Multi Objective Data Examine Method for Cloud Malware Detection and Data Security

P.Sundari
Assistant Professor, Department of Computer Science, Government Arts College (Autonomous), Coimbatore, Tamil Nadu, India.

V.Vidhya
M.Phil. Scholar, Department of Computer Science, Government Arts College (Autonomous), Coimbatore, Tamil Nadu, India.

Abstract – Software as a Service (SaaS) in cloud infrastructures is highly susceptible to various types of attacks. A common way of launching these attacks is using malware (malicious software). As hardware and software becomes cheaper and more accessible, 'cyber-attacks' are no longer only an action of powerful, sophisticated organizations, but the individual and their personal computer. Consequently the demand for cyber security is increasing significantly and remains high on the priority list for governments worldwide. With the popularity of cloud, the mobile device is becoming a very lucrative target and enterprises need to anticipate an increasing number of malware targeted at intercepting valuable financial information. The need for security is in fact a response to the increasing number of attacks led against SaaS systems. There is an urgent need to develop effective improvement mechanisms. The proposed system performs the Signature and behavior based consistency check for malware detection technique.

Index Terms – Cloud computing, Data security, Integrity verification, Public auditing, Privacy. Malware detection, Signature schemes, SAAS.

1. INTRODUCTION

Cloud computing security[2][9] defines the set of control based techniques and policies designed to follow regulatory compliance rules and to protect information, data applications and infrastructures associated with the usage of cloud computing services. The number of personal cloud users increases each year and it is not about to slow down. As the data over cloud is stored in a distributed manner, the process of protection to it is in need to a great extent. Most of the security issues occur during the process of data transfer, especially, when the total data resides at the cloud environment. The current adoption of cloud services includes numerous challenges as the users were influenced by the authenticity factors.

Based on the survey conducted by IDC security, costing model, charging model, Service Level Agreement, data migration and cloud interoperability issues were found to be the major security challenges of cloud computing. As large number of organizations move towards cloud computing techniques, some of the potential attacks [4] like Denial of Service Attacks Side, Channel Attacks and Authentication Attacks, Man in the Middle Attacks, Cryptographic Attacks and Insider Attacks [6] have become prevalent among the cloud data users. There exist several methods and techniques, which prevents the security breaches over cloud services. Some of the widely accepted security preservation techniques are discussed in the paper. The work analyses the static features extracted from files and applies Malware Detection Techniques for classifying them as benign or malware.

2. PROBLEM DEFINITION

The cloud data security is widely used by many researches [13][10]. But only few approaches were concentrated on the malware detection on cloud services. The malware is the malicious code inserted into the outsourced software. This kind of security check and malware detection is complicated in the hybrid cloud environment. The cloud data integrity [5] and dynamics checking creates the following problems [12]. The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages. Recently an Inttest [3] mechanism is proposed to perform the consistency analysis in the cloud [1].

- Data integrity verification to be performed with the privacy rules.
- It should verify and report to the data owner with the proof of verification.
- The verification report should be re-identified.
- The consistency analysis should perform with all the cloud service providers.
- The attacker pinpointing mechanisms are not studied well with the cloud malware detection.

The cloud outsourced software's can be hold by several cloud service providers. The malicious cloud service provider can change the results of the software by injecting the malicious code. The earlier works on malware detection either used signature schemes or behavior based [11] [14]. There is a need for better approach with the signature and behavior analysis with ability to track the verification report using special attestation schemes. These problems are studied in the proposed system.

3. PROPOSED SYSTEM

The proposed system designed and developed a new malware detection framework for cloud software services. Currently, the Cloud Services Providers are providing vast and different types of online services that include SaaS as a major service. The proposed framework consists of different techniques and methods to achieve the malware detection. The followings are the contributions of the proposed system.

3.1 Contributions of the Proposed System

A new malware detection and data security framework is designed and named as Multi Objective Data Examine (MODE).

The proposed system performs the Signature and behavior based consistency check for malware detection technique. This certainly utilizes the following techniques to detect the malware in the cloud.

a) Pattern Matching Techniques: The Pattern Matching Technique performs the Signature Verification and Malware Pattern Verification. It has been enhanced to support for the cloud SaaS. The software results are verified with the other service provider's results.

b) Event Mining Algorithm: The next process of malware detection is the event mining process in the cloud service. It detects the events in the cloud storage and finds the anomaly and malware patterns.

