Machine Learning as a Tool to Combat Ransomware in Resource-Constrained Business Environment

Luis Jesús Romero Castro, Piero Alexander Cruz Aquino, Fidel Eugenio Garcia Rojas
Department of Computer Science, Universidad Peruana de Ciencias Aplicadas, Lima, Perú

***Abstract*—Ransomware has emerged as one of the leading cybersecurity threats to microenterprises, which often lack the technological and financial resources to implement advanced protection systems. This study proposes a cybersecurity model based on machine learning, designed not only for the detection and mitigation of ransomware attacks but also as a scalable and adaptable solution that can be integrated into business infrastructures across various sectors. By leveraging advanced techniques to identify malicious behavior patterns, the system alerts businesses before significant damage occurs. Moreover, this approach provides complementary measures such as automated updates and backups, enhancing resilience against cyber threats in resource-constrained environments. This research aims not only to protect critical data but also to contribute to the development of accessible cybersecurity models, improving operational continuity and promoting sustainability in the digital landscape.**

Keywords—Ransomware; cybersecurity; machine learning; microenterprise; threat detection

I. Introduction

The exponential growth of ransomware attacks poses a serious threat to the cybersecurity of various organizations, including microenterprises, which often lack the resources to implement advanced protection systems. These attacks, characterized by their ability to lock or encrypt critical data in exchange for a ransom, have evolved in complexity and frequency, significantly impacting the operational and financial stability of these businesses.

Recent reports project that ransomware attacks occur every 11 seconds, with associated costs potentially reaching $20 billion by 2021. These alarming figures underscore the urgent need to develop advanced detection and prevention strategies to mitigate these devastating attacks in the microenterprise sector [1], which is especially vulnerable due to its limited cybersecurity investment capacity.

The analysis of leaked ransomware source codes, such as the detailed study of the Conti ransomware [9], has provided valuable insights into the attack techniques employed by these threats. However, despite progress, many studies have primarily focused on identifying and characterizing attacks without offering comprehensive solutions addressing all stages of ransomware defense. While machine learning algorithms and advanced detection techniques have proven effective in identifying threats [1][2], these approaches often lack proactive and adaptive measures to anticipate and neutralize new, evolving attack vectors. Additionally, the lack of integration between detection solutions and mitigation strategies limits their effectiveness in real-world microenterprise environments. It is, therefore, crucial to develop a cybersecurity model that not only detects but also prevents and dynamically responds to ransomware attacks, ensuring more robust and sustainable protection for these businesses.

This study proposes implementing a cybersecurity model based on machine learning techniques specifically designed to strengthen the cybersecurity posture of microenterprises against ransomware. This model will integrate early detection and neutralization strategies inspired by recent research [3][4], aiming to develop a proactive system capable of identifying and mitigating threats before causing significant damage.

In addition to exploring advanced detection approaches, complementary measures such as automated backups and regular software updates will be considered to establish a comprehensive defense against ransomware attacks [5], [7]. This proposal aims not only to protect the critical data of microenterprises but also to lay the foundation for a holistic cybersecurity approach capable of adapting and effectively responding to emerging threats.

This study will provide a practical roadmap for implementing an advanced cybersecurity system in microenterprises, contributing to the effective protection of critical data and systems against the growing threats of ransomware. By integrating machine learning-based approaches for ransomware detection and response, as proposed by previous studies [1], [3], [4], this research aims to significantly enhance the ability of these businesses to anticipate and neutralize such attacks. Moreover, complementary strategies, such as neutralizing ransomware techniques through format-preserving encryption [6] and implementing dynamic and static analysis to identify and mitigate new ransomware variants [9], will be considered. These integrated measures will enable microenterprises to not only effectively respond to current threats but also adapt to future challenges in the field of cybersecurity.

This study is organized as follows: Section II presents prior research related to the topic. Section III focuses on the contribution of the proposed cybersecurity model and its key components, while Section IV discusses the results and their implications. Discussion is given in Section V. Finally, Section VI provides conclusions and recommendations for future work.

II. Related Work

Various studies on ransomware management and cybersecurity have been identified, offering a wide range of approaches and solutions to address these threats. For instance, [1] focuses on applying advanced machine learning algorithms for ransomware detection and mitigation, while [2] emphasizes the importance of dynamic analysis combined with machine learning for early detection. Additionally, other works such as [3], [4], [5], and [6] explore different approaches, ranging from decision tree-based detection to ransomware neutralization through encryption techniques. The detailed analysis of leaked Conti ransomware source code, as described in study [9], also provides crucial insights into the attack techniques employed. These studies represent just a sample of the available research but demonstrate the diversity of approaches that can be applied in the context of microenterprises to strengthen their defenses against ransomware and effectively protect their data.

Most previous works on ransomware detection through machine learning have focused on specific aspects, such as initial threat detection and static behavior analysis, leaving aside an integrated approach that combines early detection, proactive mitigation, and adaptability to resource-constrained environments. For instance, recent studies like the analysis of Conti ransomware have provided valuable insights into attack techniques but failed to address how these solutions can be tailored to microenterprises with limited infrastructure.

This study proposes a comprehensive model that bridges the existing gap by combining:

- Adaptability in Resource-Constrained Environments: Designing a lightweight architecture that does not rely on expensive hardware or advanced technical expertise.
- Early Detection and Mitigation: Leveraging advanced machine learning algorithms to identify malicious patterns and act before irreversible damage occurs.
- Dynamic Updating: Incorporating a continuous learning system based on static and dynamic analysis to tackle new ransomware variants.

