
Time-Critical Detection of Ransomware Attacks in Centralized File Storage Environments by Investigating the Application Potential of Machine Learning

Theses of the Doctoral (PhD) Dissertation

Gábor Arányi

Supervisor: Dr. Veronika Szücs

University of Pannonia
Faculty of Information Technology
Doctoral School of Information Science and Technology

2026

Motivation and Objectives

In parallel with the increasing prevalence of digitalization, the operation of organizations, institutions, and enterprises is becoming increasingly dependent on information systems. Consequently, digital data assets and their associated software environments have become among the most important technological assets of many organizations. The growing complexity of information systems, deficiencies in users' security awareness, shortages of professional expertise, and outdated or inadequately maintained systems all contribute to greater exposure to cyberattacks. Ransomware attacks represent perhaps one of the most severe cybersecurity threats today, a risk further intensified by the continuous evolution of attack techniques and the proliferation of Ransomware-as-a-Service (RaaS) platforms. Attacks that previously required a high level of technical expertise have become substantially easier to execute, while healthcare and educational institutions, as well as micro, small, and medium-sized enterprises, have become increasingly vulnerable targets owing to outdated IT infrastructures, limited resources, and the lack of available expertise.

Defensive solutions such as next-generation (NG) firewalls, intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) platforms, data loss prevention (DLP) software, and antivirus solutions play an important role in protecting IT infrastructures. Nevertheless, when deployed in isolation, they are often insufficient to fend off ransomware attacks effectively and minimize their impact. Protection frequently focuses on the network perimeter and client devices, while the security of centrally stored data assets receives less attention, despite the critical importance of monitoring operations performed on stored data and enabling rapid data recovery. Protecting critical data therefore requires cost-effective and easily integrable solutions capable of ensuring rapid detection of ransomware attacks, secure data storage, and data restoration working independently of endpoint protection systems.

One objective of the research is the conceptual development of a multilayer, platform-independent protection model, the Anti-Ransomware Defense System (ARDS), which operates independently of endpoint protection, can be integrated seamlessly, and provides comprehensive protective capabilities. A further key objective is to develop a file-server-side protection solution as a component of the ARDS model. The proposed solution demonstrates the practical applicability of the concept through reference-based performance evaluation and is capable of near-real-time, resource-efficient detection of ransomware attacks using a supervised machine learning method based on sequences of file operations.

New Scientific Results

The following list summarizes my new scientific results in four theses.

Thesis 1

It can be demonstrated that the file-transfer performance of heterogeneous client–server architectures can be compared objectively using a pairwise-defined, dynamic, reference-based relative performance metric, where comparability is ensured by the ratio of transfer speeds measured for the same sequence of operations rather than by absolute performance values.

Substantiation of Thesis T1

The investigation of heterogeneous client–server architectures showed that absolute file-transfer performance values may differ significantly depending on the software environment, even when the hardware environment and file contents are identical. This phenomenon complicates the objective comparison of different configurations because absolute measurement results cannot be clearly separated from environment-specific characteristics. To address the comparability problem of performance measurements conducted in heterogeneous environments, I introduced a novel, pairwise-defined, dynamic, reference-based relative performance metric. The metric is platform-independent, provides a reproducible measurement procedure, and can be generalized provided that an appropriate reference system is defined. During the measurements, the metric was based on the ratios of transfer speeds measured for identical file-transfer directions (read and write). Thus, rather than treating absolute transfer speeds as the primary basis of comparison, it evaluates the performance of each examined configuration relative to a predefined reference system. This reduces the distortion caused by platform-specific characteristics and enables the file-transfer performance provided by different operating systems, file systems, and data-protection mechanisms to be evaluated on a common scale. Furthermore, the proposed method enables performance changes between configurations, such as those resulting from system tuning or the introduction of protective functions, to be monitored consistently.

