REVIEW

by Prof. Vassil Guliashki, Ph.D.
Institute of Information and Communication Technologies - BAS
on a dissertation thesis for acquiring the educational and scientific degree **"Doctor"**
in professional direction **4.6 "Informatics and Computer Science"**
doctoral program **„Informatics“**

titled: “RESEARCH AND ANALYSIS OF THE POSSIBILITIES FOR DETECTION OF MALWARE THROUGH MACHINE LEARNING”

by ILIYAN MAGDALENOV BARZEV

By order № 673/27.10.2025 By order No. 27/30.01.2026 of the Director of IICT - Corresponding Member Dr. Svetozar Margenov - in connection with the procedure for acquiring the educational and scientific degree "Doctor" in professional field 4.6 Informatics and Computer Sciences, doctoral program "Informatics" by **Iliyan Magdalenov Barzev** with a dissertation on the topic "Research and analysis of the possibilities for detection of malware through machine learning" I am included in the Scientific Jury.

As a member of the Scientific Jury, I have received:

1. Dissertation for awarding the educational and scientific degree "Doctor" in Bulgarian,
2. Abstract in Bulgarian,
3. Abstract in English,
4. Certificate of fulfillment of the minimum national requirements for acquiring the educational and scientific degree "Doctor",
5. List of publications on the topic of the dissertation,
6. Copies of publications on the dissertation,
7. Declaration of originality of the results obtained,
8. Similarity report from the StrikePlagiarizm.com system.

When evaluating the dissertation, the terms of the Law on the development of the academic staff in the Republic of Bulgaria (LDASRB), the Regulations for Implementation of LDASRB (Decree No. 26 of February 13, 2019) and the Regulations of Institute of Information and Communication Technologies – BAS for application of the Law for the development of the academic staff in the Republic of Bulgaria are decisive.

1. According to Art. 27 (1) of LDASRB "the dissertation work shall contain scientific or applied research results that represent an original contribution to science. The

dissertation shall show that the candidate has profound theoretical knowledge in the respective subject, as well as their abilities of independent scientific research."

2. According to Art. 27 (2) of LDASRB the dissertation work should be presented in a form and volume corresponding to the specific requirements of the primary unit. The dissertation work should contain title page; contents; introduction; presentation; conclusion – summary of the obtained results, accompanied by declaration of originality; bibliography.

The scientific supervisors of the dissertation thesis is Prof. D.Sc. Daniela Borissova.

Relevance of the topic

Malware detection and analysis is especially relevant today in the presence of wars, numerous cyber threats and hacker attacks. Malware protection is important for several reasons. Malware protection is important for several reasons: 1) data security (personal and financial data), the loss of which leads to identity theft or financial losses. 2) Damage to computer systems and information networks - infection with computer viruses leads to loss of information and expensive repairs. 3) Impact on productivity - crashes may occur, disrupting the normal rhythm of work, which is associated with loss of time and resources. 4) Data protection by many organizations is required by law.
I believe that the usefulness and relevance of the dissertation research is easily visible and understandable. I positively assess the thematic focus and current issues of the dissertation research.

Degree of knowledge of the state of the problem and creative interpretation of the literary material

Based on the first overview chapter, I positively assess the degree of knowledge of the problem of analysis and techniques for detecting and classifying malware.

Compliance of the selected research methodology with the set goal and tasks of the dissertation work

The selected research methodology is logical and consistently implemented. It includes:

- Analysis of scientific literature - to classify methods for detecting malware using machine learning.
- Development of mathematical models through which to select software for a suitable virtual machine for the purposes of detecting malware.
- Development of an approach for static analysis for detecting malware with optimizing feature extraction by combining various machine learning algorithms.
- Development of a framework for static classification of malware that uses function optimization and ensemble learning.
- Developing an adaptive, trust-aware framework for malware classification with feedback corrections that includes a self-aware model classifier.

GENERAL CHARACTERISTICS OF THE DISSERTATION THESIS

Dissertation thesis is in a volume of 143 pages with 204 tables, 43 figures, and includes an introduction, three chapters, a conclusion and a bibliography of 155 sources. It contains a list of abbreviations used.

The goal of the dissertation is to investigate and analyze the possibilities of detecting malicious software using machine learning tools, based on which to propose suitable hybrid models, frameworks and applications for obtaining better results in detecting malicious software. To achieve this goal, **the following tasks** have been formulated and implemented:

1) to analyze different machine learning algorithms regarding their performance for the purposes of detecting malicious software,

2) to determine a suitable virtual machine to be used when conducting tests for detecting and classifying malicious software,

3) to propose an improved approach for static analysis for detecting malicious software by optimizing feature extraction and combining different machine learning algorithms,

4) to propose a framework for static malware classification using feature optimization and ensemble learning,

5) to propose self-aware malware classification by routing models based on a trust system for feature selection and explainability,

6) to propose an adaptive, trust-based framework for malware classification with feedback adjustments.

