e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

SAFEGUARDING SAAS: SECURITY STRATEGIES & CLOUD FORENSICS

Prof. Zarina Shaikh[*1], Yash Bahekar[*2], Rohan Magar[*3], Sanchit Gade[*4], Prasad Khairnar[*5]

[*1]Guide Dr. D. Y. Patil Institute Of Technology Pimpri, Pune, India.

[*2,3,4,5]Student, Department Of Computer Engineering Dr. D. Y. Patil Institute Of Technology Pimpri, Pune, India.

DOI : https://www.doi.org/10.56726/IRJMETS52313

ABSTRACT

Software-as-a-Service (SaaS) is a versatile soft-ware delivery model, offering various business opportunities and challenges. This article explores its utility in diverse environments like cloud computing, mobile cloud computing, software-defined networking, and the Internet of Things. Despite security concerns, users are attracted to its benefits. The discussion delves into security challenges, including data and application security, and proposes solutions. The research focuses on identifying malicious activities in cloud-based SaaS, introducing a cloud forensic strategy for efficient cybercrime investigations. The strategy, based on a powerful cloud computing platform, serves as a guide for digital investigators dealing with SaaS attacks.

Keywords: Software-As-A-Service (Saas), Security, Cloud Computing, Cybercrime.

I. INTRODUCTION

In the rapidly evolving realm of cloud computing, Software-as-a-Service (SaaS) has become a cornerstone for organizations seeking efficient and flexible solutions. Despite its widespread adoption, concerns surrounding security have persisted since the inception of cloud computing. This review paper meticulously explores the diverse applications and challenges of SaaS applications.

This exploration delves into the intricate security challenges in SaaS environments, including data, application, and deployment security. The paper further identifies and scrutinizes malicious activities within cloud-based SaaS frameworks. This review paper enhances our understanding of digital forensics and security challenges in SaaS. By exploring advancements and methodologies, the research identifies potential areas for future development. The goal is to improve the security of SaaS systems and enable effective digital investigations in this dynamic technological landscape.

The research aims to create applications for detecting and preventing software-as-a-service attacks using soft com-puting techniques. It includes misbehaviour, signature based detection, and SQL injection analysis. The system identifies connections as malicious when remote users exhibit improper behavior with a legitimate Virtual Machine or application.

II. LITERATURE SURVEY

The survey explores cloud-based digital forensics, emphasizing its role in expediting processes [1]. It addresses challenges for providers and investigators in decentralized data processing [2], highlighting economic advantages and privacy, security, and forensic challenges [3]. It emphasizes innovative approaches, including efficient investigations using VM snapshots and addressing imaging complexities in cloud storage [4, 5]. The survey introduces architectures combining SDN and blockchain for evidence preservation [8], emphasizing the imperative need for data security in the digital era [9].

This paper discusses the challenges and benefits of digital forensic practices in cloud computing. It emphasizes the importance of cloud technologies in expediting forensic processes while addressing legal and technical complexities. The concept of "Digital Forensics as a Service" is introduced, showcasing the potential of cloud technologies in digital investigations [1].

This paper addresses the challenges faced by cloud service providers and investigators in conducting digital investigations in cloud environments. It highlights the need for new methodologies and tools to adapt to the decentralized nature of cloud data processing and storage [2].

The rapid growth of cloud computing technology is explored in this paper. While cloud computing offers economic advantages, privacy, security, and forensic issues remain significant challenges. The study acknowledges the importance of addressing these issues for the growth of cloud computing systems [3].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

This paper focuses on the challenges of conducting digital forensic investigations in multi-tenant cloud environments. It proposes an efficient approach to forensic investigation using Virtual Machine (VM) snapshots. The study highlights the dynamic nature of cloud computing and the opportunities it presents for digital investigations [4].

The paper addresses the challenge of dealing with the vast amount of data stored in cloud computing environments, making practical imaging for forensic investigators increasingly difficult. It explores acquisition times and remote acquisition methods for virtual machines in the cloud, emphasizing the importance of a partial and full approach to data acquisition [5].

This paper focuses on the challenges associated with the acquisition phase of cloud forensic investigations. It introduces a tool for acquiring virtual machine evidence from the cloud while preserving evidence integrity. The results are specific to the OpenStack cloud, but the methodology can be extended to other cloud platforms [6].