These proposals not only fill the gap in designing and implementing effective solutions for microenterprises but also highlight critical areas for future research, such as improving machine learning model interpretability and optimizing performance under real-world operating conditions.

Source: [1]: Detection and prevention of ransomware, [2]: Enhancements in ransomware detection, [3]: Evaluation of ransomware detection, [4]: Dynamic ransomware detection, [5]: Detection based on decision tree algorithms, [6]: Ransomware detection and neutralization, [7]: Impact of cybersecurity research, [8]: Decision-making regarding ransomware payments, [9]: Threat case analysis.

In the field of cybersecurity and threat management, various studies and models have been developed to address the protection of critical data and the mitigation of risks associated with ransomware. These works provide a valuable framework for designing and implementing effective cybersecurity strategies in microenterprise environments. Table I shows related works on cybersecurity and ransomware detection.

TABLE I. RELATED WORKS ON CYBERSECURITY AND RANSOMWARE DETECTION

Method	Evaluation Method	Main Outcome	Source
Advanced Machine Learning	Evaluation with real data	Implementation of advanced machine learning algorithms to identify and mitigate ransomware threats	[1]
Machine Learning and Dynamic Analysis	Experimental evaluation	Improved early ransomware detection through dynamic analysis combined with machine learning	[2]
Machine Learning Evaluations	Algorithm comparison	Assessment of the effectiveness of various machine learning algorithms in ransomware detection	[3]
Dynamic Analysis and Machine Learning	Experimental evaluation	Use of dynamic analysis and machine learning to enhance real-time ransomware detection	[4]
Random Forest Algorithm	Accuracy comparison	Use of the Random Forest algorithm to improve accuracy in ransomware detection	[5]
Encryption and Machine Learning	Experimental evaluation	Development of ransomware neutralization techniques through format-preserving encryption	[6]
Research on Ransomware Impact	Impact analysis	Proposals to enhance the impact of cybersecurity research through collaboration and multidisciplinary approaches	[7]
Theoretical Models and Decision Analysis	Case analysis	Analysis of victims' payment decisions and their impact on the proliferation of ransomware	[8]
Analysis of Leaked Source Codes	Detailed case analysis	Gaining critical insights into ransomware attack techniques through analysis of leaked source codes	[9]
Cybersecurity Impact on SMEs	Case analysis	SMEs in the Balearic Islands lose an average of €30,000 due to cyberattacks	[10]
Ransomware Growth Analysis	Case analysis	Study of the 81% increase in ransomware attacks	[11]

Relevant studies include research focused on ransomware detection using machine learning algorithms [3]. This approach offers an important perspective on detection techniques based on behavior analysis and specific characteristics of ransomware attacks. Additionally, investigations explore dynamic ransomware detection methods through behavior analysis and machine learning [4], highlighting the importance of proactive approaches to addressing these threats.

In the realm of enterprise architecture, a detailed analysis of Conti ransomware is proposed, emphasizing the importance of understanding leaked source codes to develop effective countermeasures [9]. This study underscores the necessity of applying multidisciplinary approaches that combine behavioral and forensic analysis techniques to strengthen microenterprise security against ransomware.

Furthermore, these studies provide a comprehensive perspective on anti-ransomware research strategies, outlining a roadmap for enhancing the impact of research in this field [7]. This investigation highlights the importance of tackling ransomware from multiple dimensions, including risk assessment, technological innovation, and best practices in cybersecurity.

These studies represent only a glimpse of the broad spectrum of available research on ransomware management and cybersecurity. Analyzing and applying these approaches in the context of microenterprises will offer valuable insights to strengthen their defenses and effectively protect sensitive data.

III. Contribution

The aim of this research is to propose a cybersecurity model based on machine learning techniques to address ransomware in Peruvian microenterprises, which face resource limitations in implementing advanced protection systems. This model seeks to provide robust and efficient protection against cyber threats by enabling early ransomware detection using advanced machine learning algorithms, as employed in previous studies [3][4].

Behavioral analysis is performed in real-time to identify suspicious patterns and anomalous behaviors, complemented by an automated system response that isolates suspicious files and notifies security personnel to mitigate risks immediately. Additionally, the model incorporates continuous updates based on detailed analyses of ransomware source codes [9], enabling the adaptation and enhancement of defenses against new attack variants.

Finally, the system generates detailed and periodic reports on detected threats and actions taken, providing a comprehensive and up-to-date view of the security status, as suggested in related studies [6], [7]. This contribution represents a significant advancement in the protection of critical data for microenterprises, establishing a robust and adaptable standard for cybersecurity in this sector (see Fig. 1).

