the best out of it.

REFERENCES

[1] P.Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards & Technology, Gaithersburg, MD, USA, Tech. Rep.,SP 800-145, Sep. 2011.
[2] J. Francois, et al., "Betrick: Tracking botnets using NetFlow and PageRank", presented at the 10th Int. IFIP TC 6 Networking Conf., Valencia, Spain, May 2011.
[3] D. Moore, et al., "Inside the slammer worm," IEEE Secur. Priv., vol. 1, no. 4, pp. 33–39, Jul./Aug. 2003.
[4] M. Carbone, et al., "Secure and robust monitoring of virtual machines through guest-assisted introspection," in Proc. Symp. Res. Attacks, Intrusions Defenses, The Netherlands, Sep. 2012, pp. 22–41.
[5] W. Cui, et al., "Tracking rootkit footprints with a practical memory analysis system," presented at the USENIX Security Symp., Bellevue, WA, USA, Aug. 2012.
[6] Y. Fu and Z. Lin, "Space traveling across vm: Automatically bridging the semantic gap in virtual machine introspection via online kernel data redirection," presented at the 33rd IEEE Symp. Security & Privacy, Washington, DC, USA, May 2012.
[7] B. Jain, et al., "SoK: Introspections on trust and the semantic gap," presented at the 35th IEEE Symp. Security & Privacy, Washington, DC, USA, May 2014.
[8] D. Zhao, et al., "Peer to peer botnet detection based on flow intervals," presented at the IFIP Information Security and Privacy Conf., Heraklion, Greece, Jun. 2012.

[9] F. Tegeler, et al., "BotFinder: Finding bots in network traffic without deep packet inspection," presented at the ACM Int. Conf. Emerging networking experiments and technologies, Nice, France, Dec. 2012.
[10] L. Bilge, et al., "DISCLOSURE: Detecting botnet command and control servers through large-scale netflow analysis," presented at the Annual Computer Security Applications Conf., Orlando, FL, USA, Dec. 2012.