International Journal of Recent Research and Review, Special Issue 2, 2026

ISSN 2277 – 8322

Adaptive Malware Classification and Detection with Contemporary Machine Learning Paradigms

Amar Singh Verma[1], Neha Gupta[2], Akash Saxena[3], Amit Kumar Thakore[4]

[1 2 4]*Department of Computer Science and Engineering, Dr. K. N. Modi University, India*

[3]*Department of Computer Science and Engineering, CITM, Jaipur, India*

Email: vamarverma09@gmail.com, nehaguptanneelkanth@gmail.com, akash27jaipur@gmail.com, amitthakore891@gmail.com

Abstract— This study presents an adaptive architecture for malware classification and detection by integrating historical malware evolution with contemporary machine learning approaches. A systematic review of static, dynamic, hybrid and machine learning-based detection methodologies is conducted, evaluating their effectiveness across modern computing environments. A primary contribution is the establishment of a multi-layered detection architecture that systematically aligns malware taxonomy dimensions with appropriate analysis techniques. The proposed architecture emphasizes the integration of multiple analysis modalities to achieve a balance among accuracy, robustness and operational efficiency. The significance of explainable AI and standardized benchmarks in developing robust detection systems is highlighted. By aligning historical classification frameworks with state-of-the-art detection technologies, this study establishes a foundation for developing adaptive, predictive and intelligence-driven cyber defense strategies.

Keywords— Malware classification, malware detection, machine learning, behavioral analysis, zero-day detection, explainable AI, multi-layered detection

1. INRODUCTION

Malware has become an emerged threat to security in all areas consumers, businesses and critical infrastructure. Over the past decade, it first appeared in 1988, malware has steadily increased in complexity, propagation rate and evasion capability. Classical forms such as viruses, worms and trojans have evolved into newer types, including ransomware, spyware and polymorphic malware, which are significantly increasingly challenging to detect and mitigate. Malware has been classified along multiple dimensions,

ISSN 2277 – 8322

including the propagation vector, payload behavior and execution environment. Traditional static and dynamic analysis is still part of any analysis of malware, but are being limited by new types of advance techniques such as obfuscation, packing and anti-analysis [1].

To address these limitations, recent work applies machine learning (ML) and artificial intelligence (AI) to model behavioral patterns and detect previously unseen or zero-day samples, marking a shift from rule-based signatures to adaptive, data-driven detection [3][5]. Traditional signature-based antivirus engines once provided effective defenses against known threats; however, they have become inadequate against sophisticated evasion techniques, obfuscation, packing and anti-analysis methods, as well as metamorphic and polymorphic malware variants [6]. To address these limitations, advances in heuristic, hybrid-based and behavior-based approaches have emerged that correlate code-level properties with dynamic execution behavior, improving robustness against code mutation and environment aware evasion techniques [11].

Yet despite these advancements, attackers continue to exploit gaps in existing frameworks through encryption, code polymorphism and network-level concealment, motivating the need for more integrated, multi-layered solutions [2]. This challenge has intensified with the expansion of the Internet of Things (IoT), mobile platforms and cloud services, which have enlarged the attack surface and increased heterogeneity in target environments. Consequently, detection models must now operate reliably across multiple architectures and deployment contexts while maintaining accuracy and scalability [13]. The central gap this study addresses lies in bridging historical malware taxonomies with contemporary learning-based detection methodologies. By relating the evolution of malware families and taxonomy models to corresponding detection techniques, this work establishes a structured view that links classification dimensions to suitable analysis approaches.

A. Background and Motivation

Malware is still one of the main causes of security breaches, threatens the confidentiality, integrity and availability of your digital assets. Its effects range from large scale financial impact and operational downtime in government and industrial systems to the theft of personal

ISSN 2277 – 8322

information and the disruption of services. Because each family of malware has different infection strategies, persistence mechanisms and lateral movement techniques, the diversity of malware complicates security [3]. As connectivity and automation increase, attackers systematically exploit software vulnerabilities, weak configurations and user behavior to deploy more evasive malware that can reconfigure or obfuscate itself in response to detection attempts. A modern taxonomy that integrates historical perspectives with current machine learning and behavior-based approaches can clarify how different malware traits map to specific detection requirements. In this context, this work aims to connect the development of malware taxonomy with recent detection techniques, providing a structured basis for designing robust and adaptive cybersecurity solutions that leverage prior knowledge while accommodating emerging threats [4].