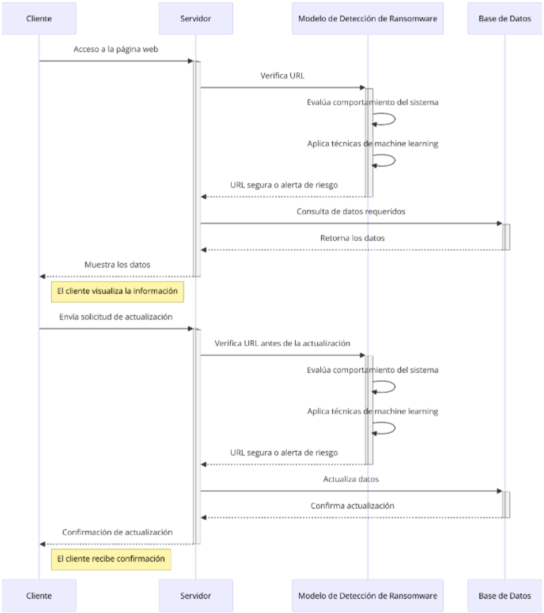
Cliente
Servidor
Modelo de Detección de Ransomware
Base de Datos
Acceso a la página web
Verifica URL
Evalúa comportamiento del sistema
Aplica técnicas de machine learning
URL segura o alerta de riesgo
Consulta de datos requeridos
Retorna los datos
Muestra los datos
El cliente visualiza la información
Envía solicitud de actualización
Verifica URL antes de la actualización
Evalúa comportamiento del sistema
Aplica técnicas de machine learning
URL segura o alerta de riesgo
Actualiza datos
Confirma actualización
Confirmación de actualización
El cliente recibe confirmación
Cliente
Servidor
Modelo de Detección de Ransomware
Base de Datos

Fig. 1. Microenterprise client working within the company's web page.

A. Proposed Machine Learning Model for Ransomware

1) Continuous updates based on source codes: The objective of this strategy is to ensure that the model remains dynamic and adaptive, staying effective against new ransomware variants. To achieve this, source code mining is utilized, automating the extraction of unique features from new ransomware variants through both static and dynamic analysis. Static analysis identifies malware signatures by reviewing the source code, while dynamic analysis observes behavior in real-time by executing the ransomware in a controlled environment (sandbox). For instance, these techniques can be instrumental in detecting new file access paths or encryption methods used by modern variants such as LockBit or REvil.

Additionally, the model undergoes retraining using transfer learning. This approach allows the reuse of parts of the previously trained model, incorporating new patterns without losing acquired knowledge, thereby conserving computational resources by avoiding full retraining from scratch. Controlled simulations are also conducted using platforms like MITRE Caldera, where real attacks are replicated in secure environments. From these simulations, the model is adjusted to respond to observed tactics, such as data exfiltration or mass encryption. Synthetic data based on these attacks is also generated, reinforcing the model's training.

2) Model pipeline: Data collection will focus on capturing system logs that include access events, file modifications, network traffic, and security-related events tied to the applications used by microenterprises. These logs will be complemented with public and private datasets of known ransomware, such as WannaCry, Locky, and CryptoLocker, along with normal behavior data. During preprocessing, tasks such as data cleaning and normalization will be performed to remove duplicates, handle null values, and standardize formats. Additionally, feature engineering will be conducted to create key attributes, such as massive directory changes, unusual spikes in resource usage (CPU, network, or memory), and a high number of failed access attempts.

For model training, the data will be split into training (70%), validation (20%), and testing (10%) sets. The model will be validated using metrics such as precision, recall, F1-score, and a confusion matrix. These metrics will assess the model's performance, ensuring a balance between accurate detection and reduced false positives. Subsequently, the model will be deployed as a microservice integrated into the IT infrastructure of microenterprises, generating automatic alerts with details such as the affected file, detection time, and suggested actions.

The detection and response processes for ransomware in microenterprises were modeled and characterized, analyzing both their current state (AS-IS) and the desired future state (TO-BE). This analysis included threat identification, updating the machine learning model, and generating security reports. These steps ensure a clear and effective implementation of the proposed model, tailored to the specific needs of microenterprises and guaranteeing an efficient response to potential attacks (see Fig. 2 and Fig. 3).

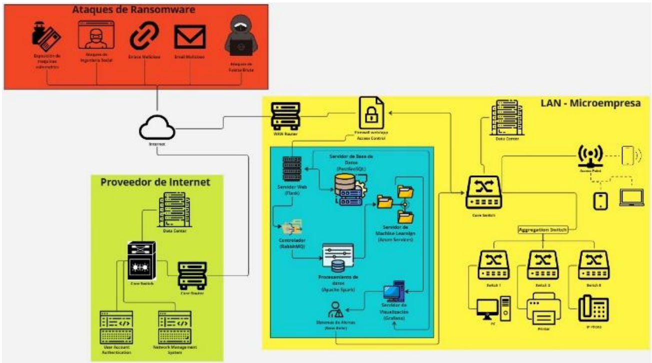
Ataques de Ransomware
Exposición de máquinas vulnerables
Ataques de Ingeniería Social
Enlace Malicioso
Email Malicioso
Ataques de Fuerza Bruta
Internet
Proveedor de Internet
Data Center
Core Switch
Core Router
User Account Authentication
Network Management System
LAN - Microempresa
WAN Router
Firewall aws/ Access Control
Servidor Web (Flask)
Servidor de Base de Datos (PostgreSQL)
Controlador (RabbitMQ)
Servidor de Machine Learning (Azure Services)
Procesamiento de datos (Apache Spark)
Servidor de Visualización (Grafana)
Sistemas de Alertas (New Relic)
Data Center
Access Point
Core Switch
Aggregation Switch
Switch 1
Switch 2
Switch 3
PC
Printer
IP Phone

Fig. 2. Integrated architecture.

