Received 05 March 2021; Accepted 01 April 2021.

CS2M: Cloud Security and SLA Management

VipulChudasama
Computer Science & Engineering,Nirma University,Ahmedabad, 382470,
Email: Vipul.chudasma@nirmauni.ac.in

AkshayMewada
Computer Science & Engineering,Nirma University,Ahmedabad, 382470
Email: Akshay.mewada jrf@nirmauni.ac.in

Vivek Kumar Prasad
Computer Science & Engineering,Nirma University,Ahmedabad, 382470

Aheesh Shah
Computer Science & Engineering,Nirma University,Ahmedabad, 382470

MadhuriBhavasar
Computer Science & Engineering,Nirma University,Ahmedabad, 382470

Email: Vivek.prasad@nirmauni.ac.in Email: Asheesh.shah@gmail.com Email:
Madhuri.bhavsar@nirmauni.ac.in

I. ABSTRACT

With the support of a vast amount of virtual storage, cloud computing (CC) delivers on-demand services over the Internet. The key characteristics of cloud computing are that no costly computing infrastructure is established by the customer and the cost of its services is lower. Cloud data protection is important to make sure that your data is secure. So the cloud service provider must be aware of the latest malware cases that allegedly occurred in the Cloud ecosystem. This paper addressed the fundamental characteristics of cloud computing, security challenges, threats, and their solutions. The study also highlights many key cloud-related subjects, namely the structure for cloud infrastructure, operation, cloud security principles, threats, and attacks. The techniques that we have used here are SLA management using RALLY for open stack private Cloud and the malware analysis has been identified using open source virus total repository. The results identified during the experiments reflect that our proposed scheme, "CS2M: Cloud Security and SLA management" performs faster as compared to the conventional techniques. Keywords: Cloud Computing, Security, Protection, SLA Management, Malware detection

II. INTRODUCTION

Cloud computing is providing a range of approaches in a secure view [6]. Although this point in time cloud features is very well known, particularly from a business perspective. But this feature contains certain security flaws that are still a problem in the cloud community. Day-by-day cloud computing is on the rise as many companies have embraced cloud technology, but many security concerns are faced in parallel [2]. Each enterprise selects a security solution when it transfers its information to remote regions. Thus according to NIST stability, interoperability and portability constitute a major barrier to cloud computing adoption. To achieve multi-tenancy, the cloud utilized the virtual environment [1]. The virtual computer includes vulnerabilities that pose an explicit challenge to the protection and privacy of cloud services. The other element in cloud computing is data migration over the Web. There are several security vulnerabilities in the API browser and the network channel. Via a multi-tenancy concept, cloud services are distributed and accessed by many users. This principle is an obstacle to creating a safety framework that protects data and services fully. Due to transparency concerns, the cloud service provider resists its users to incorporate security monitoring or intrusion detection systems in the service layer at the back of the virtualized cloud ecosystem [7].

In order to achieve a high degree of privacy and security of relevant data and services, cloud service providers are creating a Service Level Agreement (SLA) for cloud users. Unfortunately, however, there is no common method or standard procedure for the construction of an SLA [3]. From the latest literature review, we identified that we require ht security in the various levels of the cloud ecosystems. These are security at the server access level, security at the internet access level, database access level, security in data privacy, and secured program access [5]. Investigation of unauthorized or illegal acts in cloud computing can be impractical. Cloud platforms are extremely difficult to examine, since logging and data for several users may be co-located and distributed through an ever-changing range of hosts and data centers. Cloud data is usually shared in an environment alongside data from other customers. Encryption is safe, but it’s not a cure. The cloud provider should provide proof that the encryption systems have been developed and checked by trained specialists [4].

A. Motivation

Cloud security is essential to both business and personal users. Businesses have legal responsibilities in protecting clients’ information and other details. Despite the benefits of CC, the transition of local computing into remote computing has introduced several security issues and challenges to both users and providers. Hence some mechanisms are needed to address such issues seamlessly.

B. Contribution

The contribution of this research paper is to detect malware detection and analyzing malicious files. The manage-ment of the Service Level Agreement. The mechanism discussed here will proactively identify the degradation in the performance of the system. The paper also includes a detailed discussion of cloud security risks, the intrusion, and its remedies.

