


Chapter 8

Evaluating Antivirus Effectiveness Against Malware in Ascending Order for Increasing Blockchain Endpoint Protection

Humam Imad Wajeeh Al-Shahwani
University of Baghdad, Iraq


Kamal Kant Hiran
*Sir Padampat Singhanian University,
India*

Maad M. Mijwil

 <https://orcid.org/0000-0002-2884-2504>
*Baghdad College of Economic
Sciences University, Iraq*

Indu Bala
Lovely Professional University, India

Ruchi Doshi

 <https://orcid.org/0000-0002-7259-8481>
Universidad Azteca, Mexico

ABSTRACT

Blockchain represents a new promising technology with a huge economic impact resulting from its uses in various fields such as digital currency and banking; malware represents a serious threat to users, and there are many differences in the effectiveness of antivirus software used to deal with the problem of malware. This chapter has developed a coefficient for measuring the effectiveness of antivirus software. This chapter evaluates the effectiveness of antivirus software by conducting tests on a group of protection programs using a folder containing an amount of data. These programs are applied to combat viruses contained in this folder. The study revealed that the effectiveness of antivirus software is as follows: AVG scored 0%, Advanced System Protector scored 20%, Avast scored 60%, and Malwarebytes scored 80%, respectively. DOI: 10.4018/979-8-3693-1131-8.ch008

1. INTRODUCTION

Malware is a term that includes all types of malicious programs (Yang et al., 2019; Maniriho et al., 2022). In general, they all share that they are programs designed to cause harm to the user, whether it is an individual, a company, an institution, a government agency, or a technology as in our topic, which is (Blockchain) technology, but the difference between them is the way they cause (Unogwu et al., 2022; Kumar et al., 2019). This damage, due to the different purpose and benefit sought from its establishment, as well as the way it deals with anti-virus programs or anti-malware (Yang et al., 2023; Winter et al., 2022). Blockchain is an advanced database technology that allows information to be shared publicly within a network of dealers. A blockchain database stores data in blocks linked together in a chain (Santhi and Muthuswamy, 2022; Javaid et al., 2022). The data is temporally consistent because you cannot delete or modify the chain without consent from the network, and this is supposed to provide security within the chain as the blockchain network is a safe technology in itself, due to the consideration that it is almost impossible to lose data even if one of the blocks is exposed within the chain of hacking, the danger lies when ordinary users who use the endpoint of the network are compromised (Mustafa et al., 2022; Athanere and Thakur, 2022). There are many examples of well-planned (network endpoint in blockchain technology) malicious attacks that succeeded in achieving their goals, for example, targeting the user's email and then using the user's private data to finance their purposes.

The development and the complexity of the malicious software's founded on the other side a reflex development and complexity of the anti-viruses software's and tools, the anti-viruses software's and tools have a variation and differences between one and another be , on the other hand not all the users have enough knowledge of the anti-viruses software and application, there are many anti-virus that may not determine the infection or not scanning all the files within the folder or may take long time during the scanning process (Mijwil et al., 2023; Doshi et al., 2023; Kumar et al., 2022). Hence, the need of determine the level of effectiveness for the anti - virus software in practical environment according to a specific parameters that have impact effect of the anti- virus software and to the user interaction with those anti-viruses software, in this paper there are four major aspects the parameters determine to measure the level of the efficiency level of the anti - virus, then put the anti-virus under test in a practical environment to measure who far the anti-virus satisfy the parameters goals, the four major aspects of the parameters includes: Finding the infection, Scanning all the files, the time needed for scanning the required files and provide interface within local language of the users.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/evaluating-antivirus-effectiveness-against-malware-in-ascending-order-for-increasing-blockchain-endpoint-protection/338089

Related Content

Using Systems Biology Approaches to Predict New Players in the Innate Immune System

Bin Li (2011). *Handbook of Research on Computational and Systems Biology: Interdisciplinary Applications* (pp. 428-477).

www.irma-international.org/chapter/using-systems-biology-approaches-predict/52328

Simulating the Spread of an Epidemic in a Small Rural Kansas Town

Todd Easton, Kyle Carlyle, Joseph Anderson and Matthew James (2011). *International Journal of Artificial Life Research* (pp. 95-104).

www.irma-international.org/article/simulating-spread-epidemic-small-rural/54750

Visual Tracking Using Multimodal Particle Filter

Tony Tung and Takashi Matsuyama (2014). *International Journal of Natural Computing Research* (pp. 69-84).

www.irma-international.org/article/visual-tracking-using-multimodal-particle-filter/118158

Load Balancing for the Dynamic Distributed Double Guided Genetic Algorithm for MAX-CSPs

Sadok Bouamama, Khaled Ghedira and Nisrine Zaier (2010). *International Journal of Artificial Life Research* (pp. 68-86).

www.irma-international.org/article/load-balancing-dynamic-distributed-double/49684

Swarm Intelligence-Empowered Bug Prediction Strategy for Decision Support in Software Defect Prediction

Medhunhashini D. R. and Jeen Marseline K. S. (2024). *Intelligent Decision Making Through Bio-Inspired Optimization* (pp. 18-28).

www.irma-international.org/chapter/swarm-intelligence-empowered-bug-prediction-strategy-for-decision-support-in-software-defect-prediction/344560