The formulated goal and objectives have scientific and applied scientific potential for research and application in the field of information processes, information systems and technologies.

Brief analytical description of the material on which the contributions of the dissertation are built

The dissertation has an internal logic and corresponds to the requirements for academic research work.

In the first chapter, an analysis of various machine learning algorithms is made regarding their performance for the purposes of malware detection. Testing of the applicability of binary classification algorithms for malware detection is presented using a public dataset infected with 9 types of malwares, using a proposed methodology.

In the second chapter, two models for selecting a virtual machine are proposed for the purpose of conducting malware detection experiments. An improved static analysis approach is presented by optimizing feature extraction, combining various machine learning algorithms for malware detection. A proposed framework for static malware classification using feature optimization and ensemble learning is presented. To refine the classification of malware, an adaptive framework tailored to trust is proposed, allowing for malware classification with the possibility of corrections through feedback.

In the third chapter, the results of the testing of the proposed models for software selection for a virtual machine are presented. The results of the testing of the proposed improved static analysis approach by optimizing feature extraction, combining different

machine learning algorithms, are described. Numerical experiments are described using the proposed framework for static malware classification, in which feature optimization is performed and ensemble learning is used.
In the Conclusion, a summary of the results obtained in the conducted research is made and some directions for future research are indicated.
I have no critical remarks on the dissertation in terms of methodology.

Publications
The dissertation work has **4 publications** that are co-authored. Three of them are in publications with an impact rank (SJR) in the Q4 quartile of Scopus. So far, there have been 8 noted citations of the publications. The publications are indicative of the personal contribution of the doctoral student. They cover the minimum national requirements for acquiring the educational and scientific degree "Doctor". In addition, a list of three articles accepted for publication is presented. The publications presented give reason to assume that the research has the necessary publicity.

CONTRIBUTIONS

The **results** obtained can be briefly systematized in the following **contributions**:
The results obtained are systematized in the following contributions:

1) Two mathematical models are proposed, through which a selection of software for a suitable virtual machine can be made for the purposes of experimental testing for malware detection.

2) An improved static analysis approach for malware detection is proposed by optimizing feature extraction by combining different machine learning algorithms. Tests conducted with the proposed hybrid algorithms show better performance.

3) A framework for static malware classification is proposed, which uses feature optimization and ensemble learning. The results show that the false positive analysis for the ensemble is significantly lower than that of individual models.

4) Self-aware malware classification is proposed by routing models based on a trust system for feature selection and explainability. The routing logic increases the power of the ensemble with trust-based decisions and provides a flexible mechanism useful for both historical and contemporary malware features.

5) A trust-based adaptive framework for malware classification with feedback corrections is proposed. This framework is both adaptive and robust, as it includes a self-aware model classifier that uses adaptive logic to automatically choose between traditional and contemporary model layers by measuring the reliability of the prediction. The integration of explainability contributes to confidence in the decisions, which is increased by more information about the features from a local and global perspective.

I accept the formulated contributions. I believe that the results presented sufficiently cover the scope of the set goals and objectives.

The abstract in Bulgarian is 45 pages long and presents the dissertation work.
The abstract in English is 43 pages long and presents the dissertation work.

CRITICAL REMARKS

1) When introducing the metrics for evaluating the performance of the respective algorithms on page 24 of the dissertation, the corresponding formulas for each metric should also be presented.

2) In section 2.1.1. of the dissertation, three evaluation criteria are listed when deciding on choosing software for a virtual machine for detecting malware. However, four criteria are then mentioned (see page 40).

3) Some spelling errors have been noticed in the dissertation, which can be easily fixed.

COMMENT

The results obtained in the dissertation demonstrate the high performance of the developed application "Shipka Guard". It should find wide practical implementation, for example, in cybersecurity systems in state and scientific organizations, in universities, as well as in industrial enterprises. In this regard, I recommend conducting advertising demonstrations of the application's operation and its presentation at technical exhibitions and fairs.

FINAL COMPLEX ASSESSMENT

The technical critical remarks made do not belittle the contributions of the dissertation. I believe that the presented dissertation work meets the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria. The achieved results give me grounds to confidently propose to the esteemed Scientific Jury esteemed Scientific Jury to award Iliyan Magdalenov Barzev the educational and scientific degree "Doctor" in the professional field - 4.6 "Informatics and Computer Science", Doctoral Program "Informatics" for the dissertation on the topic "Research and Analysis of the Possibilities for Detection of Malware through Machine Learning".

06.03.2026.
Sofia city

На основание
331Д