ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

SECURITY IMPROVEMENT AND TRUST ENHANCEMENT IN CLOUD-BASED SERVICES

SHALABH NEGI, JAYANTHI R

School of Computer Science Engineering, VIT University Chennai Campus, Chennai Campus, Chennai, Tamil Nadu, India. Email: asha.s@vit.ac.in

Received: 19 January 2017, Revised and Accepted: 20 February 2017

ABSTRACT

Management of trust is one of the most challenging parts in cloud computing. Cloud service's features such as distributed, dynamic and non-transparent introduces several challenges for availability, privacy, and security. A method is proposed to have trust as a service between cloud service provider and customer by creating a cloud armor. This proposed methodology is used to make cloud server end and customer end system secure of any intrusion to their privacy. In this methodology, we will have a user usage pattern log as ever user has its own unique way of using his/her system; hence, in case if any odd user pattern is being encountered it will automatically block the system and simultaneously shoots a message as well as a call to the user notifying him/her about this unauthorized access. This log is set a various small pattern log, for example, keylog, preferable website visited, and time of accessing the system. Further, we have secured these logs using Rivest-Shamir-Adleman algorithm with very large key size.

Keywords: Cloud computing, Availability, Privacy, Security, Trust as a service, Cloud service provider, Cloud armor, Rivest-Shamir-Adleman, Key size, Geo-tagging.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.20525

INTRODUCTION

We all are well familiar with the vastness of cloud computing, its usage, benefits, ease of use, availability, easy deployment, and adaptability. As we all know nothing is perfect in this world everything has some flaws minor or major but it has some flaws like that only the biggest concern for cloud computing is its security which is preventing it grow at a rate which it deserves because this technology has a potential to bring revolution. Many big companies have already started accepting cloud computing as their key components and started taking benefits through it, but still, some are present who are not ready accept this technology because of its security issues.

Fingers are raised toward the security of cloud computing is due its distributed feature, i.e., data stored in cloud in various regions which are not disclosed to anybody due to privacy but its that our data are being stored in any of the cloud server of cloud service providers (CSP), but the problem is that a user does not know where his/her data are being stored, who is accessing his/her data and other thing is that whether the data that are being uploaded on the cloud by user is genuine or not, i.e., the data are being uploaded by authorized, authenticated user or not, and same with cloud, when a user is downloading data from cloud how should he trust whether data which is being downloaded is being tempered or not. Hence, basically to tackle these kinds of problems we want such a system which is efficient enough to provide authenticity, authorization, and trust so that, relation between customer and CSP can be increased and more people will adapt this technology.

Trust as a service (TAAS) is must for cloud growth so for this we are developing a methodology in which we will create log of user usage pattern of its system which then will be collected on daily bases for some time because it is possible that mood of user is always not same, so might be possible that variations might come which can create problem in our log creation that is why we are creating daily log for certain period. Then, these logs will be filtered so that, data redundancy can be removed from it and a new log having all the compilation of all those log data can be created. Then, a threshold will be created that if someone is successfully able to hack through your network and got access of your system then at that time this system will come under use, it will check usage pattern of hacker and if it fails to matches with usage pattern of owner it will block disconnect system from network, lock the system and an email, message notification will be shot to the owner with a call to bring such malicious activity to owner. If in case user allows that attempt of accessing system, it will allow the access to intruder and will create new log of him and will notify owner when he will access his system and at that time owner has to decide what kind of permission is to be provided to that usage pattern (e.g., Guest, administrative, read, write, execute, all).

System will take log of these key things:

- Keystroke speed and pattern
- Part of screen used
- Shortcuts key usage pattern and frequency
- Websites owner visits and information, he is accessing over net
- List of data that owner access in his system
- Duration of user activity on system
- Types of administrative files he is using.

These are some basic key points on the bases of which log will be created and threshold will be set.

To provide additional security these logs will be secured by large size key Rivest-Shamir-Adleman (RSA) algorithm [1] and those encryption key.

PRESENT WORK AND TECHNIQUES

We all know how important is data for any user so to make that private, isolated from all and secure is first most and prioritized concern of any user unless and until that is being fulfilled trust cannot be achieved; hence, all companies are having gold rush toward mastering this feature to dominate market.

Companies are trying to make their cloud as secure as possible because this is one of those features if it is get mastered that company will dominate this filed in short, we can say that company will have market monopoly.