C. Organization

The rest of the research paper is categorized as follows. Section II discussed the problem formulation and system model, which mentions how to formulate the problems identified during the literature review and its resultant system model. Section III is performance evaluation, where the experimentation’s have been carried out using a private cloud setup, its evaluations, and comparative analysis are explored.

III. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

Figure 1 depicts the working of the proposed model called CS2M. The Model describes the SLA negotiation process between the end-user and the cloud service provider. This starts with the contract between these two. Then, when the end-user gives importance to the security of the data, which is managed by the cloud. The Cloud provides the security w.r.t to the malware detection through the service developer. The steps that are followed in the said model are described below:-

1) This consists of the two steps procedure (a) whether the security concepts are carried out in the SLA (Type A), if this is not carried out then follow the step/request type B. In Type B the cloud user will ask for the security (malware detection) to the CSP. The CSP then transfer the said request to the service developer.
2) The service developer will fetch the security details from the end-users.
3) The service developer derives the security designs from 3A and derives its policies from 3B.
4) The derived policies and design will be incorporated into the Cloud system model.
5) The finalize design and policy will be in synchronize with the service model.

At last, secure services will be offered to the end-users. Figure 2 describes the flowchart for the same.The algorithm 1 shows the procedure to be followed for acquiring the services from the service manager. Algorithm 2 describes the detailed description of the malware analysis for the infected files.In Algorithm 2 the output states are classified as IDEAL, WARNING, CRITICAL. The IDEAL condition means the data are safe and it is working in their normal ways. WARNING means the attack effects are in their inception state and the CRITICAL means the attack has a major impact on the utility of the cloud resources.

B. Problem Formulation and its solution statements

The Booting time is considered here to see the performance of the VM and is generated through the NOVA services of open stack rally. The booting time acts as a metric here. If the Booting time is not matching with the ideal scenario, then the model switches to the malware analysis process. In which the process ID and hash values will be generated from the VIRUS TOTAL Repository. If the state of the file is infected, then we generate the process list of the infected file and terminate that particular process from the VMs.

IV. PERFORMANCE EVALUATION

A. Simulation Results

The simulation results are carried out in a private open stack cloud. The parameters such as Full duration, load duration, and the average booting time of virtual machines are generated from the RALLY software tool. The RALLY gives the success rate of the running services in the cloud. Figure 1 depicts the relation between the average booting time of the VMs, load duration (Time from the first iteration start to last iteration end) of the VMs, and the full duration (This time includes iterations time (Load duration) plus the time taken by another action related to the task, mostly Contexts execution time) of the VMs.This figure also mentions the malware attack duration during the