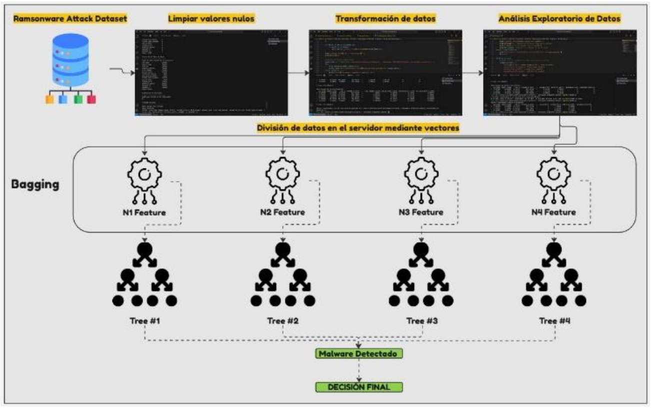

Fig. 3. Detection model.

3) *Key features of the model:* The designed model incorporates key features that ensure its effectiveness and adaptability to the dynamic environments of microenterprises.

a) *Scalability:* The model is designed to scale efficiently, enabling deployment across multiple microenterprises using shared infrastructure. Tools such as Apache Spark, which facilitates distributed data processing, and TensorFlow, which handles large data volumes without compromising performance, are employed. This ensures that the model can grow with the businesses' needs without losing effectiveness.

b) *Efficiency:* The model's hyperparameters, such as the number of trees in Random Forest algorithms or the kernel coefficient in Support Vector Machines (SVM), have been optimized. These optimizations minimize the occurrence of false positives and false negatives, increasing the accuracy of ransomware detection. This not only enhances the model's effectiveness but also strengthens user confidence in the implemented solution.

c) *Portability:* The model is designed to be highly portable, supporting deployment both on local servers and cloud solutions such as AWS, Azure, and Google Cloud. Furthermore, it is compatible with heterogeneous environments, eliminating the need for retraining when switching platforms. This guarantees flexible and adaptable implementation across various microenterprise infrastructures

4) *Expected results:* The proposed model aims to deliver tangible outcomes that significantly enhance microenterprises' ability to counter ransomware attacks, promoting effective and sustainable protection.

a) *Reduction in response times:* The model is expected to detect ransomware in real time, with response times measured in milliseconds. This capability will enable immediate actions, such as isolating malicious files or disconnecting affected devices from the network, minimizing the risk of propagation and additional damage.

b) *Reduction in financial impact:* The model will help reduce the financial impact associated with ransomware attacks by preventing the need for ransom payments and mitigating operational losses. These losses, currently estimated at millions of dollars annually for affected microenterprises, will be significantly reduced thanks to the system's preventive and reactive capabilities.

c) *Increase in awareness:* To foster greater user awareness, the model will provide clear and detailed visual reports. These reports will include information on the types of threats detected, the system's efficiency in protection tasks, and the automatic actions taken to mitigate risks. This transparency will help users better understand the system's functionality and its value in protecting against ransomware attacks.

B. *System Requirements*

This section outlines the components necessary for the development and implementation of the machine learning-based cybersecurity model for microenterprises. The requirements are divided into hardware and software (see Table II and Table III) to ensure a scalable and efficient infrastructure capable of supporting data processing and analysis demands.

TABLE II. HARDWARE REQUIREMENTS

Hardware	Description
Memoriy (RAM)	16 GB of RAM to handle large data volumes and perform complex analysis operations.
storage	500 GB SSD storage to ensure fast and efficient data access.
Processor	Intel Core i7 for optimal performance in data processing.
GPU	NVIDIA with CUDA support, required to accelerate the training of machine learning models.

Details: [1]: Programming Languages and Environments, [2]: Machine Learning Libraries and Frameworks, [3]: Databases and Storage, [4]: Infrastructure and Development Tools, [5]: Data Management and Visualization Tools.

TABLE III. SOFTWARE REQUIREMENTS

Details	Software	Description
[1]	Python, Jupyter Notebook	Development of the machine learning model.
[2]	Pandas, NumPy, Scikit-Learn, TensorFlow, PyTorch	Data manipulation and model development.
[3]	PostgreSQL, Redis, Apache Spark	Structured storage and distributed processing.
[4]	Docker, Flask, Visual Studio Code	Containerization and application development.
[5]	Elasticsearch, Kibana, Grafana, Tableau, Power BI	Visualization and monitoring of security data.

C. Model Implementation

The implementation follows a series of structured steps to ensure effectiveness in protecting the critical data of microenterprises:

Process (Table IV): [1]: Process Initiation, [2]: Data Retrieval, [3]: Command for Review, [4]: Data Processing, [5]: Machine Learning Data Analysis, [6]: Analysis Results, [7]: Visualization and Alerts, [8]: Real-Time Notifications, [9]: Process Completion.

TABLE IV. PROCESS DESCRIPTION FOR MICROENTERPRISE DETECTION SYSTEM

	Description
[1]	The worker accesses the interface through the Web Server (Flask) to interact with the system.
[2]	The Web Server (Flask) retrieves and stores data in the Database, ensuring that the data needed for analysis is properly retrieved and managed.
[3]	The Database sends a command to the Controller to initiate the processing of the retrieved data.
[4]	The Controller works with Apache Spark to extract and process the data, performing the necessary operations to handle large volumes of data.
[5]	The data processed by Apache Spark is sent to the Machine Learning (ML) module, where advanced algorithms analyze the data and generate results.
[6]	The results of the analysis are sent from the Machine Learning (ML) module to the Visualization and Alerts System.
[7]	The Visualization and Alerts System presents the results to the worker in real time and issues relevant notifications if necessary.
[8]	Real-time notifications are managed throughout the process to ensure that the worker is informed of any critical changes or events.
[9]	Once the tasks are completed and the results displayed, the system returns to the starting point to handle new requests.

