Protect the virtual machine from malicious events using a secure deep learning framework for the cloud.

Vinit Kumar

Koneru Lakshmaiah Education Foundation, Guntur 522502,India

K saikumar, Department of ECE, Koneru Lakshmaiah Education Foundation, India-522302,

saikumarkayam4@ieee.org

Abstract

In recent decades, user communication has been digitalized with some advanced applica- tions. However, securing the digital cloud system is complicated because of the vulner- ability of large files and malicious events. Therefore, a present research study intendedto design a novel Dragonfly-based Genetic Deep Belief Network (DGDBN) technique to protect the VM from malware activities in the cloud environment. Hence, to validate the presented model, the cloud user files data was considered and imported to the system as input. Then further processes such as preprocessing feature extraction, attack detection andclassification were performed. Once the malicious event is predicted, it is neglected by the cloud user environment. Furthermore, implemented novel DGDBN model is tested in the MATLAB programming environment. Finally, the performance parameters like accuracy, precision, reconfiguration time, Recall, F-measure, and data overhead were measured and compared with associated approaches.

Keywords Virtual machine · Deep belief neural network · Cloud user · Malicious events ·Optimization

1 Introduction

Cloud computing is the most widespread and generally used computing standard. Virtual- ization is the dominant cloud computing tool in which several users can access and share the same computing frame self-reliantly [1]. Cloud to the customers offers virtually lim- itless assets. Cloud computing has numerous advantages, including dependability, qual- ity, and service delivery robustness [2]. It provides favours to the customers in multiple ways, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Soft- ware as a Service (SaaS) [3]. The environment benefits greatly from the cloud comput- ing system in multiple ways, such as healthcare, business, and education. Because it may use both private and public cloud capabilities, the hybrid cloud is a unique cloud com- puting approach [4]. Initially, the malware can be prevented by a signature-based sys- tem, securing specific patterns and signatures for unknown files. The antimalware vendors produce the signature after known malware analysis and distribute it to the client com- puters to update the signature database. An essential step in studying malware detectionis finding several features, such as normal and malware files [5]. Then, static approaches are used to find the malware through benign programs utilizing the binary program fea- tures and extracting the opcode by disassembling the file. According to the weakness of static approaches, the dynamic approach can monitor the VM in terms of dynamic features,namely system calls and the presence of a string in process memory [6].

Two foremost virtualization techniques are there in cloud computing; they are: hard- ware-based and operating system-based [7]. In hardware-based technology, a VM is the core system to offer cloud services to users. The collections of processing elements in the cloud are named virtual machines distributed to networks. VMs are located in failed cloud system nodes, which tend to relocate VM from one node to another. The two management systems of VM in cloud service centres are static and dynamic placement[8]. Static order focuses on the positioning of many VMs, and dynamic sequence focuses on VMs' connected migration when the system is running. The security suscepti- bility of the cloud nature reveals VMs at the end of risk. To safeguard VM against adware attacks, a highly capable adware attack detection system is required [9]. Internet mal- ware introduces a vast threat to computer system security. Subsequently, malware aims to collect locally sensitive information such as passwords, information on the bank account, and CD keys and leverage infected hosts for several attacks, included with spam relay, IP laundering, DDoS, and phishing. These malicious actions are frequently represented the information harvesting and dispersion of information.

The cloud user files database was initially gathered and trained to the system as the input.

- Moreover, a novel DGDBN was developed with the required feature analysis and pre- diction modules.
- Primarily, the data was preprocessed, and feature extraction was performed. Here, the n-gram features are considered meaningful features.
- Therefore, the attack was detected and classified using the fitness function of the Drag-onfly-designed model and protected the VM from cluster-based authentication.
- Also, the proposed DGDBN model was implemented in the MATLAB tool and com- puted the performance measurements such as accuracy, precision, Recall, and f-meas- ure.

2 Related Works

A few recent works related to virtual machine protection systems are discussed.

Alkadi *et al.* [25] proposed a Deep Learning structure to identify surface cyber-attacks and enhance data privacy in the cloud and IoT. A VM also makes use of this methodto yield more privacy at the time of active movement. This technique would enable the real-time and safe transfer of the VMs between data centres or system providers. Intro- duced structures used the following elements; privacy-preservation-based blockchain, cloud vendor and smart contracts, Collaborative Intrusion Detection System (CIDS) and Central Coordinator Unit (CCU) for detecting and classifying various overrunning mali- cious attacks. But, combining a blockchain-based approach and deep learning led to some demerits, like difficulty in transmission, which indicated the transmission rate of creating new structures for all clients.

3 System Model and Problem Statement

The Virtual Machine Introspection (VMI) is a fine-grained VM security solution for identifying malware through introspection, and the Virtual Machine Monitor (VMM) reconstructs the volatile memory state of the live guest Operating System (OS) Vir-tual machine Monitor (VMM). The Online Malware Detector (OMD) and the Offline Malware Classifier (OFMC) were two sub-components of this system model's malware detector. When the dataset was cross-referenced with the observed hidden and suspi- cious process, the OMD determined whether the malware was present.