The proposed system performs the malware detection with the attacker Pinpoint Mechanism, which helps in detecting the Malicious Service Provider in the cloud.

The verified malware reports are attested for the further process using ElGamal signature algorithm.

3.2 DETECTION PROCESS

The system performs the following process in detection process. Integrated analysis for the data freshness is tested by data users. Data over both consistency and inconsistency is verified for the data recovery. Verification algorithm is used to pinpoint colluding attackers more efficiently than the existing system.

Integrated Evidence Scheme:

- Consistency data analysis
- Inconsistency data analysis
- Combining consistency and inconsistency data analysis results.

ATTACK PINPOINT

The system performs the evidence and pinpoints the attacker. The data owner can view the total audit [6], evidence and auto correction report. The report contains all pinpointed attacker nodes and autocorrected data and its attested user details.

AUTO CORRECTION FOR DATA RECOVERY

Auto correction is done by using cache data. The need of auto correction is to give a valid and original to the cloud data users or subscribers. The falsification can be done by users or cloud providers of the data. In order to avoid the corrupted data delivery the auto correction algorithm is proposed and implemented.

EVIDENCE USING ECDSA

The evidence using ECDSA is handled in this module. The evidence is performed whenever the auto correction is performed by the data users. The malicious attacker is been pinpointed and the malicious data content or packet is replaced with the original data content or packet. The autocorrected authentication will be attested on the packet header.

DDA (DYNAMIC DATA AUDIT) ALGORITHM STEPS:

1: A software service details arrives at integrity verification locale

2: Get software name of owner m

3: Get the id of CSP R

4: Let n be the malicious file of owner m

5: Read every data and match the message with the original

6: If the data match with the malicious behavior of users and DDA (Dynamic Data Audit) results then do step 7

7: Let Xn = 1 if message is corrupted, Xn = 0 otherwise

8: if (Xn == 1) then

7: find the error location and store Cs

9: if (CS>threshold) then store the data in corrupted list- set evidence

10: else normal data

11: end if

12: Check corrupted and good data list which denoted as Cd and Gd respectively

13: if ($m==Cd_m$) then

14: data m is corrupted. data recovery processm.

15: else if (m==Cd_m) and Xn = 0 then

16: data m is normal. Test is reset for m.

17: else if (m==Gd_m) and Xn = 1 then

18: Test continues with new observations

19: else

20: end if

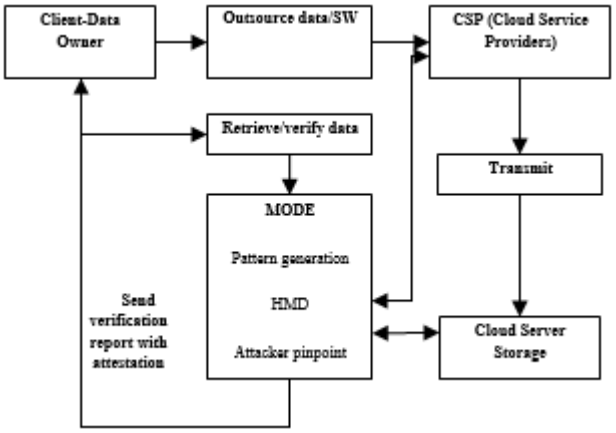

Fig 1 The overall process involved with the Proposed System

The proposed work implements the DDA (Dynamic Data Audit) scheme for effective malware detection in cloud data, which helps to detect malware, service integrity attack and to pinpoint malicious service providers in the cloud interface. The proposed DDA provides the malicious attack detection and result auto correction to scheme which helps to automatically correct compromised results to improve the result quality.

4. IMPLEMENTATION AND RESULTS

The system has constructed with the cloud SAAS based approach. The server has the monitoring and authentication criteria providing processes. In the proposed system, a client node sends out a request message to server to access the software. The server will receive all details of the client and verifies the software for malware issues.

The system presents two methods to monitor and secure the software from malwares. An important characteristic of client authentication and software verification criteria is that the amount of computation needed to resolve it can be estimated fairly well.

Note that the authentication criteria used in the defense against cloud malware need not require naturally sequential operations. It is important that a data cannot be accessed by anyone until a pre-determined authentication is solved.