The study discusses the ubiquity of cloud computing and the potential challenges related to cloud security and new threats. It emphasizes the importance of digital forensic investigations in the context of cloud security incidents and outlines the challenges related to forensics data collection [7].

This paper introduces a novel digital forensic architecture that combines Software-Defined Networking (SDN) and blockchain technology to address the challenges of evidence collection and preservation in Infrastructure-as-a-Service (IaaS) cloud environments. The approach focuses on distributed evidence collection and preservation [8].

The paper highlights the need for data security and tamper resistance in the digital era. It discusses the impact of cybercrime on forensic evidence and introduces the use of blockchain for enhancing the security of forensic evidence [9].

This paper addresses the challenges related to conducting digital investigations in cloud settings. It emphasizes the need for appropriate forensic capabilities in cloud computing to investigate illegal activities. The study outlines the steps involved in digital investigations in cloud computing [10].

Cloud computing stands out as a transformative influence in today's IT environment, reshaping how businesses operate and impacting daily life. Its disruptive technology promises long-lasting effects, showcasing both its appeal and the challenges it presents to existing security frameworks. This article conducts a thorough examination of the current security landscape in cloud computing, utilizing insights gathered from an extensive survey conducted by the author. With a specific focus on the Software as a Service (SaaS) model within cloud computing, the paper delves into the inherent security challenges within this framework. Additionally, it aims to chart the future trajectory of security research in the dynamic field of cloud computing, acknowledging the need to address evolving security concerns [11].

The rapid expansion of cloud computing has fundamentally transformed the dynamics of contemporary network services, introducing a plethora of on-demand and flexible cloud-based services. While these advancements bring undeniable benefits, the adoption of cloud technology has raised significant security apprehensions. This research paper presents a survey that concentrates on three primary facets of cloud security: computer security, network security, and information security. Through a thorough literature review, it synthesizes recent developments in cloud security, providing a comprehensive understanding of the subject. The results of this survey contribute both theoretical insights and empirical evidence, establishing a solid groundwork for prospective research endeavors in the field of cloud security [12].

This research paper tackles the increasing data security issues within the rapidly growing realm of cloud computing. Concentrating on safeguarding data against cyber threats, the suggested resolution introduces a model that integrates a Trusted Third Party (TTP) and a Cloud Forensics Investigation Team (CFIT). Through this collaborative approach, the trustworthiness of service providers is enhanced, facilitating the detection and legal action against cyber attackers with robust evidential support [13].

This research delves into the changing dynamics of security in cloud computing throughout the last ten years. Despite the evident economic advantages and improved service quality, security concerns have consistently ranked as a significant challenge, with a notable emphasis in 2020. The paper offers a comprehensive classification of security issues within the context of the three-layer model encompassing Infrastructure as a

Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). It scrutinizes the present condition of security in cloud computing [14].

The paper explores the security challenges in the rapidly emerging industry of cloud computing. Recognizing the unprecedented nature of these challenges, the article underscores the need for collaborative efforts among researchers in IT and information security. The risks inherent in the cloud computing model are introduced, with a specific focus on the affected factors within the Software-as-a-Service (SaaS) security model. To address the current status of SaaS security, the paper proposes a novel method that integrates the Role-Based Access Control (RBAC) mechanism and the cloud cube model. This innovative approach aims to establish a secure mode for SaaS applications [15].

This paper proposes a novel approach to digital forensic readiness in the cloud by introducing a non-malicious Botnet as a Service (BaaS). Focused on proactive strategies, the model aims to gather digital information for potential evidence while adhering to international standards like ISO/IEC 27043. The BaaS implementation offers an innovative solution to address the existing gap in cloud forensic techniques [16].

In conclusion, the literature survey highlights cloud computing's impact on digital forensics and security. It emphasizes the challenges, underscores the need for robust investigations [7], and provides focused security analysis, guiding future research [11]. Addressing critical aspects of cloud security, the survey recognizes the transformative impact of cloud technologies, paving the way for informed discussions and research directions [12]. Serving as a valuable resource, it uncovers evolving challenges and potential areas for further exploration in the dynamic field of cloud computing security [13, 14].

