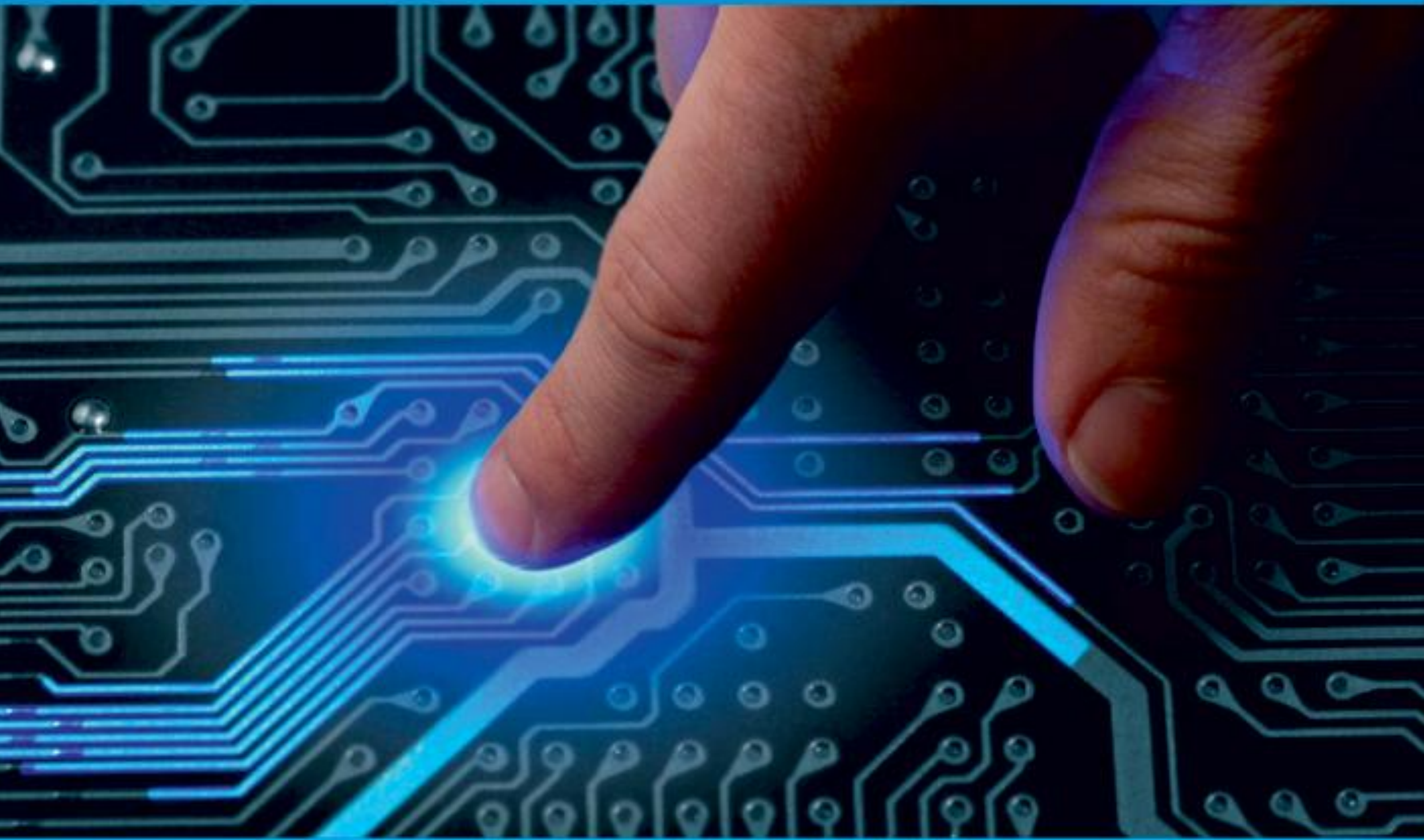
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.542

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906113 |

SAAS Attack and Prevention Using Machine Learning in Cloud Environment: A Survey

Anant Nanasaheb Deore[1], Gaurav Namdev Pingale[2], Shubham Bharat Hazare[3], Pradeep Raju Shinde[4], Prof. Radha Shirbhate[5]

UG Student, JSPM's Bhivarabai Sawant Institute of Technology & Rsearch Wagholi, Pune, Maharashtra, India[1,2,3,4]