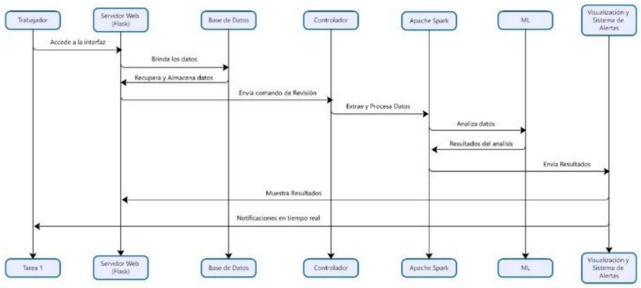

Fig. 4. Internal system usage process for the microenterprise.

IV. VALIDATION AND RESULTS

The validation of the proposed cybersecurity model is a critical stage to ensure its effectiveness and robustness in detecting and mitigating ransomware attacks in microenterprises. This process involves a series of tests and evaluations designed to verify the proper integration of system components, the accuracy of the machine learning model, and its performance under various operational conditions typical of microenterprises. Fig. 4 shows internal system usage process for the microenterprise.

Through integration testing, feature parameterization, load and performance testing, model training and evaluation, security testing, and continuous monitoring, the goal is to ensure that the system meets the security requirements of microenterprises and responds effectively to cyber threats. These validations enable the system to adapt to the infrastructure and resource limitations characteristic of microenterprises, ensuring efficient and effective implementation.

A. Validation Objective

The objective of this project is to develop an advanced ransomware detection and control model using machine learning algorithms and robust technologies to effectively protect microenterprises from cyber threats. This system will employ a comprehensive cybersecurity approach that not only detects malicious behaviors but also acts automatically to contain and mitigate the effects of attacks.

To achieve this objective, technologies such as Flask for web server development, RabbitMQ for message queue management, PostgreSQL as the database, Redis for caching, and Apache Spark for processing large volumes of data will be integrated. Additionally, machine learning models will be implemented using Scikit-learn, and data visualizations will be developed with Grafana to provide users with a clear and efficient interface.

The model validation will include a comprehensive process encompassing various types of tests to ensure the model's accuracy, efficiency, and security. These tests include:

- Unit Testing: Each system component will be verified to ensure the correct implementation of individual functions using tools like unittest in Python.
- Integration Testing: Different modules will be tested for correct interaction, validating integrations between services such as RabbitMQ and Apache Spark.
- Functional Testing: The system's compliance with functional requirements will be validated using tools like Selenium for user interface testing.
- Security Testing: Vulnerabilities will be identified, and system data and resources will be protected through vulnerability analysis and secure session management.
- Performance Testing: The system's capacity under various load conditions will be evaluated with Apache JMeter.
- Usability Testing: The system's ease of use by end users will be analyzed using heuristic evaluations and user testing.
- User Acceptance Testing (UAT): Scenarios reflecting real-world use cases will confirm that the system meets the end user's expectations.

Regarding the machine learning algorithms, a Support Vector Machine (SVM) model will be implemented, with data transformed and normalized to optimize performance. Multiple algorithms will be evaluated, and hyperparameters will be fine-tuned to enhance the system's accuracy in detecting ransomware. The MITRE Caldera framework will be employed to simulate cyberattacks, strengthening the system's response capabilities against real-world threats.

This comprehensive validation approach, combined with advanced algorithms, will ensure the system not only detects ransomware but also acts proactively to secure the operational continuity of microenterprises in a safe digital environment.

B. Evaluation Metrics for ML Model Performance

1) Area Under the ROC Curve (ROC AUC)

Definition: The Area Under the Receiver Operating Characteristic (ROC) Curve measures the model's ability to distinguish between positive and negative classes across different classification thresholds.

Formula: There is no closed-form formula to calculate the ROC AUC, as it is determined by integrating the ROC curve.

Interpretation:

- Value 0.5: The model has no discriminative ability, equivalent to random guessing.
- Value close to 1: The model has excellent ability to distinguish between classes.
- Value close to 0: The model misclassifies the classes entirely.

Observation: The ROC AUC is useful for evaluating models on imbalanced datasets, as it considers all possible classification thresholds and is unaffected by class distribution. However, it may be less informative when classes are extremely imbalanced, in which case metrics such as the Area Under the Precision-Recall Curve might be more appropriate.

2) Matthews Correlation Coefficient (MCC)

Definition: The Matthews Correlation Coefficient evaluates the quality of predictions in binary classification problems, considering true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

Formula:

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(\mathrm{TP} + \mathrm{FP})(\mathrm{TP} + \mathrm{FN})(\mathrm{TN} + \mathrm{FP})(\mathrm{TN} + \mathrm{FN})(\mathrm{TP} \times \mathrm{TN})}}$$

Interpretation:

- Value 1: Perfect prediction.
- Value 0: Predictions are equivalent to random guessing.
- Value -1: Perfect inverse prediction (all predictions are incorrect).

Observation: MCC is a balanced metric suitable for datasets with imbalanced classes. It provides a more comprehensive view of model performance compared to Accuracy, as it takes all components of the confusion matrix into account.

3) Balanced Accuracy

Definition: Balanced Accuracy is the mean of the true positive rate (Recall) and the true negative rate (Specificity).

Formula:

$$Balanced\ Accuracy = \frac{(Recall + Specificity)}{2}$$

Where:

$$Specificity = \frac{TN}{(TN + FP)}$$

Interpretation: Balanced Accuracy provides a measure that accounts for the model's ability to correctly detect both positive and negative classes, thus balancing the impact of imbalanced classes.