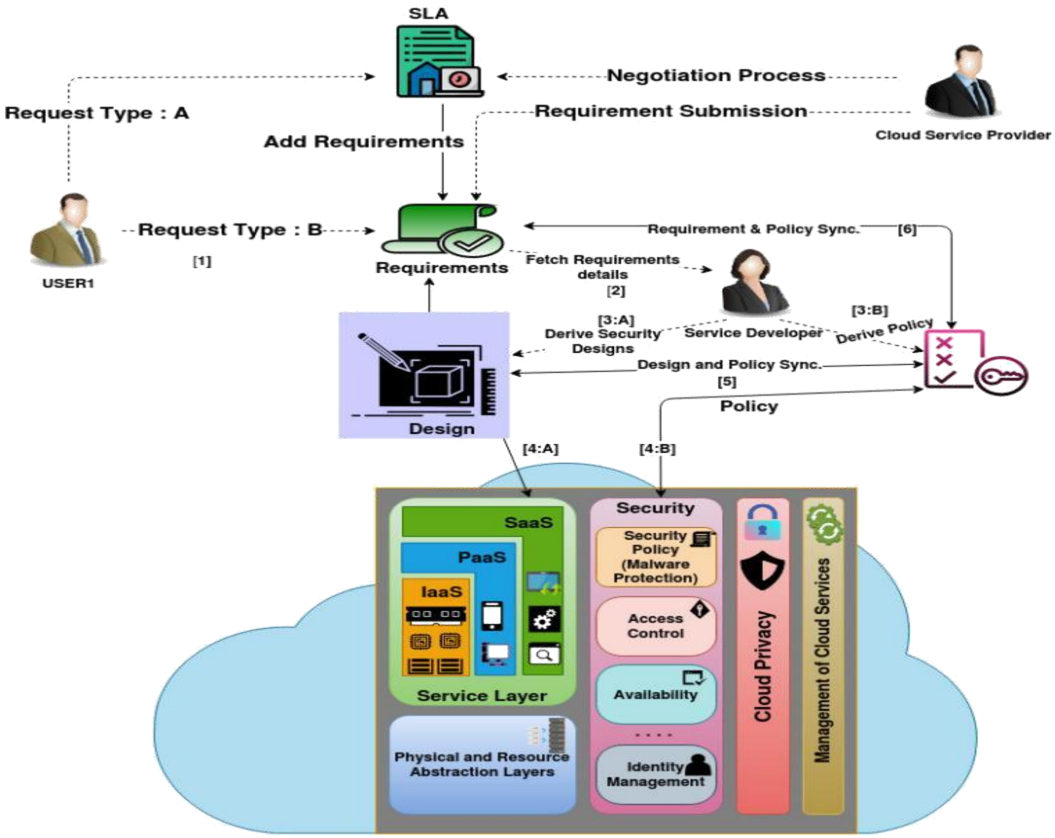


Fig. 1: CS2M model diagram

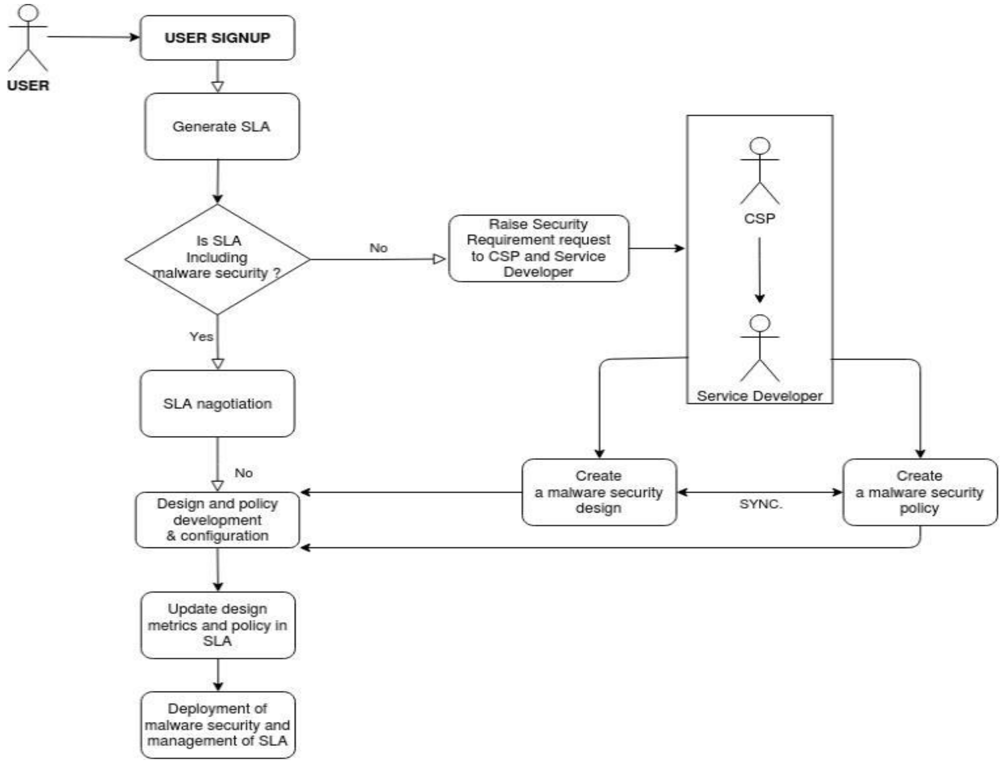

USER
USER SIGNUP
Generate SLA
Is SLA Including malware security ?
No
Raise Security Requirement request to CSP and Service Developer
CSP
Service Developer
Yes
SLA nagotiation
No
Design and policy development & configuration
Create a malware security design
SYNC.
Create a malware security policy
Update design metrics and policy in SLA
Deployment of malware security and management of SLA