The scientific contribution of the research lies not solely in defining the performance of a FreeBSD-based configuration, but in developing a generalizable, reference-based evaluation method that offers an objective comparison method of heterogeneous service environ-

ments. Using this method, the performance of different operating systems, file systems, encryption procedures, and data-storage architectures can be assessed by means of a unified metric. The approach is therefore applicable not only to the configurations examined in the present research but also provides a general methodological framework for future comparative system studies.

The relative performance metric defined during the investigations yielded consistently interpretable results for all examined configurations and enabled the objective comparison of different operating systems, file systems, and data-protection configurations. The results obtained in the various measurement series confirmed that the reference-based metric is suitable for quantitative tracking of performance changes, thereby supporting the methodological proposition formulated in the thesis.

Author's publications supporting Thesis T1:

[S1] Szücs, V., Arányi, G., & Dávid, Á. (2021). Introduction of the ARDS-Anti-Ransomware Defense System Model-Based on the Systematic Review of Worldwide Ransomware Attacks. *APPLIED SCIENCES-BASEL*, 11(13). <http://doi.org/10.3390/app11136070> - SJR Q2, WoS Q2 IF: 2.838

[S2] Arányi, G.; Vathy-Fogarassy, Á.; Szücs, V. Evaluation of a New-Concept Secure File Server Solution. *Future Internet 2024*, MDPI, 16, 306. <https://doi.org/10.3390/fi16090306> - SJR Q2, WoS Q2 IF: 3.6

Thesis 2

It can be demonstrated that, in a centralized file-server environment implemented in a virtualized client–server infrastructure, timestamped, time-series-continuous server-side file-operation log data can be transformed, through appropriate pre-filtering, normalization, and aggregation into one-second time windows, into a structured time-series representation. On this basis, certain machine learning models are capable of efficiently detecting, in near real time and without client-side information, the intensive file-operation activity generated by ransomware employing full encryption.

Substantiation and Limitations of Thesis T2

The study covered classical ransomware variants employing full encryption (Ryuk, WannaCry, NotPetya, LockBit, and TeslaCrypt), which generate intensive file-creation, renaming, and deletion operations during execution. Measurements were conducted in a vir-

tualized client–server infrastructure providing centralized file services. The analysis was performed on a time-series-continuous dataset aggregated into one-second time windows, with the reference state defined on the basis of file-usage patterns typical of office users. The measurements demonstrated that timestamped file-operation log data generated on the file-server side alone contain sufficient information to identify changes in intensity and patterns associated with the ransomware activities examined. During normal operation, the number and temporal distribution of creation, renaming, and deletion operations formed a stable reference state, whereas ransomware activity produced an order-of-magnitude change in intensity and a characteristic deviation in pattern within a short period. As a result of pre-filtering and time-window aggregation, the log data were represented not as a raw set of events but as a structured, time-series-continuous numerical representation. This representation provided directly usable input for supervised machine learning models, establishing the basis for the automated detection of ransomware activity. Based on event sequences aggregated in consecutive time windows, the temporal evolution of file-operation activity could be monitored continuously; consequently, the detection process could be interpreted as near-real-time monitoring rather than retrospective analysis.

The methodological contribution of the research is the development of a server-side, time-window-based data representation that relies exclusively on file-server log data and provides the input representation required for machine-learning-based detection of ransomware activity. The method is not tied to any specific machine learning algorithm and can therefore be used as input for various classification models.

The conclusions apply to centralized file-server environments in which file operations can be logged with timestamps and attackers perform an intensive file-system-level encryption process. The study did not cover ransomware variants that generate only minimal file-operation activity or do not employ encryption. The reference state was established under a typical office workload; therefore, investigating changes in user behavior during long-term operation and the generalizability of the method to newer ransomware families (concept drift) constitutes a further research direction. In addition, the timeframe of the present research did not permit validation of the method over an extended period. Its stability and adaptability during longer operational periods therefore require further empirical investigation.

