RESEARCH ARTICLE OPEN ACCESS

Preventing Zombies in Virtual Network System Using HIPS

V.Nancy[1], P.Ramadoss[2], N.Vasumathi[3]
[1]M.E, Computer Science and Engineering Parisutham Institute of Technology & Science Affiliated to Anna University Chennai Tamil Nadu- India
[2]Assistant Professor Parisutham Institute of Technology and Science Affiliated to Anna University Chennai Tamil Nadu- India
[3]M.E, Computer Science and Engineering Parisutham Institute of Technology & Science Affiliated to Anna University Chennai Tamil Nadu- India

Abstract
Cloud Security is the most imperative issue which has fascinated a lot examine and development errors in last few years. While enjoying the handiness brought by this new emerging technology, user's qualms of trailing control of their own data can become a significant obstacle to the wide adoption of cloud services. To deal with this problem, we suggest a new extremely decentralized information accountability framework to keep track of the actual usage of the user's data in the cloud. Here we offer an object-centred approach that enables enclosing our logging mechanism together with user's data and policies. We leverage the Logging mechanism to both create a dynamic and traveling object and to ensure that any access to user's data will trigger validation, automated logging and auditing. As modification we are generating the encrypted key for Logs retrieval. It improves the security of Log record transmission over the cloud server and enables count based accountability on download access.
Keywords: cloud computing; accountability; decentralized; logs; auditing.

I. INTRODUCTION

Cloud computing is an inclusive platform that resides in a large data center and they dynamically provide servers to address a wide range of needs in the current environment. Cloud Computing plays a vital role in the modern world as it reduces the work of the users and make it very simple for accessing various resource across the world. It enables the user to access resource without installation of software and hence it is user friendly. They avoid collision by increasing the availability of service. Wastage of resources is completely deployed as the services are provided on demand base. It is very helpful in the critical situation by disaster recovery and business continuity. They form the basis for building various internet applications which makes the whole world to shrink. Cloud Computing offers a compelling business case to acquire a cheaper alternative than the current Data Centre Infrastructure more on cost reduction. Cloud Computing offers a compelling business case to build a more efficient and effective alternative than the current organization structure. The number one reason enterprises are looking to the cloud is to support their growing use of mobile devices (Brand Interaction as a Service) followed closely by helping to reduce their costs.

II. EXISTING SYSTEM

In cloud computing atmosphere users may not identify the machines which really process and host their data. While enjoying the dexterity brought by this new technology, users also start worrying on losing control of their own data. The data processed on clouds are frequently outsourced, leading to a number of issues related to accountability, including the handling of individually identifiable information. Such worries are becoming a significant obstacle to the wide adoption of cloud services. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional entree control tactics developed for closed domains such as databases and operating systems, or attitudes using a centralized server in distributed situations.

In general, NICE includes two main phases:

1. Deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic. A NICE-A intermittently scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability toward the collaborative attack goals, NICE will resolve whether or not to put a VM in network inspection state.

2. Once a VM arrives at inspection state, Deep Packet Inspection (DPI) is applied.

Architecture:

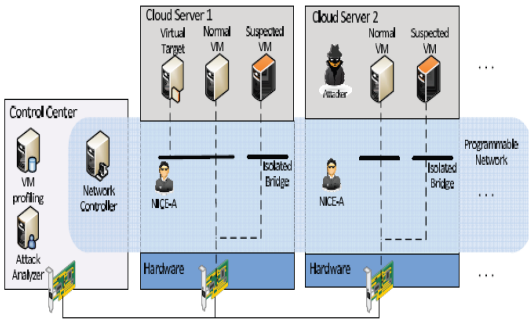

Fig:1 Existing System Architecture.

NICE : NIDS and Counter Measure Selection in VM system

- Multiphase disseminated vulnerability revealing.
- Measure the impact.
- Countermeasure selection mechanism.

IMPLEMENTATION MECHANISM:

- Attack graph based analytical model
- Reconfigurable virtual network based counter measure.

2.1 SYSTEM COMPONENTS

2.1.1 VM Profiling:

Virtual machines in the cloud can be outlined to get precise information about their state. Major factor that sums toward a VM profile is its connectivity with other VMs. Any VM that is connected to more quantity of machines is more decisive than the one connected to fewer VMs because the effect of negotiation of a highly connected VM can cause more damage. Also required is the awareness of services running on a VM so as to validate the authenticity of alerts affecting to that VM. An attacker can practice port-scanning program to perform a powerful examination of the network to look for open ports on any VM. All these factors combined will form the VM profile.

Operation

NICE is a novel multiphase dispersed network intrusion detection and prevention framework in a virtual networking environment that seizures and inspects mistrustful cloud traffic without interposing user's applications and cloud services.