B. Definition of Malware

Malware can be defined as any software deliberately crafted to perform unauthorized, harmful or evasive activities to information systems and networks [4]. Unlike legitimate applications, malware typically executes without informed user consent, aiming to compromise system integrity, exfiltrate sensitive data or subvert benign operations. Common categories include viruses, worms, Trojans, ransomware, spyware and rootkits, which differ in their infection mechanisms, activation triggers and persistence strategies but share the primary objective of violating security policies [5].

Empirical studies show that malware is delivered through multiple channels, such as malicious email attachments, compromised or spoofed websites, bundled or pirated software and exploitation of unpatched vulnerabilities in services and applications [5]. Once active on a host, malware may log keystrokes, capture credentials, exfiltrate files, encrypt data for ransom or establish remote control channels to command-and-control (C2C) infrastructure.

C. Historical Context

Malware emerged with the development of networks and the evaluation of destructive malware samples used to infect standalone systems. As computer networks began growing larger through improved network connectivity and access to the internet, which has allowed Worms and Email-Delivered Viruses to have the ability to spread rapidly, and

ISSN 2277 – 8322

bypassing signature-based security mechanisms. Worms and mass-mailing attacks during the 1990s and early 2000s revealed the deficiencies in patch management and endpoint protection mechanisms, this led to a significant increase in the use of antivirus software and intrusion detection systems. Unfortunately, both were largely relied on signature updates not effective against the new code variants or obfuscated binaries. As a result of this, dynamic and behavior based methods of analysis were developed by analysts and professionals. These included Sandboxing, System call monitoring, Network flows and file operations at runtime to detect new types of malware that did not match previously seen code [7].

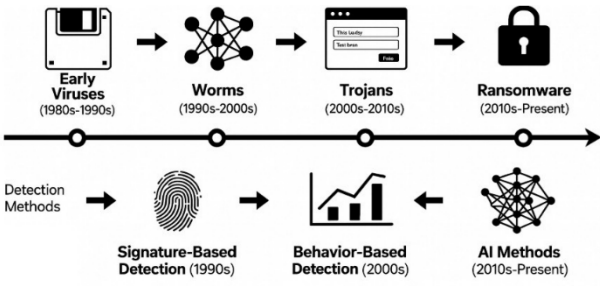

Fig. 1. Historical context

Malware now generally attacks three things: credentials, intellectual property, and critical infrastructure. with a single toolchain being made up of a mix of the components of lateral movement, exfiltration and extortion. Understanding the historical evolution of malware attacks is essential for proposing effective taxonomies and for mapping the detection systems to the techniques and goals that are representative of each generation of threats [8].

D. Research Objective and Scope

The primary objective of this study is to structural correspondence between malware taxonomy development and evolving detection methods, to describe how classification schemes affect and restrict analysis and defense methods. This study evaluates at how malware structure have changed over time, how the existing taxonomies describe these three dimensions, how well current detection techniques work on different types and growth stages of malware.

By synthesizing insights from surveys, empirical studies and proposed frameworks, the work seeks to outline a unified perspective that can refer the design of taxonomy-aware detection architectures and serve as a future research direction in malware analysis.

2. LITERATURE REVIEW

A. Historical Development of Malware

Along with rapid evolution, malware has also become more advanced with

ISSN 2277 – 8322

sophisticated attack techniques, diverse attack motivations and improved methods for avoid detection [1]. In the 2000, ransomware introduced direct financial extortion by encrypting the user or organizational data and demanding payment for decryption [1]. Another major change in the landscape of cybersecurity in 2010 i.e. rise of polymorphic and metamorphic malware, capable of dynamic change in their appearance to evade detections. Since the introduction of machine learning (AI/ML), there has been a continued rise in the development and use of fully automated, machine learning (AI/ML)-assisted malware for malicious code delivery, evasion, targeting and C2C activities. This will result in a further escalation of the speed, stealth and adaptability of malware. Detection techniques have evolved in parallel, moving from signature-based methods to more sophisticated heuristic, behavioral and learning-based systems in response to these changing malware characteristics. The historical context of an attack is important in interpreting current attack vectors, and developing new defensive measures [1].