Fig. 2: Flowchart of the proposed CS2M model

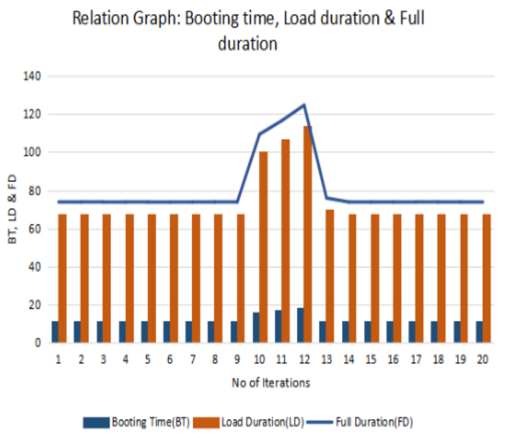
Algorithm 1 CS2M Service Adoption Algorithm

```
    Input : Malware Service Request : $< T_1, R_1 >$
    Output : Malware Security Deployment : $S_1$
procedure MALSECREQUEST($< T_1, R_1 >$)
    Searching the malware service adoption
    if ($< T_1, R_1 >== Available$) then
        $DoNothing$
        $Generate\ Token\ T_1 for R_1$
        $Allocate\ (T_1, R_1) \rightarrow CSP$
        $Transfer\ Request(T_1, R_1) \rightarrow DS$
    end if
    while $((T_1, R_1)\ != Null)$ do
        $Initialize\ [Design(D_1), Policy(P_1)]$
        $Configure:\ (D_1, P_1)$
        if $Configuration\ == Successful$ then
            $Deploy\ (D_1, P_1)$
            $Update(D_1, P_1) \rightarrow SLA$
        end if
    end while
end procedure
```

Received 05 March 2021; Accepted 01 April 2021.

Algorithm 2 CS2M Service Adoption Algorithm

```
    Input :Average Booting time,Process list (10 VMs):
$T_b = [T_{b1}, T_{b2}, T_{b3}, ......T_{b10}]$ and
$P_l = [P_{l1}, P_{l2}, P_{l3}, .....P_{ln}]$
    Output : States : IDLE, WARNING, CRITICAL
1:  procedure MALWDETECT($T_b$, $P_l$)
2:    Checking the Status of the Nova Services
3:      while $(Nova.Service == Available)$ do
4:        Initialization of $T_c = 0$
5:        if $(T_c <= T_b)$ then
6:          $State \rightarrow IDLE$
7:        else if $(T_c > T_b$ and $T_c < T_b + 1.00)$ then
8:          $State \rightarrow WARNING$
9:        else
10:         $State \rightarrow CRITICAL$
11:         $Deployment\ of\ Malware\ Service$
12:         $Fetch\ (Process\ List\ p_{list} = [P_1, P_2, ..., P_n] \rightarrow TaskManager)$
13:         $Fetch\ Values\ V\ =\ [V_{md5}, V_{sha1}, V_{sha256}, V_{resource}]$
14:       end if
15:       if $(< P_{list}, V_{md5} >== Positive)$ then
16:         $Set\ Flag \rightarrow Infected$
17:         $Initialize\ List_{Infected} = [\,]$
18:         $Terminate\ \&\ Delete\ Infetced\ Process$
19:       else
20:         $Goto \rightarrow Step2$
21:       end if
22:     end while
23: end procedure
```



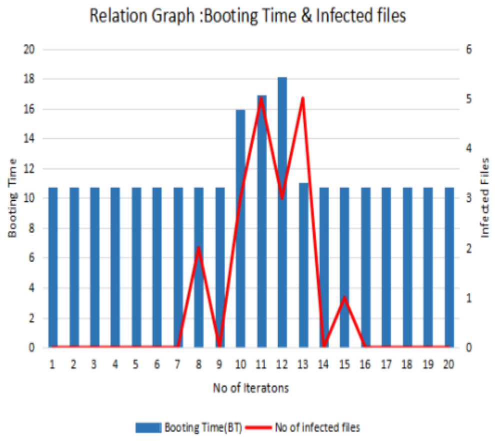


Fig. 3: Relation between Booting time, Load duration and Fig. 4: Relation between Booting time and infected
files

Full duration.