- NICE integrates a software switching solution to quarantine and scrutinise suspicious VMs for further investigation and shield. NICE hires a novel attack approach for attack detection and preclusion by correlating attack behaviour and also suggests active counter- measures.

- NICE improves the implementation on cloud servers to minimize resource ingesting.

Disadvantages

- Data handling can be farm out by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also hand over the tasks to others, and so on. If there is no logging mechanism the data proprietor cannot able to see their data usage.
- Users are permissible to join and leave the cloud in a flexible mode so there is a chance for extra consumption on the resources beyond the subscription limit.

Virtual machines in the cloud can be outlined to get precise information about their state. Major factor that sums toward a VM profile is its connectivity with other VMs. Any VM that is connected to more quantity of machines is more decisive than the one connected to fewer VMs because the effect of negotiation of a highly connected VM can cause more damage. Also required is the awareness of services running on a VM so as to validate the authenticity of alerts affecting to that VM. An attacker can practice port-scanning program to perform a powerful examination of the network to look for open ports on any VM. All these factors combined will form the VM profile.

III. PROPOSED SYSTEM

To overcome the troubles of existing system, they propose a new approach, namely Cloud Information Accountability (CIA) framework which relies on information accountability. Suggested CIA framework affords end-to-end responsibility in a highly distributed fashion. One of the main inventive features of the CIA framework is to deceit in its competence of sustaining lightweight and authoritative accountability that combines aspects of access control and authentication. Using CIA, data owners can trail not only the service-level agreements are being honoured, but also impose access control rules as needed. 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 regain the logs as needed.

Advantages:

- With the help of Logging modes (Push and Pull) the user will have control over his data at any time.

- They go away from traditional access control in that they provide a certain degree of usage control for the protected data after these are delivered to the receiver.
- They are providing security investigation to prevent the Logging details from the malicious users.

Architecture:

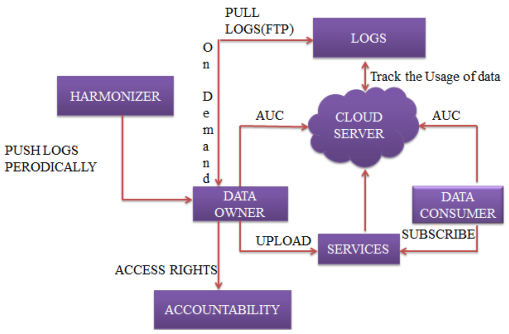

Fig.2 Proposed Architecture

The architecture has various individual functions which don't interrupt the other components or modules. The user can view their corresponding services in the cloud based upon their requirement. They no need to go into the entire process or model for the specific small service.

Functions:

HARMONIZER: It pushes the logs periodically to the data owner without any interruptions. It updates the data correctly to the owner for their references.

ACCOUNTABILITY: It provides the corresponding access rights to the users so that the unnecessary collisions can be avoided. Only the authorized users are allowed to use the particular resources.

LOGS: It acts as similar to the database and they store the information which is necessary for the future reference in case of any occurrence of the flaws. They have various fields which are registered as soon as the consumer utilizes those resources.

3.1 SYSTEM COMPONENTS

There are four components which plays a vital role in performance improvement for providing the quality factor. The flaws can be easily detected owing to the individuality of the project. They are stated as follow

1. DATA OWNER
2. DATA CONSUMER
3. ACCOUNTABILITY
4. LOGS

3.1.1 DATA OWNER

The data owners register in the server which is specifically used for authentication purpose. After their registration they are given a unique username and password for entering into the cloud environment. Here the username is used as the email id on basis of Identity based encryption algorithm. The password is stored in logs as database for future reference or clarifications. There are three modes:

- VIEW
- TIMED
- DOWNLOAD

By using the above three subscriptions the owner can restrict the usage of unauthorized users and also they can avoid the collision by providing the specific services. Certain data has time limit so that the consumers can't view it for more than that limit, they can utilize that data within that particular time.

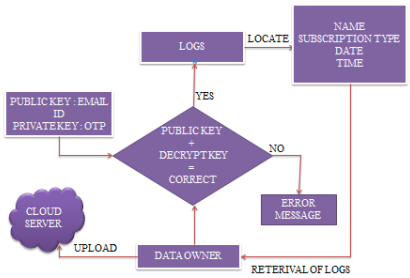

Fig:3 Flow diagram for Data Owner

a) Steps:

1. The data owner uploads the data or services in the cloud for the utilization of consumers by using their corresponding unique id and password.
2. If the data owner wants to retrieve any log details about the consumers they can use their email id as the public key and the private key will be generated by the server on the basis of OTP (One Time Password).
3. The data owner needs both public key and decryption key for retrieving the logs from the database and hence it provides the security through authentication.