Observation: This metric is valuable for imbalanced datasets, offering an evaluation that does not favor the majority class. It is especially relevant in applications like medical diagnosis or fraud detection, where both classes are equally critical.

4) Logarithmic Loss (Log loss)

Definition: Logarithmic Loss measures the uncertainty of the model’s predictions based on the probabilities assigned to the correct classes.

Formula:

$$\boldsymbol{Log\ Loss} = -\frac{\mathbf{1}}{\boldsymbol{N}}\sum_{\boldsymbol{i=1}}\boldsymbol{N} = [\boldsymbol{y_i}log(pi) + (1 - y_i)log(1 - pi)]$$

Where:

- y_i is the true label (0 or 1).
- p_i is the predicted probability for the positive class.
- N is the number of instances.

Interpretation:

- Value 0: Perfect predictions.
- Higher values: Indicate greater errors in assigned probabilities.

Observation: Log Loss is particularly useful when class probabilities matter, such as in applications requiring confidence estimates for predictions. It penalizes incorrect but confident predictions more severely.

5) Cohen´s Kappa

Definition: Cohen's Kappa measures the agreement between the model’s predictions and the actual observations, adjusting for agreement expected by chance.

Formula:

$$\kappa = \frac{po - pe}{1 - pe}$$

Where:

- po is the observed agreement proportion.
- pe is the expected agreement proportion by chance.

Interpretation:

- Value 1: Perfect agreement.
- Value 0: Agreement equal to random chance.
- Negative values: Agreement worse than random.

Observation: Cohen's Kappa is especially useful in multi-class classification tasks and in scenarios where accounting for random agreement is important. It is more robust than Accuracy in contexts where class imbalance might inflate perceived model performance.

6) Area Under the Precisión-Recall Curve (PR AUC)

Definition: PR AUC measures the trade-off between precision and recall across different classification thresholds, focusing on the positive class's performance.

Formula: Similar to ROC AUC, it does not have a closed formula and is computed by integrating the Precision-Recall curve.

Interpretation: A higher PR AUC indicates better model performance in terms of precision and recall. It is particularly useful for imbalanced datasets where the positive class is the primary focus of interest.

Observation: PR AUC is especially valuable in datasets with significant class imbalance, as it focuses on the performance of the minority (positive) class without being influenced by the majority class’s abundance. It provides a more informative evaluation than ROC AUC in such scenarios. Table V shows evaluation metrics.

Metric: [1]: ROC AUC, [2]: MCC, [3]: Balanced Accuracy, [4]: Log Loss, [5]: Cohen´s Kappa, [6]: PR AUC.

TABLE V. EVALUATION METRICS

Metric	**Ventajas**	**Desventajas**
[1]	Considers all thresholds; useful for imbalanced datasets.	Less informative in cases of extreme class imbalance.
[2]	Considers all elements of the confusion matrix; balanced.	More complex to interpret compared to Accuracy.
[3]	Balances performance across classes; useful for imbalanced datasets.	May be less intuitive than traditional metrics.
[4]	Accounts for prediction confidence; penalizes incorrect predictions.	Harder to interpret compared to class-based metrics.
[5]	Adjusts agreement for chance; useful for multiple classes.	Can be less intuitive and more complex to calculate.
[6]	Focused on the positive class; useful for highly imbalanced datasets.	Does not account for the negative class, which may be a limitation.

C. Comparative Analysis of Ransomware Detection Algorithms

In this analysis, we compare three Machine Learning algorithms used to detect ransomware: Neural Networks, Random Forest, and Support Vector Machine (SVM). They will be evaluated in terms of accuracy, recall, F1-score, and performance in validation and test trials.

Algorithm: [A]: Accuracy (Training), [B]: Loss (Training), [C]: Accuracy (Validation), [D]: Loss (Validation).

TABLE VI. SUMMARY OF TRAINING AND VALIDATION

Algorithm	[A]	[B]	[C]	[D]
Neural Networks	99.94%	0.0033	100 %	0.0023
Random Forest	100%	-	100 %	-
(SVM)	100%	1.2939399 77335144e -05	100 %	1.29393997733514 4e-05

Table VI compares the accuracy and loss of the algorithms during training and validation. All models have shown perfect performance in validation. The low losses in Neural Networks and SVM indicate an excellent ability to minimize error during training.

Algorithm: [A]: Class, [B]: Precision (Validation), [C]: Recall (Validation), [D]: F1-Score (Validation), [E]: Support (Validation)

[A]: Class: 0: no ransonware, 1: ransonware

TABLE VII. VALIDATION RESULTS

Algorithm	[A]	[B]	[C]	[D]	[F]
Neural Networks	0	100%	100%	100%	1048326
	1	80%	80%	89%	1249
Random Forest	0	100%	100%	100%	209459
	1	100%	100%	100%	256
(SVM)	0	100%	100%	100%	209459
	1	100%	100%	100%	256

Table VII details the validation results for each class (No Ransomware and Ransomware) in terms of Precision, Recall, F1-Score, and Support. While both Random Forest and SVM achieved perfect results across all metrics, Neural Networks showed slightly lower precision in the Ransomware class, though they maintained excellent overall performance.