The online mal- ware scanning required the generated hash digest for each extracted

Table 1 Summary of state-of-the-art approaches

Author	Methods	Advantages	Disadvantages
Alkadiet al. [25]	Deep Blockchain Framework (DBF)	Most effective in detecting insider and outsider attacks in both IoT and cloud	High communication complexity, traffic overhead
Tian et al. [26]	MDCHD	Deployment for the cloud environments is easy, with a minimal perfor- mance cost	It can bear only one VM at a time, also restricted in identifying sneaky malware
Alasrhanet al. [27]	Fuzzy multiple criterion decision-making schemes	Higher throughput, minimizing traffic in the cloud market	Some cloud market nodes deny sending packets and eliminate part of them
Pankeret al. [28]	Trusted detection framework	Better performance	During the acquisition process of volatile memory, the VM becomes idle tem- porarily, which may cause a hamper in service to the users
Gao et al. [29]	Semi-supervised transfer learning with RNN	It attained high accuracy with low FPR	The running time of the RNN was much longer

4 Proposed DGDBN

It is difficult to identify malware in a cloud setting. The standard malware detection sys- tem would have a long running time and low accuracy in the cloud. Therefore, to carry out the malware detection mechanism with high accuracy, a Dragonfly-based Genetic Deep Belief Network (DGDBN) was proposed in this work. The proposed mechanism included unique levels: fetching input data, preprocessing, feature extraction, malware detection, classification and protection of VM levels. This work

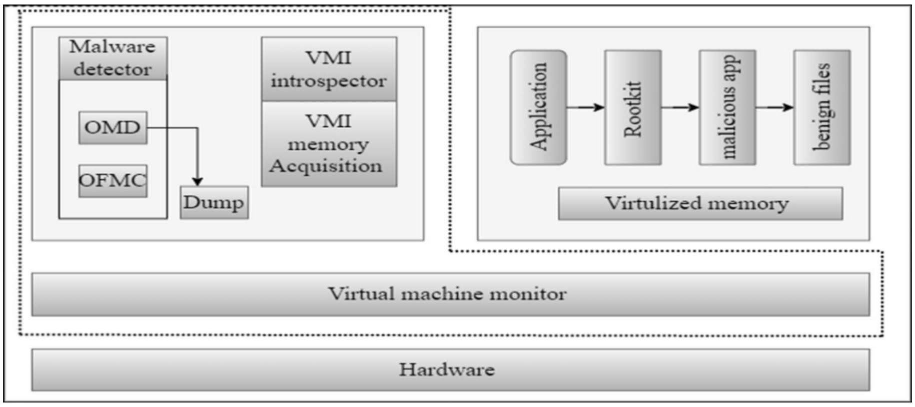

Fig. 1 System model

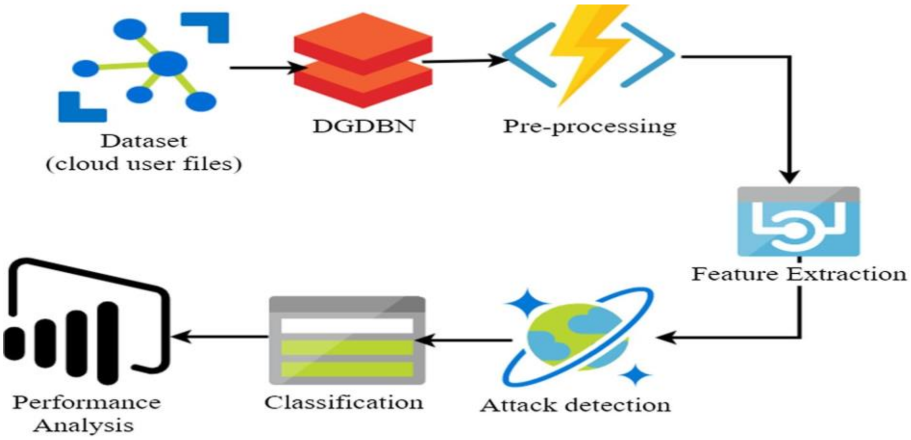

Fig. 2 The Block diagram of DGDBN

5 Result and Discussion

The proposed approach was developed on the MATLAB platform and running on win- dows 10. The cloud user files data was considered to measure the robustness of the designed model. Here, the CH is activated for verifying the user integrity and blocking access of the unauthenticated users.