The following results show the overall comparison with the existing system such as IntTest. The chart shows that the proposed system is more reliable and efficient than the existing system.

Type	IntTest	MODE
Malware Detection Accuracy	92	97
Time Efficiency	90	98
Signature Cost Efficiency	91	97

Table 1 Analysis with the Existing System

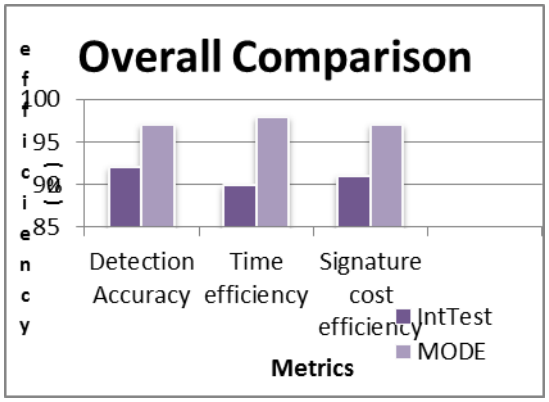

Fig 2 Comparisons between IntTest and MODE Techniques

5. CONCLUSION

With the tremendous availability of cloud provider, reliability and security issues is one of the important and challenging tasks in cloud environment. For this here present the design and implementation of MODE with effective HMD mechanism, this is a novel integrated service integrity attestation framework for software-as-a-service cloud systems. MODE employs an effective signature scheme with HMD and attestation mechanism. This effectively prevents the data from malicious attacks. This is successfully implemented using .Net platform and the results and outputs are satisfactory. In future the proposed MODE can be expanded in the dynamic nature, where the revocation can be expanded into the on demand revocation system. Changing the algorithms and techniques for the on demand revocation will be done in the future. There are still so many issues to be explored. Opportunities are enough in this arena for some groundbreaking contribution and bring significant development in the industry. Here the use of MODE is tested on a commercial data stream processing platform

running inside a production virtualized cloud computing infrastructure.

REFERENCES

[1] Alvaro, Peter, Neil Conway, Joseph M. Hellerstein, and William R. Marczak. "Consistency Analysis in Bloom: a CALM and Collected Approach." In *CIDR*, pp. 249-260. 2011.

[2] Conway, Gerry. "Introduction to Cloud Computing." (2011).

[3] Du, Juan, et al. "Scalable distributed service integrity attestation for Software-as-a-Service clouds." *IEEE Transactions on parallel and distributed systems* 25.3 (2014): 730-739.

[4] Gruschka, Nils, and Meiko Jensen. "Attack surfaces: A taxonomy for attacks on cloud services." *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*. IEEE, 2010.

[5] Hongwei, Peng Zhang, and Jun Liu. "Public data integrity verification for secure cloud storage." *Journal of networks* 8.2 (2013): 373-380.

[6] Kandias, Miltiadis, Nikos Virvilis, and Dimitris Gritzalis. "The insider threat in cloud computing." *International Workshop on Critical Information Infrastructures Security*. Springer, Berlin, Heidelberg, 2011.

[7] Liu, Chang, et al. "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates." *Parallel and Distributed Systems, IEEE Transactions on* 25.9 (2014): 2234-2244.

[8] Liu, Qin, Guojun Wang, and Jie Wu. "Consistency as a Service: Auditing Cloud Consistency." *Network and Service Management, IEEE Transactions on* 11.1 (2014): 25-35.

[9] Luo, Jun-Zhou, et al. "Cloud computing: architecture and key technologies."*Journal of China Institute of Communications* 32.7 (2011): 3-21.

[10] Wang, Boyang, Baochun Li, and Hui Li. "Oruta: Privacy-preserving public auditing for shared data in the cloud." *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*. IEEE, 2012.

[11] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." *Computers, IEEE Transactions on* 62.2 (2013): 362-375.

[12] Wang, Qian, et al. "Enabling public auditability and data dynamics for storage security in cloud computing." *Parallel and Distributed Systems, IEEE Transactions on* 22.5 (2011): 847-859.

[13] Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." *Parallel and Distributed Systems, IEEE Transactions on* 24.9 (2013): 1717-1726.

[14] Zhu, Yan, et al. "Dynamic audit services for outsourced storages in clouds."*Services Computing, IEEE Transactions on* 6.2 (2013): 227-238.