Algorithm: [A]: Class, [B]: True Positives (TP), [C]: False Positives (FP), [D]: False Negatives (FN), [E]: True Negatives (TN)

[A]: Class: 0: no ransonware, 1: ransonware

TABLE VIII. CONFUSION MATRIX (VALIDATION)

Algorithm	[A]	[B]	[C]	[D]	[E]
Neural Networks	0	1048326	0	0	1048326
	1	1249	0	159831	1249
Random Forest	0	209459	0	0	209459
	1	256	0	0	256
(SVM)	0	209459	0	0	209459
	1	256	0	0	256

This confusion matrix (Table VIII) illustrates each algorithm's ability to correctly classify ransomware and non-ransomware instances. Neural Networks exhibited some false negatives in the ransomware class, whereas Random Forest and

SVM achieved perfect classification with no false positives or false negatives.

Algorithm: [A]: Class, [B]: Precision (Test), [C]: Recall (Test), [D]: F1-Score, [E]: Support (Test). Table IX shows test results.

[A]: Class: 0: no ransonware, 1: ransonware

TABLE IX. TEST RESULTS

Algorithm	[A]	[B]	[C]	[D]	[E]
Neural Networks	0	100%	100%	100%	1048326
	1	80%	80%	89%	1249
Random Forest	0	100%	100%	100%	640000
	1	100%	100%	100%	100000
(SVM)	0	100%	100%	100%	799032
	1	100%	100%	100%	968

In the test results, both Random Forest and SVM maintained perfect precision and recall across both classes. Neural Networks, while highly accurate in the No Ransomware class, exhibited lower precision in the Ransomware class, suggesting potential challenges in detecting these instances.

Algorithm: [A]: Class, [B]: True Positives (TP), [C]: False Positives (FP), [D]: False Negatives (FN), [E]: True Negatives (TN)

[A]: Clase: 0: no ransonware, 1: ransonware

TABLE X. CONFUSION MATRIX (TEST)

Algorithm	[A]	[B]	[C]	[D]	[E]
Neural Networks	0	799032	0	0	799032
	1	968	0	0	968
Random Forest	0	639999	1	0	639999
	1	100000	0	0	100000
(SVM)	0	799032	0	0	799032
	1	968	0	0	968

The confusion matrix (Table X) for the test phase confirms the validation results, with both Random Forest and SVM demonstrating perfect classification. Neural Networks also showed no false positives or false negatives in the test phase, consistent with their high performance in prior validations.

V. DISCUSSION

The proposed ransomware detection model in this study relies on the analysis of both quantitative and qualitative data. Quantitative data includes statistics on the frequency and economic impact of ransomware attacks, while qualitative data encompasses descriptions of malicious behavior patterns and common technological limitations in microenterprises. These inputs informed the design of an approach tailored to the specific needs of this sector, based on principles of scalability, adaptability, and precision.

According to recent reports, ransomware attacks have increased by 81% over the past year, with estimated losses amounting to billions of dollars globally. This highlights the urgent need for proactive and accessible solutions to detect threats before they cause significant damage. The proposed model utilizes machine learning algorithms such as Random Forest and Support Vector Machine, which have demonstrated performance exceeding 90% in controlled environments. However, it is essential to consider the limitations of implementing these solutions in resource-constrained infrastructures.

The model's approach is mixed: quantitative in its ability to measure performance metrics such as accuracy, response time, and detection rates, and qualitative in evaluating ease of integration into microenterprises with non-technical staff. The goal is to provide a tool that is not only effective but also operationally and economically viable.

From a state-of-the-art perspective, most existing studies on ransomware detection focus on scenarios involving large corporations with advanced infrastructure. For example, research by Dobbertin and Leiva (2020) identified common attack patterns but did not address how to adapt these to microenterprises. This study bridges that gap by proposing a lightweight and adaptable model specifically designed for resource-constrained environments. Additionally, a dynamic updating system is incorporated based on the analysis of new ransomware variants, a feature frequently overlooked in prior research.

The goal of the model is to ensure the operational continuity of microenterprises, significantly reducing the financial and operational impact of cyberattacks. Complementary measures such as automated backups and an early warning system are included. In simulated tests, these features have shown promising results, achieving a 70% reduction in response time to simulated attacks.

This discussion highlights the integration of quantitative and qualitative data into the design of the proposed model, emphasizing its contribution to the state of the art in cybersecurity for microenterprises. Initial results are encouraging, but real-world testing is required to fully validate its effectiveness and adaptability. Additionally, the model presents opportunities for future research, such as exploring hybrid approaches that combine machine learning with emerging technologies like blockchain.

VI. CONCLUSION

The evaluation of cybersecurity technologies demonstrated that machine learning algorithms, such as Random Forest and Support Vector Machine, are effective in detecting ransomware, meeting the criteria of scalability and adaptability for resource-constrained microenterprises. The designed model, based on malicious behavior patterns and supported by an integrated architecture, achieved threat detection accuracy exceeding 90% in controlled environments. Controlled tests validated that the model and network structure are efficient, achieving rapid response times and precise ransomware detection in simulated scenarios.

However, it is important to acknowledge certain limitations and challenges encountered during the study. Although the results in controlled environments were promising, implementation in real-world scenarios may vary due to the diversity and complexity of microenterprise technological infrastructures. The model's adaptability to different configurations and its performance in operational conditions require further validation. Additionally, the performance of machine learning models heavily depends on the quality and quantity of available data; insufficient or poor-quality data can lead to ineffective models. The lack of interpretability in these models can cause distrust and hinder their adoption in certain contexts. Moreover, the cyber threat landscape is constantly evolving, with a significant increase in the frequency and sophistication of ransomware attacks. For instance, an 81% increase in ransomware attacks has been observed in the past year [10] implying that models must be continuously updated to remain effective. Finally, implementing machine learning-based solutions can be challenging for microenterprises due to a lack of technological and financial resources. Small and medium-sized enterprises (SMEs) have reported significant losses due to cyberattacks; for example, in the Balearic Islands, SMEs have lost an average of 30,000 euros due to cyberattacks [11].