Thesis 3

It can be demonstrated that, in the examined environment, normal user activity and the intensive file-operation patterns induced by ransomware employing full encryption can be treated as a binary classification problem and both can be detected effectively using classical and ensemble machine learning methods with a decision latency suited to the time-critical progression of the attack.

Substantiation of Thesis T3

In the course of the research, I developed a preprocessing procedure for timestamped file-operation log data generated on the file-server side. The procedure applies pre-filtering and aggregation into one-second time windows. As a result of data preparation, file-creation, renaming, and deletion operations were represented not as a raw sequence of events but as a structured, time-series-continuous numerical representation that could be used directly as input to supervised machine learning models.

The reference state was defined based on typical office file-usage patterns associated with different job roles. During normal operation, the intensity and temporal distribution of file operations remained within a stable range, whereas the examined ransomware variants (Ryuk, WannaCry, NotPetya, LockBit, and TeslaCrypt) produced an order-of-magnitude increase in intensity and a clearly distinguishable change in temporal patterns within a short period. These deviations appeared not as isolated events but as persistent behavioral patterns across consecutive time windows, enabling a clear distinction between normal periods and periods affected by an attack. Since the objective of the research was to detect the presence of ransomware activity rather than identify individual malware families, the detection task could be formulated as a binary classification problem. The investigations conducted on the structured data representation confirmed that both classical and ensemble machine learning models are capable of distinguishing between normal and attack-affected time windows. Following hyperparameter optimization, all examined models achieved a sensitivity above 0.84, while the XGBoost model outperformed the others with a value of 0.919. For the 209 attack-affected seconds in the test dataset, this corresponded to 192 correct detections. XGBoost also provided the most favorable trade-off among sensitivity, precision, and the false-positive rate and achieved the best result in the cost-based evaluation.

The measurements also confirmed that the time required for the decision-making process is by order of magnitude adequate for the time-critical detection of ransomware attacks. For the best-performing XGBoost model, the time required to perform classification on input

data corresponding to 392 time windows was 0.93 ms, while values between 0.19 ms and 3.41 ms were measured for the other models. Time-window-based processing and the low computational requirements of the models allowed the classification result to become available virtually immediately after data collection, while the resource demand remained within the capacity of general-purpose servers used in small- and medium-sized enterprise environments.

The investigations therefore demonstrate that, in the examined environment, normal user activity and the intensive file-operation patterns induced by file-system-level ransomware can be treated as a binary classification task and, with appropriate data preparation, can be detected effectively using classical and ensemble machine learning methods with a decision latency suited to the time-critical progression of attacks. The conclusions apply to the full-encryption ransomware variants included in the study and to centralized, virtualized file-server infrastructures. The reference state was established under a typical office workload. The research did not address changes in user behavior occurring during long-term operation or validate the method over periods of several months or years. Furthermore, the generalizability of the method to subsequently emerging ransomware variants with substantially different operational characteristics was not investigated (concept-drift analysis); these issues therefore constitute directions for further research.

Author's publications supporting Theses T2 and T3:

[S1] Szücs, V., Arányi, G., & Dávid, Á. (2021). Introduction of the ARDS-Anti-Ransomware Defense System Model-Based on the Systematic Review of Worldwide Ransomware Attacks. *APPLIED SCIENCES-BASEL*, 11(13). <http://doi.org/10.3390/app11136070> - SJR Q2, WoS Q2 IF: 2.838

[S3] Arányi, G.; Miseta, T.; Szücs, V. Ransomware Detection Based on Server-side File Operation Logs using Machine Learning. *Journal on Information Security, Advances in Information Forensics and Security*; Springer, 2025. <https://doi.org/10.1186/s13635-026-00229-7> - SJR Q2, WoS Q2 IF: 2.1

Thesis 4

It can be proven that, in order to assess the practical usability of the classical and ensemble machine learning models examined, no single performance metric is sufficient on its own, and the combined use of accuracy, F1 score, sensitivity, specificity, confusion matrix, and cost-based evaluation together ensure a comprehensive comparison that takes practical considerations into account.