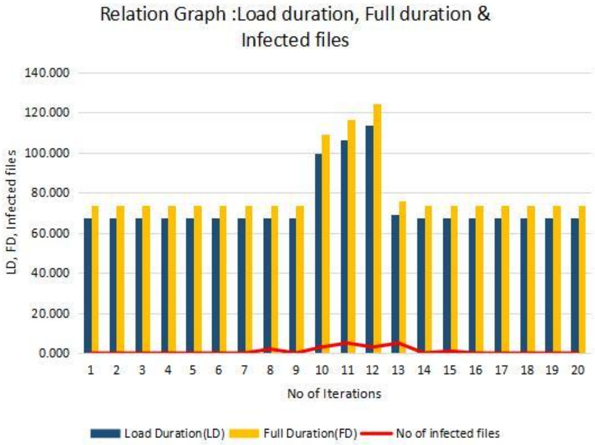


Fig. 5: Relation between Load Duration, Full Duration and infected files

9 to 13 iteration. Figure 4 describes with an increase of the booting time and this leads to the CRITICAL state. Our cS2M model identifies the malicious file in the mentioned iterations. The malware files were detected through the virus total APIs scheme through the MD5, SHA1, SHA256 parameters. Figure 5 shows the relationship between the full duration, load duration, and infected files, where we can observe that when malware happens, then the ideal execution time increases concerning several malicious or infected files.

V. CONCLUSION

Under the cloud model, the security issue becomes more complex as new dimensions have approached the problem field of model architecture, such as elasticity multi-tenancy, and layer dependence stack. This paper provides a thorough review of the topic of cloud security. We looked at the issue from a cloud design perspective, the offered features perspective, cloud stakeholders perspective, and cloud computing service frameworks point of view. Based on this analysis, we derive a thorough overview of the cloud security issue and areas where a potential security solution can target.

VI. ACKNOWLEDGEMENT

The research paper is a part of the project approved under DST (Department of Science and Technology), Government of India, New Delhi.We thanks DST for funding the project.

References

[1] SattarFeizollahibarough and MehrdadAshtiani. “A security-aware virtual machine placement in the cloud using hesitant fuzzy decision-making processes”. In: The Journal of Supercomputing (2020), pp. 1–31.

[2] Puneet Jai Kaur and SakshiKaushal. “Security concerns in cloud computing”. In: international conference on high performance architecture and grid computing. Springer. 2011, pp. 103–112.

[3] Xiaochen Liu et al. “A behavior-aware SLA-based framework for guaranteeing the security conformance of cloud service”. In: Frontiers of Computer Science 14.6 (2020), pp. 1–17.

[4] AkshayMewada et al. “Establishing Trust in the Cloud Using Machine Learning Methods”. In: Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019). Springer. 2020, pp. 791–805.

[5] Vivek Kumar Prasad and Madhuri D Bhavsar. “Monitoring IaaS Cloud for Healthcare Systems: HealthcareInformation Management and Cloud Resources Utilization”. In: International Journal of E-Health and Medical Communications (IJEHMC) 11.3 (2020), pp. 54–70.

[6] Vivek Kumar Prasad and Madhuri D Bhavsar. “SLAMMP Framework for Cloud Resource Management and Its Impact on Healthcare Computational Techniques”. In: International Journal of E-Health and Medical Communications (IJEHMC) 12.2 (2021), pp. 1–31.

[7] Inderbir Kaur Sandhu, Manisha Malhotra, and PraneetRangi Randhawa. “A Review of Trust and Security Concerns in Cloud Computing Adoption Intention in the Higher Education Sector: Research in Progress”. In: Impacts and Challenges of Cloud Business Intelligence (2021), pp. 1–12.