IP check security

Amazon web services (AWS) by Amazon provides this feature in which we can provide our system IP [2] from which we are going to use those services, which provides security such that person cannot use system unless he is not using that system whose IP is being provided.

Service level agreement (SLA)
It is an official document between the CSP and customer. This document list all key points of services CSP will be providing to customer on bases of these aspects responsibilities, availability, quality, and utmost important security. These services include mean time to repair, recover, between failure and disaster management.

Regulary updating security architecture
Routine and regular updates of vital security architecture. Putting your network under constant vigilance so that, if any unhealthy activity is encountered it can be prevented, i.e. problem can be nipped in the bud.

Using appropriate encryption algorithm
Using appropriate encryption algorithm such as attribute-based signatures [3], RSA. These are some of the old but most powerful encryption technique which is hard to break and thus, widely adopted across globe.

Cloud armor
Cloud consumers credibility assessment and trust management of cloud services [4]. It is a trust management framework based on reputation which provides some set of functionality for delivering TAAS including:

- A protocol for preserving the credibility of trust and preserves users' privacy (Fig. 1).
- Robust and adaptive credibility for measuring trust feedback credibility.

This framework uses zero-knowledge credibility proof protocol for preserving consumers' privacy but also enables trust management system (TMS) to provide credibility.

T-broker
It is brokering scheme of trust-service for many user requests. It is a third-party brokerage architecture for multiple cloud environment; here, T-broker [5] works as a middleware for trust, management, and service matching. It uses a light weight feedback mechanism that can effectively reduce networking risk and improves efficiency of system.

Algebraic manipulation detection (ADM)
ADM [6] is a scheme on which cheater detection and identification technique is based. ADM, m-disjunction presents a code for cheater detection and identification.

Open cloud forensics (OCF) model and FE cloud architecture
Digital forensics helps in investigating cybercrime because of its characteristics, rapid adoption, and flexible qualities. OCF and FE cloud architecture [7] enables effective cloud forensics (Fig. 2).

Hybrid encryption
Hybrid encryption or attribute based hybrid encryption [8] in this system the data confidentiality, fine-grained access control and correctness o delegated computing's results are well guaranteed.

FLAWS IN PRESENT WORK AND TECHNIQUE

We have seen what all are the present working techniques and technology for enhancing TAAS so that, relation between customer and CSP and be enhanced but currently deployed techniques have some faults in them such as:

- The IP check security of AWS has limitation, if we enable this as a service then user is only allowed to access cloud.
- Services from that bonded IP which takes the feature of using cloud services from anywhere any time.
- SLA is just an agreement which always contains some loops whole which can be exploited by user as well as CSP; hence, we cannot fully rely on this methodology for providing TAAS.
- Regular updating security architecture can be a bit hectic a system under surveillance and regular update is a bit burden. It takes extra workforce and resources to carry out this task which can enhance the service charges for customer. Hence, to avoid this kind of thing we want an automated system to carry out this task which is intelligent enough to maintain security easily, cost effectively, and with more efficiently.
- Current algorithm needed to be updated so replacement of their small key size is being done form large key sizes.
- Other and major fault in some of these system is that they are accessing those private information or field of customer which are not to be accessed by a CSP.

A customer will never want someone to access his private data without his knowledge because if it gets transmitted to cloud server and someone can see his data and then try to breach his privacy then it will be a big problem; hence, we need to avoid this type of data sharing of customer to cloud as well as accessibility of this kind of data to anyone for benefit of customer itself.