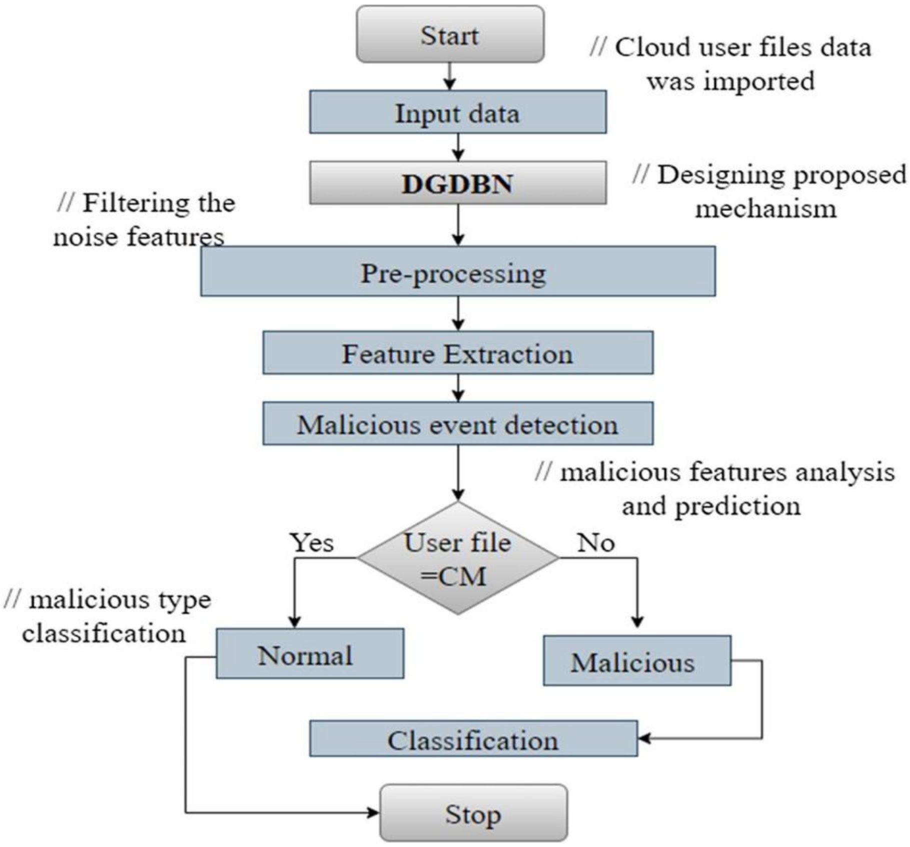
Start
// Cloud user files data was imported
Input data
DGDBN
// Designing proposed mechanism
// Filtering the noise features
Pre-processing
Feature Extraction
Malicious event detection
// malicious features analysis and prediction
Yes
User file =CM
No
// malicious type classification
Normal
Malicious
Classification
Stop

Fig. 3 Flowchart of DGDBN

6 Conclusion

This study deals with malware detection, which aims to protect the VM from malware activities. Here, the DGDBN technique was utilized to detect malicious activities in the VM. Initially, preprocess the data to remove the unwanted noise and enter the data into thefeature extraction process. The feature was extracted using the fitness function of the pro- posed model for classifying the malware. Thus, the proposed model detected and organizedthe malware efficiently and enhanced the VM to protect it from malware activities. The developed DGDBN model attained a highly accurate result of 99.6%, so the improvement percentage compared to the other models was 3%. The advantage of this framework helpedto improve the classification process of malware present in the VM easily. It takes more time for the attack detection process. So, in the future, the hybrid form of DL models with efficient optimization techniques will improve the protection of VMs from malware events.

References

1. Geetha, R., Suntheya, A. K., & Srikanth, G. U. (2020). Cloud integrated IoT enabled sensor network security: Research issues and solutions. *Wireless Personal Communications, 113*, 747–771. https://doi. org/10.1007/s11277-020-07251-z

2. Dawson, J. A., McDonald, J. T., Hively, L., Andel, T. R., Yampolskiy, M., & Hubbard, C. (2018).

Phase space detection of virtual machine cyber events through hypervisor-level system call analysis. In: *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, IEEE. https://doi.org/10.1109/ICDIS.2018.00034

3. Kim, H., Kim, J., Kim, Y., Kim, I., & Kim, K. J. (2019). Design of network threat detection and classification based on machine learning on cloud computing. *Cluster Computing, 22*(1), 2341–2350. https://doi.org/10.1007/s10586-018-1841-8

4. Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Computers & Security, 74, 340-354.

5. Al Makdi, K., Sheldon, F. T., & Hussein, A. A. (2020, November). Trusted security model for IDS using deep learning. In 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS) (pp. 1-4). IEEE.

6. Raju, K., Pilli, S. K., Kumar, G. S. S., Saikumar, K., & Jagan, B. O. L. (2019). Implementation of natural random forest machine learning methods on multi spectral image compression. Journal of Critical Reviews, 6(5), 265-273.

7. Saba, S. S., Sreelakshmi, D., Kumar, P. S., Kumar, K. S., & Saba, S. R. (2020). Logistic regression machine learning algorithm on MRI brain image for fast and accurate diagnosis. International Journal of Scientific and Technology Research, 9(3), 7076-7081.

8. Saikumar, K. (2020). RajeshV. Coronary blockage of artery for Heart diagnosis with DT Artificial Intelligence Algorithm. Int J Res Pharma Sci, 11(1), 471-479.

9. Saikumar, K., Rajesh, V. (2020). A novel implementation heart diagnosis system based on random forest machine learning technique International Journal of Pharmaceutical Research 12, pp. 3904-3916.