TABLE I: CLASSIC VS CONTEMPORARY MALWARE

Attribute	**Classic Malware**	**Contemporary Malware**
Type	Trojan, Worm, Virus	AI-powered malware, Polymorphic/ Metamorphic, Ransomware
Attack Vector	File boot sector, Network email, Disguised apps	Email attachments, Exploit kits, Infected files, Automated AI exploits
Evasion Techniques	Simple hiding, Signature alteration, Replication, Social engineering	Encryption, Anti-debugging, Code mutation, Behavioral adaptation
Typical Targets	Data, Applications, Networks, Devices,	Enterprises, Individuals, Antivirus systems, IoT, Cloud environments
Impact	Disruption, Rapid spread, Data theft	Financial extortion, Detection evasion, Persistent attacks

The timeline generally highlights the progression of malware from viruses, worms, Trojans, ransomware to advanced polymorphic and AI-assisted malware. Also, every new generation of malware builds on technologies already used in the past while finding new systems and platforms to infect. This chronological

ISSN 2277 – 8322

perspective underscores the need for adaptable detection strategies that can accommodate both legacy threats and emerging attack models [2].

TABLE II: MAJOR HISTORICAL MALWARE TYPES

Type	Period	Attack Method	Impact	Ref.
Virus	1980s	File infection	System disruption	[1][6]
Worm	1990s	Network propagation	Rapid spread	[1][6]
Trojan	Late 1990s	Disguised files	Data theft	[2][7]
Ransomware	2000s	File encryption	Financial loss	[2][7]
Poly/Metamorphic	2010s	Self-modifying code	Evade detection	[5][14]
AI-powered	2020s	Adaptive learning	Stealth attacks	[3][4]

Such models are useful for incident response and mitigation planning, since they essentially measure operational effects instead of implementation details, however they rely on observational based approach will thus incur difficulty from obfuscation, environment-aware behavior or delays in execution [2].

Propagation-based models classify malware based on infection and propagation mechanisms, categories include email-borne worms, network-scanning worms, drive-by downloads and removable-media infections. They provide a mechanism for propagation modeling and establishing containment strategies; however, with modern multi vector threats; often span several categories simultaneously [3].

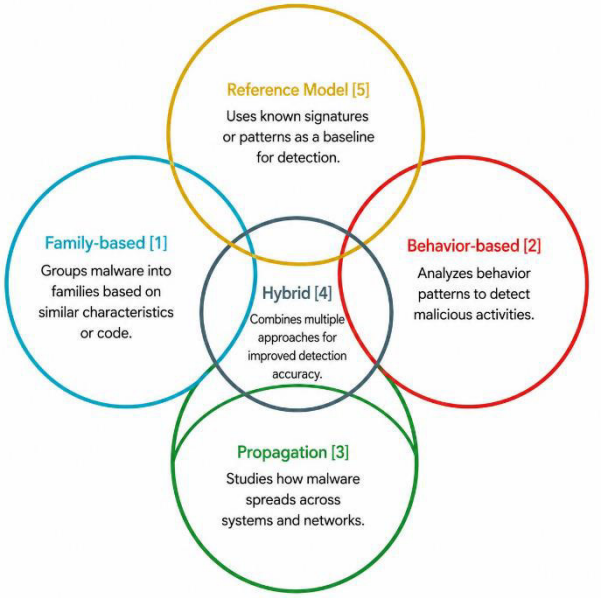

Fig. 2. Malware Taxonomy Models: Outline figure visualizing relationship and overlaps among malware taxonomy models, with reference

Family-Based Taxonomy Model: Malware taxonomy models provide structured methods of classifying malware and comparing different types of malware. These classification frameworks allow threat actors and organizations involved in attacks to identify malware families for

ISSN 2277 – 8322

identification purposes; attribute specific malware threat to identified families; label malware datasets according to their relationship to previously identified malware families; and choose the most appropriate detection methods [4].

1) Behavior-Based Taxonomy Model: It is based on classifying of malware according to actions that can be observed on systems and networks, such as keylogging, data exfiltration, lateral movement, or file encryption [5].

2) Propagation-Based Taxonomy Model: The model classifies malware by its propagation pathways and infection behavior in computing environments; it provides a clearer understanding of how malware spreads and provides a framework for building network-level defenses against it.