   If
   {
   public key and private key is correct
   Then locate the log;

}
Else
{
Error message;
}

4. The log has fields such as name, subscription type, date, time as the record.

3.1.2 DATA CONSUMER

This module deals with consuming the services from the cloud, who are the actual users of the cloud services. The data consumer will utilize the cloud services without any interruptions as it is decentralized so one need not wait for the others to complete. Actions can take place parallel by improving the efficiency by time consumption. They enter into the cloud environment by registering themselves with their corresponding mail id as their unique user id and respective password which are stored in the database for further queries.
The flow of the consumer is posturized below:

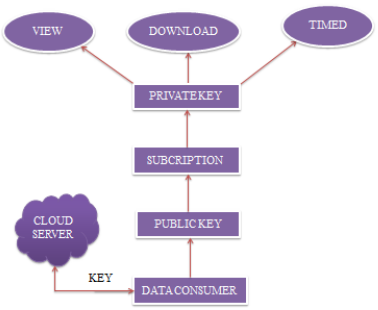

Fig:4 Flow Diagram for Data Consumer

a) Steps:

1. Data Consumer subscribes the services in the cloud by using the public key which is their corresponding email id.
2. Then the private key is generated by the server randomly and it is displayed in the data consumer's area.
3. They utilize the resources by inflowing the valid private key and the particular resources can be accessed by the consumer.
4. The services can be implied in three modes such as view, timed and download.

3.1.3 ACCOUNTABILTY

It is important to clearly define what is meant by 'accountability' as the term is susceptible to a variety of different meanings within and across disciplines. It provides management of the availability and security of the data used, stored, or processed within an organization. Effective privacy protection for PII in some business environments is thus heavily compromised. There are three types of access rights they are

- Read
- Write
- Execute

3.1.4 LOGS

The Logs are the modules which are similar to the database used to store the details about the consumer who consumes the owner's services from the cloud environment. The logs ensure the authentication and confidentiality via verification and validation process. If there is any problem or fault occurs then these logs are used by the owner's for cross checking the details of the users. The logs have various arenas which are used as the component for storing the details of the consumers in the database. There are various types they are as follows:

- Name of the consumer
- Specification type
- Time
- Date

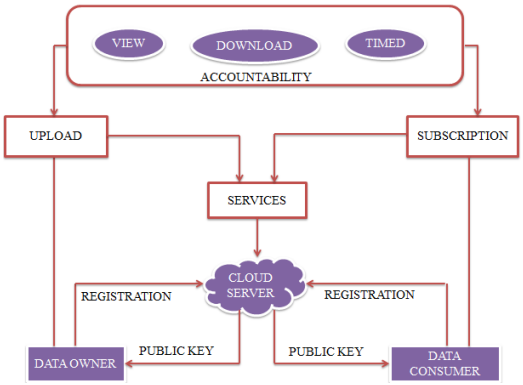

Fig:5 Overall Flow Diagram.

They have three mechanisms based on which the security is somewhat enhanced. They lead to various quality factors such as scalability, reliability etc. They are

- ***IBE(Identity Based Encryption)*:** Used for concealing the information in confidential way. This encryption is very crystal clear to use during secure transactions.
- ***Push:*** For the every periodical time the Cloud Server will send the access details of the user to the data owner.
- ***Pull:*** Data owner has to send the request to the Cloud Server regarding the access details of their data up to the particular time.

IV. CONCLUSION

The main objective of this process is to establish an effective prevention system for providing security through accountability. Zombies can be slightly avoided through the techniques such as providing accountability and secure logs in cloud environment. Here the IBE algorithm provides authentication by using the public key and randomly generated private key so that hackers cannot use the services from cloud without proper authentication. Cloud Computing offers some incredible benefits: unrestricted storage, entree to alleviating rapid processing power and the skill to easily segment and process information.

FUTURE WORK

Future work can be based on the security enhancement in order to provide the effective transmission within the cloud environment. In the first phase an efficient framework is provided for ensuring the accountability and logging through various authentication procedures. In the Second phase more security is provided by transferring the key generated randomly using OTP directly to their respective email id which they have entered in the registration process. By doing this way unauthorized users will not misuse the resources in the cloud. Then by implementing in various platforms the interoperability could be witnessed so that this framework becomes compatible for using various OS.

REFERENCES

[1] 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.

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

[3] 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.

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

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

[6] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008.

[7] C. Wang, K. Ren, and W. Lou, "Towards secure cloud data storage," Proc. of IEEE GLOBECOM'09, submitted on March 2009.

[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Cryptology ePrint Archive, Report 2008/432, 2008.

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," Cryptology ePrint Archive, Report 2009/281, 2009.

[11] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008.

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

[13] A. Pretschner, F. Schuo ¨tz, C. Schaefer, and T. Walter, "Policy Evolution in Distributed Usage Control," Electronic Notes Theoretical Computer Science, vol. 244, pp. 109-123, 2009.

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

[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.