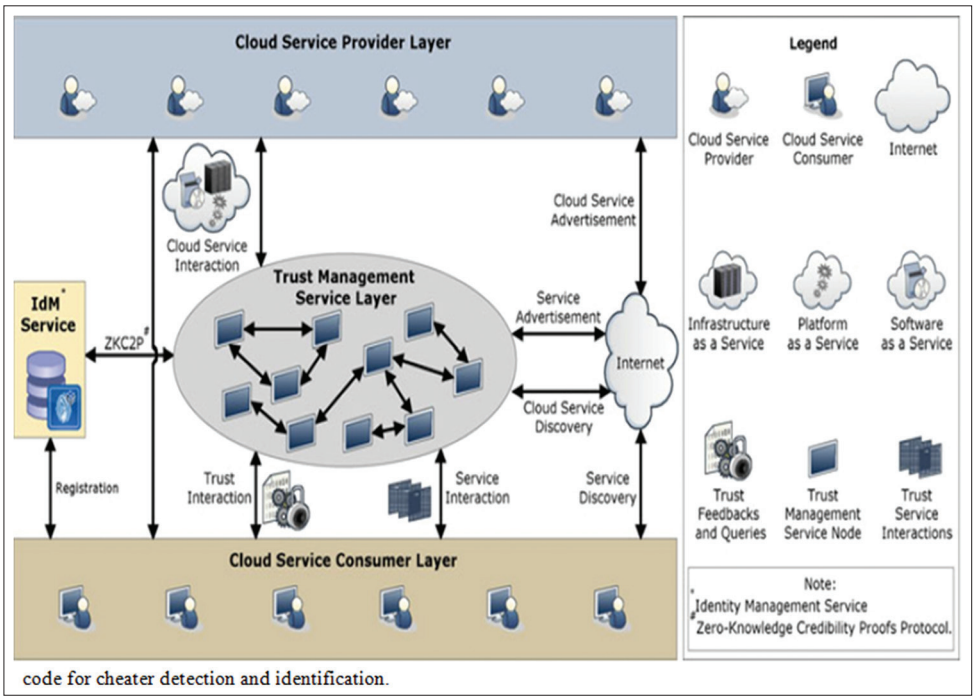

Fig. 1: The architecture of trust management system framework of cloud armor

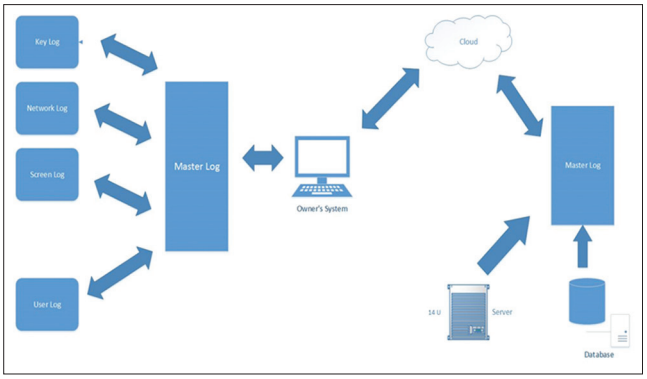

Fig. 2: Architecture of log security

These are some reasons which do not allow to create complete trust based system; therefore, need of new TMS with better efficiency and new methodology which no one has seen before because new technique and technology provide new way of approach for handling the problem which is much better as it removes the faults of existing techniques and technology.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar.

PROPOSED METHODOLOGY AND TECHNIQUE

Pattern log matching in this technique we are going to read user unique usage pattern i.e., how user uses his system, how he interacts with his system. Every user has its own unique way of using his system and utilizing its system to full potential, some use their system to do just light work, for example, such as just creating presentation, maintaining excel sheets, excessing their email, listen to songs, watch movies, and some other user on the other hand have completely different usage approach they use their system for hardcore gaming purpose, high level calculation, programing, designing, song missing, and movie making, such as this every user has its own typing speed, typing format, customization of his desktop, utilities, and on internet websites preferences.
If we are going to see all those services which are unique for a user and we can utilize it for our system, then there are n numbers of thing but some which are important and we implementing in this technique are:

- Keystroke speed and pattern.
- Part of screen used.
- Shortcuts key usage pattern and frequency.
- Websites owner visits and information, he is accessing over net.
- List of data that owner access in his system.
- Duration of user activity on system.
- Types of administrative files he is using.
- How user has customized his system (e.g., kind of wallpaper he puts in background, icons he used if he hides his toolbar, taskbar or no).

These are some basic key points on the bases of which log will be created and threshold will be set.

