

2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)

Intelligent Malware Detection System Based on Behavior Analysis in Cloud Computing Environment.

Jibu K Samuel

Department of Computer Engineering
Amal Jyothi College Of Engineering
Kerala, India
jibuksamuel2023@cs.ajce.in

Mahima Thankam Jacob

Department of Computer Engineering
Amal Jyothi College Of Engineering
Kerala, India
mahimathankamjacob2023@cs.ajce.in

Melvin Roy

Department of Computer Engineering
Amal Jyothi College Of Engineering
Kerala, India
melvinroy2023@cs.ajce.in

Sayoojya P M

Department of Computer Engineering
Amal Jyothi College Of Engineering
Kerala, India
sayoojyapm2023@cs.ajce.in

Anu Rose Joy

Department of Computer Engineering
Amal Jyothi College Of Engineering
Kerala, India
anurosejoy@amaljyothi.ac.in

Abstract—IBMD(Intelligent Behavior-Based Malware Detection) aims to detect and mitigate malicious activities in cloud computing environments by analyzing the behavior of cloud resources, such as virtual machines, containers, and applications. The system uses different machine learning methods like deep learning and artificial neural networks, to analyze the behavior of cloud resources and detect anomalies that may indicate malicious activity. The IBMD system can also monitor and accumulate the data from various resources, such as network traffic and system logs, to provide a comprehensive view of the behavior of cloud resources. IBMD is designed to operate in a cloud computing environment, taking advantage of the scalability and flexibility of the cloud to detect malware and respond to security incidents. The system can also be integrated with existing security tools and services, such as firewalls and intrusion detection systems, to provide a comprehensive security solution for cloud computing environments.

Index Terms—Virtualization, Cloud computing, , behavioral detection, malware detection.

I. INTRODUCTION

Malware detection in cloud computing is the process of identifying and preventing malicious software or code from infiltrating cloud-based systems, applications, and data. With the growing popularity of cloud computing, the risk of malware attacks has become a major concern for organizations that rely on the cloud to store and manage their data. Malware attacks can result in data theft, system disruption, and financial losses. To combat these threats, various malware detection techniques are employed, such as signature-based detection, behavior-based detection, and machine learning-based detection. These techniques analyze and monitor cloud-based systems for any suspicious activities, and upon detection, they take prompt action to prevent any further damage. With the increasing sophistication of malware attacks, the need for robust malware detection in cloud computing has become more important than ever. By implementing effective malware detection systems,

organizations can assure the and integrity and security of their data in the cloud.

Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment is a cutting-edge technology designed to detect and prevent malware attacks in cloud computing environments. The system utilizes advanced artificial intelligence and behavior-based techniques to identify and neutralize malicious activities in real-time. With the increasing adoption of cloud computing, the need for robust malware detection systems has become paramount. The intelligent behavior-based approach offers an effective solution to counter the ever-evolving nature of malware attacks. This system provides enhanced security and protection to organizations, their data, and their clients, ensuring that they remain safe and secure in the cloud.

A. Cloud Computing

Cloud computing refers to the delivery of computing services over the internet, such as servers, storage, databases, networking, software, and analytics. Users can access and use these services on-demand and only pay for what they use. Cloud computing allows for scalability, reliability, and cost-effectiveness compared to traditional on-premises computing. Cloud computing offers several benefits, including:

- **Scalability:** Cloud computing allows users to scale up or down their computing resources according to their needs, making it easier to handle sudden increases in demand.
- **Cost-effectiveness:** Cloud computing can reduce the costs associated with maintaining on-premises infrastructure, such as hardware, maintenance, and upgrades.
- **Reliability:** Cloud computing providers typically offer high availability and redundancy, which ensures that services remain accessible and reliable even in the event of hardware or software failures.

979-8-3503-3324-4/23/\$31.00 ©2023 IEEE

Authorized licensed use limited to: Swinburne University of Technology. Downloaded on March 18, 2025 at 11:17:08 UTC from IEEE Xplore. Restrictions apply.