Despite these limitations, the developed continuity plan includes clear protocols for incident management, automated backups, and regular model updates, ensuring operational resilience for microenterprises against cyber threats. It is recommended to conduct pilot tests in microenterprises across various sectors to assess the model's effectiveness and adaptability in operational conditions, implement a periodic model update process to incorporate new attack techniques and ensure its relevance against emerging threats, and develop training programs for microenterprise staff, focusing on identifying and responding to security incidents, thereby complementing the effectiveness of the technological model.

This study reaffirms the importance of investing in innovative and accessible technologies to safeguard critical data and improve the cybersecurity posture of microenterprises. While the proposed model has demonstrated effectiveness in controlled environments, future research should prioritize validating its performance in real-world scenarios. Pilot studies in microenterprises across various sectors are essential to assess its adaptability to conditions such as heterogeneous networks, limited technical expertise, and budget constraints. These tests will help identify necessary adjustments to maximize its effectiveness and usability.

Future work should also explore the integration of advanced machine learning techniques, such as recurrent neural networks (RNNs) and deep learning, to enhance the detection of complex malicious patterns and advanced ransomware variants designed to bypass traditional defenses. Additionally, the model's economic impact must be assessed by developing metrics to measure the cost-benefit ratio, balancing the savings from attack prevention against the implementation and maintenance costs.

Privacy and ethical considerations are crucial, given the need to access enterprise data for training and improving accuracy. Techniques like federated learning, which allows local model training without sharing sensitive data, could ensure data privacy. Furthermore, scalability and portability should be evaluated by testing the model’s performance on cloud platforms to enable efficient implementation across diverse technological infrastructures, from local servers to distributed cloud environments.

The incorporation of emerging technologies, such as blockchain, represents another promising avenue. Blockchain could enhance the model by improving data integrity and traceability of security events, especially in managing real-time security alerts. These advancements, combined with continuous refinement to address emerging cyber threats, will ensure that microenterprises remain resilient in an evolving digital landscape. By focusing on these areas, future research can contribute to the development of more robust, efficient, and accessible solutions, advancing the field of cybersecurity for microenterprises.

REFERENCES

[1] Hammadeh, K. and Kavitha, M. (no date a) Unraveling ransomware: Detecting threats with Advanced Machine Learning Algorithms, International Journal of Advanced Computer Science and Applications (IJACSA). Recovered from: https://doi.org/10.14569/IJACSA.2023.0140952

[2] (2020) Two-stage ransomware detection using dynamic analysis and Machine Learning Techniques | Request PDF. Recovered from: https://doi.org/10.1007/s11277-020-07166-9

[3] Seong Il Bae, Gyu Bin Lee y Eul Gyu Im. (2020) Ransomware detection using machine learning algorithms. Concurrency and Computation Practice and Experience. Recovered from: https://www.scopus.com/record/display.uri?eid=2-s2.0-85068027073&origin=reflist

[4] Urooj, U, Al-rimy, B, Zainal, A, Ghaleb, F, Rassam, M. (2022). Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. Applied Sciences (Switzerland). Recovered from: https://doi.org/10.3390/app12010172

[5] Khammas, Ban Mohammed. (2020). Ransomware Detection using Random Forest Technique. ICT Express. Recovered from: https://doi.org/10.1016/j.icte.2020.11.001

[6] Lee, J. et al. (2023) Neutralization method of ransomware detection technology using format preserving encryption, MDPI. Recovered from: https://doi.org/10.3390/s23104728

[7] Jamie Pont, Osama Abu Oun, Calvin Brierley, Budi Arief, and Julio Hernandez-Castro. 2019. A roadmap for improving the impact of anti-ransomware research. In Nordic Conference on Secure IT Systems. Springer, 137–154. Timothy Mclntosh (2022) Ransomware mitigation in the modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Computing Surveys. Recovered from: https://doi.org/10.1145/3479393

[8] Cartwright, E., Hernandez Castro, H., Cartwright, A., 2019. To pay or not: game theoretical models of Ransomware. J. Cybersecur. 5 (1), 1–12. Alena Yuryna Connolly y Hervé Borrion (2022) Reducing Ransomware Crime: Analysis of Victims’ Payment Decisions. Computers and Security. Recovered from: https://doi.org/10.1016/j.cose.2022.102760

[9] Saleh A., Yang X., Wei S. (2022) An Analysis of Conti Ransomware Leaked Source Codes. IEEE Acces. Recovered from: https://doi.org/10.1109/ACCESS.2022.3207757

[10] BTR Consulting. (2024, December 11). *81% increase in ransomware attacks in one year*. TyN Magazine. Retrieved from https://tynmagazine.com/aumento-del-81-de-ataques-ransomware-en-un-ano

[11] Tchernokojev, P. (2024, September 25). *Small and medium-sized enterprises in the Balearic Islands lose an average of 30,000 euros due to cyberattacks*. Cadena SER. Retrieved from https://cadenaser.com/baleares/2024/09/25/las-pymes-de-baleares-pierden-30000-euros-de-media-por-ciberataques-radio-mallorca