Assistant Professor, JSPM's Bhivarabai Sawant Institute of Technology & Rsearch Wagholi, Pune, Maharashtra, India[5]

ABSTRACT: Software-as-a-service (SaaS) is a type of software service delivery model which encompasses a extensive range of business opportunities and challenges. Users and service providers are unenthusiastic to integrate their business into SaaS due to its security concerns while at the same time they are attracted by its benefits. This article highlights SaaS utility and applicability in different environments like cloud computing, mobile cloud computing, software defined networking and Internet of things. It then embarks on the analysis of SaaS security challenges spanning across data security, application security and SaaS deployment security, possible solutions or techniques which can be applied in tandem are presented for a secure SaaS platform. This research to identify the malicious activity in cloud base Software as Service (SaaS) environment. Besides investigating crimes related to the cloud environment in forensically sound manner, the process of performing cybercrime investigation in the cloud environment is known as cloud forensics. This process is facing complex challenges due to the dynamic nature of cloud computing. It also address a cloud forensic strategy is proposed for assisting digital investigators and experts for investigation of cybercrimes in effective and efficient manner. The proposed strategy is based on cloud computing platform that providing enormous processing and storage capabilities. This strategy can be as guided to the digital investigators and practitioners to follow it in performing of investigation of SaaS attacks

I.INTRODUCTION

Cloud computing has become a part of the competitive market today. Many organizations utilize cloud administrations. Despite the fact that distributed computing administrations is developing and picking up notoriety, the dread about the utilization of cloud administrations is as yet an open issue. Different issues hindering appropriation are distinguished in the writing; one of the real ones is security. Security hazards in the territory of distributed computing has stood out since its start. New conventions and apparatuses are consistently sought after to improve the security quality of a distributed computing administration or specialist organization

Different distributed computing specialist co-ops are accessible with their administrations in the cloud condition. These administrations join different determinations, highlights and techniques for accomplishing security. A few administrations center around secure access to an administration and information by encryption, and some are concentrating on secure system itself. Procedures received by different suppliers to accomplish security are of shifting nature. A cloud client may look for an administration dependent on his necessity and level of security given by an administration. To dissect a specific administration dependent on its different security properties is a test. The real test is to believe a cloud administration or specialist organization as far as security. One can endeavor to show such „confidence" in a cloud administration, as a sort of trust esteem. This theory investigates the likelihood of structure such a framework for trust computation, and its various aspects.

II.PROBLEM STATEMENT

Few days ago, there was an incident where one person's VM was deleted by his own friend. Assume both persons as Jack and John respectively. John purchased some amount of cloud space and became CSP himself. Now Jack was in need to get cloud platform to host his mail exchange server. On the request of jack, his friend John hosted server on cloud. Jack started growing good with his business and John due to greedy intentions thought to take over his business. So John somehow was successful in hacking Jack's system and sent a mail requesting to delete his VM and deleted the VM too.

Now when investigation was held and investigator asked John to give access to logs saying that he was requested through a mail by Jack to do so. Thus the situation arises where to perform the forensic investigation and without the data evidences it is not at all possible to proceed further. And it we file a case against the criminal it would be a very long process that we cannot even imagine sometime.

Therefore, we are looking forward for a mechanism which would provide a two factor authentication by either CSP or any third party provider before deletion of any VM. This would prevent the unauthorized deletion of VM on cloud.

III.OBJECTIVES

The objectives of this research work include the following:

- Explore the challenges and requirements of forensics in the virtualized environment of cloud computing
- To detect the runtime SAAS attack on cloud environment.
- Implement a system with three different modules like IDS, IPS and IRS as well.
- Design a digital forensic framework for the cloud computing systems from the view point of investigator and/or cloud architecture
- Address the issues of dead/live forensic analysis within/outside the virtual machine that runs in a cloud environment

IV.OUR CONTRIBUTION

Cloud computing has completely changed the way the digital data is stored, transmitted and processed. With such a paradigm shift from desktop systems to network of servers geographically located, many technological and legal challenges may be encountered when we intend to perform digital forensics in different types of cloud platforms. In the past few years, many researchers have contributed in identifying the forensic challenges, designing forensic frameworks and data acquisition methods for cloud computing systems. Though all these works identify the technical /organizational /legal challenges of cloud forensic analysis, no concrete solutions have been proposed to address the challenges of applying forensics to the cloud environment in general that is acceptable to the forensic investigator or LEAs (Law Enforcement Agencies) of this digital space. The related research done so far is all about studying the issues in the cloud forensic arena, except for some specific contributions like FROST (Digital Forensic Tools for the OpenStack Cloud Computing Platform) [56]. Therefore there is a real requirement to undertake forensic research in cloud on a large scale. The major challenges of cloud forensics originate from the very characteristics with which the cloud computing platform is identified.