III. PROPOSED METHODOLOGY

In response to the escalating security concerns in Software-as-a-Service (SaaS) environments within cloud computing, this section presents a comprehensive model designed to enhance cloud security and streamline forensic investigation processes. The proposed model addresses critical challenges such as misbehaviour detection and signature-based detection. The model can be outlined as shown in the Fig. 1. and is followed by the brief explanation.

Fig 1 Outline of Proposed Model

The proposed model is structured to ensure a robust and dynamic defense mechanism against potential security threats. The model comprises the following key components:

1) User: Represents the entity initiating requests within the system.
2) Server: Serves as the central authority managing access to cloud data, acting as a gatekeeper.
3) Virtual Machines (VMs): Multiple instances symbolize cloud data servers, encapsulating the distributed nature of cloud computing.
4) Pattern Matching Algorithm: A sophisticated process for identifying patterns in user requests, facilitating the detection of potential threats.
5) Similarity Weight: A quantitative measure indicating the match between a request and existing security policies, aiding in decision-making.
6) Admin: The administrative role responsible for reviewing and approving requests, ensuring exceptional cases are appropriately handled.

Below is the flow of the operations in the proposed model:

1) User Request: Initiates the process with a user sending a request to the server.
2) Request Validation: The VPN server validates the request, ensuring proper formatting and permissions.
3) Pattern Matching: If valid, the request undergoes pattern matching to identify similarities with existing security policies.
4) Similarity Weight Generation: A numerical value is calculated based on identified patterns.
5) Threshold Comparison: The weight is compared to a predefined threshold.
6) Decision Point:

a. Above Threshold: The query executes, granting user access to data.
b. Below Threshold: The request is routed to the admin for review.

7) Admin Review: The admin evaluates the request, either approving or denying it, and may update policies for future matching.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

8) Malicious Request Blocking: The admin possesses the capability to block malicious requests, safeguarding the overall system.

The proposed architectural model is designed to enhance the system's resilience against security threats, incorporating key components such as the 'User,' 'Server,' and 'Virtual Machines (VMs).' A central element is the 'Pattern Matching Algorithm,' identifying user request patterns for threat detection, complemented by the 'Similarity Weight' for decision-making.

Administrative oversight is embodied in the 'Admin' role, responsible for handling exceptional cases and ensuring the robustness of the system. The operational sequence unfolds with a 'User Request,' traversing through stages like 'Request Validation' and 'Similarity Weight Generation.' The 'Decision Point' becomes a critical juncture where the system either executes the query if it surpasses a predefined threshold or directs it to the 'Admin' for a comprehensive review, contributing valuable insights for future policy enhancements.

An essential feature is the 'Malicious Request Blocking', empowering the admin to proactively block nefarious requests. This capability serves as a proactive measure, reinforcing the overall security posture of the system by preventing potential threats from compromising its integrity.

The Fig. 2. Data Flow Diagram 0 (DFD0) for the SaaS attack and defense system provides a comprehensive illustration of the key components and interactions within the system. At its core are three external entities: the User, who interacts with the SaaS application; the Attacker, representing malicious actors attempting to exploit the application; and the System Admin, responsible for managing and securing the SaaS environment.

Fig 2 Data Flow Diagram 0 (DFD0)

The primary processes within the system are clearly outlined, starting with the "Input Query" process where the user submits queries or data to the SaaS application. The subsequent "Check Query" process involves the system validating the user's input for potential threats or malicious code. To fortify the system against attacks, the "Get Rules" process retrieves security rules and configurations from the database.

The central process, termed the "SaaS Attack & Defense System," encapsulates the various mechanisms employed for protecting the system. This includes intrusion detection, data encryption, and access controls, collectively working to ensure the security of the SaaS application.

The system's adaptability to evolving threats is demonstrated through the "Update Rules" process, where the system administrator modifies security rules based on new threats or vulnerabilities. The data stores, represented by "DB" (Database) and "VM" (Virtual Machine), play pivotal roles in storing data, rules, and creating a virtual environment for executing the SaaS application or implementing security measures.

The data flows through the system seamlessly, with a user-initiated query being checked for security risks, validated against stored security rules, and processed through the SaaS Attack & Defense System. The system administrator, in turn, can update security rules in the database, creating a dynamic loop that allows the system to adapt and defend against future attacks.

IV. CONCLUSION

This paper explores Software-as-a-Service (SaaS) in cloud computing, examining its potential and challenges, with a focus on security concerns. It sets the stage for a comprehensive discussion on the practical utility of SaaS. The paper critically examines SaaS security challenges, focusing on data, application, and deployment security. The proposed model underscores the importance of identifying malicious activities in a SaaS environment.

The literature survey reviews pivotal research on digital forensics, investigating challenges in cloud environments and innovative solutions. The paper outlines a research project concentrated on designing SaaS attack detection and prevention applications, covering aspects like misbehaviour detection, signature-based detection, and SQL Injection prevention. The model outlines a structured architecture involving users, servers, virtual machines, pattern matching algorithms, similarity weights, and administrators to ensure a secure cloud data system. The paper enhances our grasp of cloud security challenges and the role of digital forensics in tackling them. The proposed model offers a dynamic defense for SaaS environments, addressing potential threats. The study emphasizes the evolving nature of cloud computing, highlighting the ongoing need for exploration and development in cloud security and forensics.

V. REFERENCES

[1] J. Farina, M. Scanlon, N. -A. Le-Khac and M. -T. Kechadi, "Overview of the Forensic Investigation of Cloud Services," 2015 10th International Conference on Availability, Reliability and Security, Toulouse, France, 2015, pp. 556-565, doi: 10.1109/ARES.2015.81.

[2] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 2011, pp. 1-10, doi: 10.1109/SADFE.2011.17.

[3] S. Bhatia and J. Malhotra, "Forensic Based Cloud Computing Architecture – Exploration and Implementation," 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2019, pp. 37-45, doi: 10.1109/ICCCT2.2019.8824813.

[4] D. R. Rani and G. Geethakumari, "An efficient approach to forensic investigation in cloud using VM snapshots," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-5, doi: 10.1109/PERVASIVE.2015.7087206.

[5] N. Thethi and A. Keane, "Digital forensics investigations in the Cloud," 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, India, 2014, pp. 1475-1480, doi: 10.1109/IAdCC.2014.6779543.

[6] B. K. Raju, Meera G and G. Geethakumari, "Cloud forensic investigation: A sneak-peek into acquisition," 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, India, 2015, pp. 348-352, doi: 10.1109/CoCoNet.2015.7411209.

[7] S. Syed and V. Anu, "Digital Evidence Data Collection: Cloud Challenges," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 6032-6034, doi: 10.1109/BigData52589.2021.9672014.

[8] M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," in IEEE Access, vol. 7, pp. 153349-153364, 2019, doi: 10.1109/ACCESS.2019.2946978.

[9] S. Patil, S. Kadam and J. Katti, "Security Enhancement of Forensic Evidences Using Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 263-268, doi:10.1109/ICICV50876.2021.9388486.

[10] Mandal, Pawan and Rajput, Isha. (2023). Cloud Forensics: Exploring the Challenges and Mapping Out Solutions for the Future. 10.13140/RG.2.2.18945.53605.

[11] Rai, Rashmi & Sahoo, Gadadhar & Mehfuz, Shabana. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture. 3. 10.5121/ijccsa.2013.3401.

[12] X. Sun, "Critical Security Issues in Cloud Computing: A Survey," 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Omaha, NE, USA, 2018, pp. 216-221, doi: 10.1109/BDS/HPSC/IDS18.2018.00053.

[13] Sheik Khadar Ahmad Manoj, D.Lalitha Bhaskari,Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment, Procedia Computer Science,Volume 85,2016,Pages 149-154,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2016.05.202.

[14] Khoda Parast, Fatemeh & Sindhav, Chandni & Nikam, Seema & Yekta, Hadis & Kent, Kenneth & Hakak, Saqib. (2021). Cloud Computing Security: A Survey on Service-based Models. Computers & Security. 114. 10.1016/j.cose.2021.102580.

[15] S. Liu, K. Yue, H. Yang, L. Liu, X. Duan and T. Guo, "The Research on SaaS Model Based on Cloud Computing," 2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2018, pp. 1959-1962, doi: 10.1109/IMCEC.2018.8469462.

[16] Kebande, Victor & Venter, H.s. (2014). A Cloud Forensic Readiness Model Using a Botnet as a Service. 10.13140/2.1.4880.2249.