3) Hybrid Taxonomy Model: Conversely, the model incorporates multidimensional classification by including the family, behavior and propagation attributes within one analytic framework, due to that modern malware exhibits increasingly sophisticated and multifaceted characteristics; thus, a single criterion classification will not give enough information to categorize malware completely.

4) Reference-Based Taxonomy Model: Like many other models, the model relies on many standardized frameworks, taxonomies and knowledge base. The model used on complex threats that often change, such as polymorphic malware and APTs (Advanced Persistent Threats), there are two things that need to be done correctly; generating the correct labels and mapping these same labels to known behaviors.

TABLE III: MALWARE TAXONOMY MODELS COMPARISON

Model Type	**Defining Principle**	**Example Categories**	**Main Advantage**	**Main Challenge**	**Refs.**
Family-based	Groups by code, lineage or structural similarity	Trojan, Virus, Worm	Easy identification and historic tracing	May miss behavioral changes	[2][14][9]
Behavior-based	Classifies by action or system impact	Spyware, Ransomware	Detects new or unknown threats	Requires accurate behavior tracking	[2][4][9]
Propagation-based	Groups by spread or infection method	Network worm, File	Clarifies spreading risks	May overlap with other traits	[2][7][3]

ISSN 2277 – 8322

		infector			
Hybrid/Composite	Combines multiple classification factors	Hybrid threats	Handles complex malware types	Complex to implement	[3][9][14]
Reference-based	Standardizes using agreed frameworks	Study or industry standards	Ensures consistency across studies	Limited flexibility	[2][1]

C. *Classic Detection Approaches*

Traditional malware detection techniques serve as a basis for modern defense techniques, which consist predominantly of signature-based detection, heuristic based detection and behavioral analysis. This technique uses pattern matching, rule-based anomaly detection as well as runtime monitoring for the detection of malicious behavior. These techniques have been extensively used in the development of endpoint and network security [7].

1) Signature-Based Detection: Such methods based on the comparing of contents of files or segments of code against a database of malicious or suspicious patterns. The method provides a rapid detection with relatively low rates of false positives for known samples. However, this method is ineffective against zero-day threats, heavily code obfuscation binaries [9][35][37].

2) Heuristic-Based Detection: Heuristic approaches are based on scoring and rules to detect potentially suspicious constructs, such as unusual API sequences, packing behavior or anomalous control flow, even in the absence of a specific signature. Thus they are able to detect more types of malware at the expense of increasing the probability of false alarms, and therefore must be carefully calibrated, often integration with other detection [31][34].

3) Behavioral Analysis: The challenge with behavioral detections is that behavioral detections consume more computing resources than signature-based detections. In addition, some types of behavioral detections can be avoided by creating behavior that are dependent on being in a particular environment or are delayed over time. Static variant of the technology is used to analyze the code to predict its behavior; whereas dynamic variant is used by running the sample in a controlled environment. Both variants are more resilient to code-level obfuscation but can be elevated in computational demands, and can be evaded by environment-aware or time-delayed behavior [8].

ISSN 2277 – 8322

TABLE IV: EFFECTIVENESS COMPARISON OF CLASSIC MALWARE DETECTION APPROACHES

Approach	**Analysis Type**	**Strengths**	**Weaknesses**	**Example Tools (Historical)**
Signature-Based	Static	Fast, low false positives for known threats	Zero-day blind	Virus Total (early hashing)
Heuristic-Based	Static/Dynamic	Novel threat detection	High false positives	Early IDS like Snort rules
Behavioral	Dynamic	Captures evasion tactics	Resource-intensive	Cuckoo Sandbox precursors

Empirical studies indicate that signature-based techniques can achieve extremely high accuracy levels on widely-used data sets. However, their performance significantly degrades when they encounter polymorphic or metamorphic samples. Heuristic-based and behavioral-based detection approaches improve generalization capabilities but are associated with higher resource consumption, increased latency, and reduced explainability, which leads to new combinations of signature-based and non-signature-based methods to create hybrid detection systems [35].