Explanation how this method will be carried out:

- This technology will create various logs for owner on the bases of above criteria.
- These logs will be not just created for 1 or 2 session but for few weeks because it is possible that user mood might differ during this period as our mood is not same for all days; hence, user pattern can differ when owner is angry, happy, in mood of fun, sad, etc. by taking these much logs we will have good amount of data log to tally. We will filter these logs into a master log so that, it will be compared with another pattern when encountered. In this master log file, we will set a condition in which when user pattern is able to get threshold of 80-85% between master log and new pattern then only access to system will be allowed otherwise system will be disconnected from network, simultaneously system will be blocked and message with email will be shot to owner.
- Only when owner gives permission to access then only other user will be allowed to access the system otherwise he will not be able to access it.
- System then will create a new log of that unknown pattern under guest log so that, in future owner if want to add in his log file he can do that.
- Owner can give different privileges to that log like as guest log he can decide that if in future this guest log is encountered give him permission of read, write, execute only, all of them.

EXPLANATION

Here, we are taking a Linux environment in that taking basic Ubuntu 14.04. There is a file in every system which contains logs by default in Linux it is stored under syslog file.

Command to access those file:

```
nagato@i1:~$ tail-f/var/log/syslog
```

Here, tail command is used to tail the directory and -f is used for follow.

Other shortcut method is to search for default feature of Linux syslog it will show all the log created for that system for this log to store what we can do is to redirect it to a file using this command:

```
nagato@i1:~$ cat|grep/var/log/syslog>logfile.txt
```

This will copy all system log to a text file name logfile here.

For continuous store of log file what we write a script which will maintain and copy all log in individual file.

There are various files in/var directory having many useful log

```
nagato@i1:~$ cd/var
nagato@i1:/var$ ls
backups crash local log metrics run spool
cache lib lock mail opt snap tmp
```

For taking key log we can user keylogger script it will help to take all the data together of keystroke used, speed of typing, etc.

Later, we will secure all these logs using very large size key for RSA so that, this log file will not be easily accessed by any other person.

FEATURES OF THIS TECHNOLOGY

This technology has features which will make it key component of trust enhancement between customer and CSP.

Some key features are:

- It is smart system able to sense variation very quickly thus, having quick response time.
- Intelligent enough to handle scenario according to its variation.
- Owner can leave his system open and go because if anybody tries to access his system without his knowledge it will block system and as well as notify it to owner.
- It can be deployed on cloud, user end and on server end, i.e., admin end.
- In future, this technology can be interfaced with mobile phones, play stations, and hybrid vehicles.

CONCLUSION AND FUTURE APPROACH

This technology is defined to overcome trust issues between customer and CSP which is very important for the growth and complete

acceptance of cloud technology because this technology has all potential to revolutionize IT sector; therefore, keeping that scenario in mind this system is designed. System is still in its initial stages but it has all requirements to come up with all the fault in security of cloud.

Future of this system will be it can be deployed on any interface which is connected to network and are prone to have security breach.

ACKNOWLEDGMENT

The author would like to thank his Research Facilitator Professor Jayanthi R, who supported this vision of author and guided him to go on with this idea. Professor Jayanthi R. saw the potential in this idea and helped author in every possible way guiding him at each and every step.

REFERENCES

1. Huang X, Senrio, Senior Member of IEEE, Wang W, Member IEEE. A Noel and Efficient Design for an RSA Cryptosystem With a Very Large Key Size. IEEE Transaction on Circuits and Systems-II: Express
2. AWS Documentation Provided by Amazon.
3. Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model. IEEE Transaction on Cloud Computing. Vol. 2, No. 4, October-December; 2014.
4. Noor TH, Sheng QZ, Member IEEE, Yao L, Member IEEE, Dustdar S, *et al*. Cloud armor: Supporting reputation-based trust management for cloud services. IEEE Transaction on Parallel and Distributed Systems. Vol. 27, No. 2, February; 2016.
5. Li X, Ma H, Zhou F, Yao W, Member IEEE. T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services. IEEE Transaction on Information Forensics and Security. Vol. 10. No. 7, July; 2015.
6. Wang Z, Karpovsky M, Life Fellow IEEE, Bu L. Design of reliable and secure devices realizing Shamir's secret sharing. IEEE Transaction on Computers. Vol. 65. No. 8, August; 2016.
7. Zawoad S, Hasan R. University of Alabama at Birmingham. Trustworthy Digital Forensics in the Cloud. IEEE Transaction on Computer, March; 2016.
8. Xu J, Wen Q, Li W, Jin Z. Circuit ciphertext-policy attribute-based hybid encryption with verifiable delegation in cloud computing. IEEE Transaction on Parallel and Distributed Systems. Vol. 27. No. 1, January; 2016.