Substantiation of Thesis T4

The investigations conducted during the research demonstrated that the practical applicability of ransomware-activity detection cannot be assessed on the basis of a single performance metric. Particularly in the presence of an imbalanced class distribution, accuracy alone may provide a misleading indication of model performance because it does not reflect the differently weighted consequences of the various types of classification error. Analysis of the confusion matrix made it possible to determine the proportions of false-positive and false-negative decisions, while sensitivity and specificity highlighted the trade-off between detection capability and false alarms. The F1 score served as a composite indicator that took all of these factors into account; however, it too proved insufficient on its own for assessing practical applicability. Cost-based evaluation enabled the performance of the models to be compared by assigning weights to improper classification outcomes. It thereby illustrated the extent of the damage that individual classification errors could cause in a real-world environment. The results indicate that the joint application of accuracy, F1-score, sensitivity, specificity, the confusion matrix, and cost-based evaluation represent a suitable approach for comparing the performance of different machine learning models and assessing it in a manner that is meaningful from the perspective of practical deployment. The scientific novelty of the research lies in demonstrating that the evaluation of models used for ransomware detection can be treated as a multicriteria decision problem, in which the practical suitability of the models can be substantiated through the integrated application of classical performance metrics and cost-based evaluation.

Author's publication supporting Thesis T4:

[S3] Arányi, G.; Miseta, T.; Szücs, V. Ransomware Detection Based on Server-side File Operation Logs using Machine Learning. *Journal on Information Security, Advances in Information Forensics and Security*; Springer, 2025. <https://doi.org/10.1186/s13635-026-00229-7> - SJR Q2, WoS Q2 IF: 2.1

Application of the New Scientific Results

The results of the research may contribute to improving protection against ransomware for resource-constrained micro, small, and medium-sized enterprises, as well as for other organizations employing centralized data storage. The reference-based performance-evaluation method developed in the research can be applied as a general methodological tool for comparative studies of heterogeneous IT environments. In parallel, the machine-learning-based detection approach relying on server-side file-operation logs may complement existing backup and recovery solutions, support the early detection of ransomware attacks, and enable rapid incident response. Further research may include validation using malware families that employ advanced encryption strategies, evaluation in real operational environments, investigation of the applicability of deep learning models, and the use of detection events to support automated backup and recovery processes. Incorporating the analysis of read operations constitutes another potential research direction and may facilitate the earlier detection of attacks involving data exfiltration.

Further Publications

Personal researcher profile in the Hungarian Scientific Bibliography (MTMT):
<https://m2.mtmt.hu/api/author/10069952>

Szücs, Veronika ; Arányi, Gábor ; Dávid, Ákos; Security Awareness of HCI in DigitAll Reality, ACTA POLYTECHNICA HUNGARICA 22 : 6 pp. 9-23. , 15 p. (2025).DOI:

10.12700/APH.22.6.2025.6.2 , SJR Q2, WoS Q2 IF: 1,8

Szücs, V., Arányi, G., & Dávid, Á. (2021). Security awareness of HCI in DigitAll Reality. In 12th IEEE International Conference on Cognitive Infocommunications (CogInfoCom 2021) (pp. 1095–1096)

Szücs, V., Arányi, G., & Vathy-Fogarassy, Á. (2022). Security of IT systems in healthcare institutions. Healthcare Informatics Before and After COVID-19 - Proceedings of the 35th Neumann Colloquium (pp. 45–50)

Arányi, G., & Szücs, V. (2023). IoT related security issues and black-box testing experiences in a smart lighting system. International Scientific Journal Security & Future, VII(2), pp. 61–64.

Arányi, G., Kocsis, T., Marsi, T., & Szarvák, A. (2020). Cyber Threats. Budapest: University of Public Service, Institute of Public Administration Further Training