PROJECT FEATURES

1. Absence of uniform standards and protocols- This leads to technical difficulties in forensic data collection and analysis
2. Investigation in virtualized environment is a real challenge- as virtualization is a key technology used to implement cloud services
3. Multi-tenancy and multi jurisdiction- which result in legal concerns with respect to cloud forensics
4. Evidence segregation is a big issue- due to the “resource pooling” characteristic of the cloud
5. Partial forensic examination- Absence of tools for pre-processing of virtual disks and memory to help in completing the investigation process
6. Absence of digital forensic triage in cloud data analysis- use of parallel processing techniques to index virtual disk data to speed up investigation process
7. Interoperability between cloud providers- no interoperability as such between cloud providers
8. Lack of transparency- the operational details of cloud data centers are not transparent enough to cloud investigators
9. Maintaining chain of custody- due to the multi-layered and distributed architecture of cloud, the chain of custody of data may be difficult to verify
10. Loss of data control- cloud user or investigator will have little or no control (or knowledge) over the physical locations of the digital evidence
11. Virtual machine data is not persistent- if a virtual machine is terminated, there is no procedure available for recovering its data
12. Identification of evidence- sources of evidence pertain to different cloud platforms and hence no unique method for identification
13. Live forensics- Live data acquisition will have data integrity or preservation problem

V. SCOPE OF WORK

Cloud computing is maturing and continues to be the latest, most hyped concept in information technology industry. Cloud computing evokes different perceptions in different people. These developments may create problems to law enforcement agencies (LEA) throughout the world who are actively involved in cyber crime investigation especially in cloud. The work "A Novel Digital Forensic Framework for Cloud Computing Environment", would help an investigator or the Cloud Service Provider to get an overall idea of performing digital forensic investigation in cloud computing environment. The digital forensic methods that are suggested in this research can scale to cloud data for handling the analysis of the cloud crimes. The proposed methods of the partial analysis would help the forensic investigator in minimizing the overall processing time of a cloud crime under investigation. The digital forensic research community which is actively involved in the designing and development of the cyber forensic tools for cloud computing systems could consider the cloud forensic architecture presented in this work as a reference model. In brief, the work presented as part of this report can be a way forward to combat cyber crimes in cloud computing systems.

HARDWARE RESOURCES REQUIRED

- Processor : Pentium iv 2.6 GHz
- Ram : 512 mb dd ram
- Monitor : 15 color
- Hard Disk : 20 gb
- Floppy Drive : 1.44 mb
- CD Drive : lg 52x
- Keyboard : standard 102 keys
- Mouse : 3 buttons

SOFTWARE RESOURCES REQUIRED

Operating system	: Windows 7 Ultimate.
Coding Language	: Java / J2EE
Front-End	: Swing
Data Base/Back End	: HDD Drive
Cloud Service : Amazon EC2 as public cloud	

REFERENCES

[1] Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari "Providing Security and Integrity for Data Stored In Cloud Storage" ICICES, 2014.

[2] "Agentless backup is not a myth," 2011.

[3] NIST, "NIST Cloud Computing Forensic Science Challenges", National Institute of Standards and Technology Interagency or Internal Report 8006, 2014.

[4] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky "Scenario-based Design for a Cloud Forensics Portal" IEEE, 2015.

[5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.

[6] M. Jensen, N. Gruschka, and R. Herkenhoner,¨ "A survey of attacks on web services," Computer Science-Research and Development, vol. 24, no. 4, pp. 185–197, 2016.

[7] Saibharath S, Geethakumari G "Cloud Forensics: Evidence Collection and Preliminary Analysis" IEEE, 2015

[8] BKSP Kumar RajuAlluri, Geethakumari G"A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing" IEEE, 2015.

[9] Mr. DigambarPowar, Dr. G. Geethakumari "Digital Evidence Detection in Virtual Environment for Cloud Computing" ACM, 2012.

[10] Hubert Ritzdorf, NikolaosKarapanos, SrdjanCapkun "Assisted Deletion of Related Content"ACM, 2014.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING