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:03/March-2024 Impact Factor- 7.868 www.irjmets.com

CLOUD MALWARE PROTECTION STRATEGIES

Sandeep Reddy Gudimetla[*1]

[*1]HCL America.

DOI : https://www.doi.org/10.56726/IRJMETS51189

ABSTRACT

In the digital age, cybersecurity is always at the top of the list of matters of concern, especially when the data is always on the client's end and not properly secured. This article explores more advanced approaches for cloud malware protection in which real-time detection tools and automation malware removal techniques form a crucial cornerstone of the network security system. Detecting illicit activity in real-time in a cloud setting is vital for discovering and responding to threats as soon as they emerge, which is now being achieved through deep learning techniques and an intelligent identification model. Unlike the responsive tools that detect and delete the malware, the latest auto tools focus on a proactive approach alongside the efficiency of complex malware removal, even on ransomware. These techniques ensure cloud platforms' integrity and security, indispensable nowadays as they draw the interconnected world. This is because malware will keep evolving and inventing itself, so new and improving techniques must be developed for detection and removal. With cloud computing platforms becoming increasingly a business and personal life backbone, the significance of strong malware protection measures in the future is just an oversimplification.

I. INTRODUCTION

As technology has been developing quickly, cloud computing has shaken up data storage, access, and management while providing unique advantages such as flexibility and scalability. Malware attacks on clouds are distinct threats given that clouds are distributed and serve infrastructures that process and store vast amounts of sensitive data. In this case, two key aspects of cloud malware protection are explored: built-in detection and malware evasion facilities. Confronting threats in real-time is a cutting-edge that captures and handles malware as it is being executed. Despite the swiftness of Malware detection, it is essential to address the attack quickly to avoid the negative impact ranging from data theft to complete system compromise. In contrast to the preventive malware elimination tools, which form the first line of defense by blocking threats before they enter the computers, other automated malware removal tools offer a second layer of defense, which systematically scans and removes all unidentified threats that can have bypassed the initial security measures. Both the usage of control and the concept of security are integrated into the cloud security framework as they must be tried. The targeted use of current research and emerging innovation technologies will serve as the foundation for this article and present the in-depth future of such countermeasures. For this, it studies how combining these techniques can do singly and together offer cloud pools a strong defense against malware attacks.

II. REAL-TIME DETECTION IN CLOUD ENVIRONMENT

Real-time perception in the public cloud realm is one of the main factors of today's cybersecurity methods. The suggested model will be an ongoing survey of cloud environments to detect, provide protection, and rectify impairments before they affect systems. This non-pretense characteristic of cryptocurrency is vital to furthering a portfolio that covers all the gaps and has a breach avoidance feature. The delays in the detection that we see today are the result of the multiple factors that are involved and of the algorithms that we currently have, which can be inadequate to filter and identify threats in a timely manner. An Intelligent Malware Detection Model can identify potentially dangerous malware with a fine-tuned machine-learning algorithm that empowers it to do this accurately [1]. Another method to use involves deep learning; Deep learning Models to Use is a Technique to Behavior-based Malware Analysis, where they explain how deep learning models can detect behavioral anomalies, which may indicate an attack [2]. The techniques, which capitalize on the AI features, a token of revolution, and these present configurations of being time, space, and behavior are the heroes against the dynamic and revolutionary nature of the malware, giving it an upper hand in detecting and reacting to malware threats in real-time.

Another essential factor is the reliability of real-time detection in cloud design, and it is quite expensive to deploy the system into the cloud economy. This unification guarantees that data storage and various applications thus maintain functioning while working under continuous monitoring. The real-time area is the most difficult to manage because cloud services are dynamic and scalable and can change at any time without warning [3]. Despite these challenges, real-time systems' development and employment are of great importance, as they are imperative for depending on the integrity and security of cloud services. The further development and improvement of these systems indicate the essence of staying in front of the complex cyber threats that are becoming increasingly refined.

III. AUTOMATED MALWARE REMOVAL TOOLS FOR CLOUD PLATFORMS

After malware detection in the cloud, the most important thing is its complete and efficient elimination. Automated malware elimination tools play a crucial role here due to their fast and effective feature, which enables instant identification and removal of threats in seconds. Computer security tools contain features that help them clean the infected computer pieces from malware while repairing the damage done by any malware and returning the system to its integrity and functionality. An efficient detection and removal of ransomware is implemented by utilizing volatile memory features as indicators in the cloud environments [4]. This strategy highlights the need for state-of-the-art cybersecurity instruments that are adaptable to emerging types of attacks and go several steps ahead in intercepting intricate cloud-based malware attacks, such as ransomware.

Cloud infrastructures and malware have a variety of forms. Thus, thorough knowledge of malware removal tools and cloud structures forms the foundation of automated malware removal tool development. The access control mechanisms must be so advanced that they can handle the multi-tenant nature of cloud services. This ensures that the actions against malware affecting one customer or service don't adversely impact other users and services. Moreover, the cloud's scale and elastic properties require the tools to restructure their operational units according to the circumstances and available resources in hand. Incorporating AI into such tools can enhance their effectiveness [2]. Through subsequent attack scarring and threat evolution, the automatic corruption tools will step ahead of the attackers [5]. They will form a very deployable defense system akin to the targeted threats, providing a robust defense mechanism that can co-evolve alongside the threats driving its creation.

IV. CONCLUSION

In conclusion, effective cloud malware protection, containing real-time detection and automated removal, is vital in today's digitally connected world. These strategies, rooted in developed technologies like AI and machine learning, are crucial for protecting cloud surroundings against evolving cyber threats, thus confirming the security and integrity of vast amounts of essential data.

V. REFERENCES

[1] G. Karthick, B. R. Jeyavadhanam, V. V. Ramalingam and S. Ling, "Improved Intelligent Malware Detection Model in Cloud Environment. „" Lecture Notes in Networks and Systems, p. 343–353, 2024.

[2] N. Z. Gorment, A. Selamat and O. Krejcar, "A recent research on malware detection using machine learning algorithm: current challenges and future works," Advances in Visual Informatics, p. 469–481, 2021.

[3] A. McDole, M. Gupta, M. Abdelsalam, S. Mittal and M. Alazab, "Deep learning techniques for behavioral malware analysis in cloud IaaS," Malware Analysis Using Artificial Intelligence and Deep Learning, p. 269–285, 2020.

[4] Prachi and S. Kumar, "An effective ransomware detection approach in a cloud environment using volatile memory features," Journal of Computer Virology and Hacking Techniques, no. 10.1007/s11416-022-00425-2, 2022.

[5] S. K. Medaram and L. Maglaras, "Malware mitigation in cloud computing architecture," Security Informatics and Law Enforcement, p. 235–278, 2023.