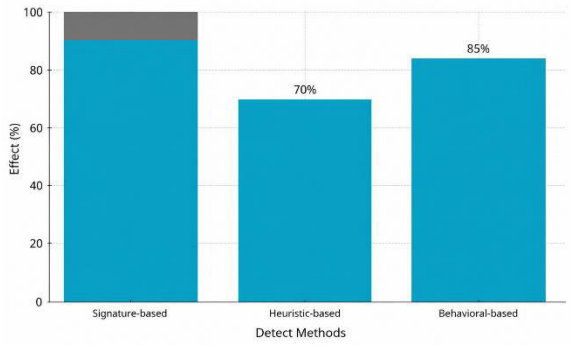

Fig. 3. Effectiveness Comparison of Classic Malware Detection Approaches

D. Recent Advancements and Research Gaps

Since 2020, significant technological advancements have been made within the framework of malware detection systems, certainly with the inclusion of machine learning, deep learning and large-scale data analysis through cloud storage capabilities [34].

1) Machine Learning Hybrids: Hybrid models combine static features such as opcodes, strings or imported functions with dynamic traces including system calls and network flows, often using classical classifiers or CNN–LSTM architectures to perform multi-variant classification. Federated and distributed learning variants have been proposed to train models collaboratively across endpoints or organizations while

ISSN 2277 – 8322

preserving data privacy, reducing central collection requirements and latency [27][34].

2) AI and Deep Learning: Deep learning approaches employ architectures such as CNNs, recurrent networks and graph neural networks to learn discriminative representations from raw binaries, API call sequences or control-flow graphs. Systematic reviews indicate that these models frequently achieve higher detection rates than traditional machine learning on diverse platforms, including Windows, Android and IoT, particularly for complex or obfuscated malware. Edge and cloud deployments enable near real-time analysis of large telemetry streams, supporting continuous monitoring in mobile and distributed environments [18][34].

3) Emerging Paradigms: It include blockchain-assisted integrity verification, where distributed ledgers help detect tampering and maintain trusted provenance, as well as explainable AI methods that clarify model decisions to support incident response and regulatory compliance. Research has also explored adversarial robustness, as attackers can craft perturbed binaries or traces to mislead ML models and quantum-resistant primitives for future-proofing cryptographic components in detection pipelines [19],[44].

TABLE V: EVOLUTION OF DETECTION ACCURACY OVER TIME

Paradigm	Key Technique	Accuracy Gain (%)	Platforms
ML Hybrids	CNN-LSTM + Features	20-30	Windows/Android
Deep Learning	GNN on API Graphs	15-25	IoT/Cloud
Emerging	XAI + Blockchain	10-15	Edge/Mobile

Despite these advances, there are still many challenges. The primary challenges includes; improving the robustness of models against adversial attack, supporting scalable real-time detection on embedded and other resource constrained environments, providing solutions to resolve the issues related to imbalanced and evolving dataset, developing taxonomy-aware models that are explainable and operationally viable. Addressing these challenges will be critical to the advancement of modern detection methods in line with the evolving malware ecosystem described in this review.

3. CHALLENGES IN MALWARE DETECTION

Malware detection faces three interconnected and escalating challenges

ISSN 2277 – 8322

that together undermine traditional defenses. Signature-driven systems struggle with zero-day and highly mutated samples, motivating combined use of static, dynamic and behavioral approaches for more resilient detection [4],[44].

A. Evasion Techniques:

First, evasion techniques have become increasingly sophisticated. Modern malware extensively uses obfuscation, packing and anti-analysis to hinder inspection and avoid both static and dynamic detectors. Polymorphic and metamorphic variants deliberately modify code structure while preserving functionality, reducing the effectiveness of pattern-based signatures and simple feature extractors. In dynamic settings, anti-debugging checks, environment fingerprinting, sandbox evasion and adversarial perturbations further distort runtime traces or mislead machine learning models, degrading detection accuracy [1][16].

B. Zero-Day and Variant Proliferation:

Building on this evasion problem is a second challenge: the sheer volume of zero-day variants. The volume of new and slightly modified samples registered each day overwhelms manual analysis workflows and signature generation pipelines. Zero-day and fileless malware, combined with AI-assisted sample generation, reduce the ability of learned models to generalize from historical datasets, particularly when training data are imbalanced or outdated. Heterogeneous behaviors across ransomware, mobile and IoT malware further complicate model design and often increase false negatives in specialized environments [4][5][35].

C. Static and Dynamic Analysis Limitations:

Underlying both evasion and proliferation challenges is a third limitation: the inherent constraints of static and dynamic analysis approaches. Static analysis is inherently limited against encrypted or obfuscated code, while dynamic analysis requires controlled environments that may not reflect real-world conditions. 3 These combined challenges necessitate a shift from single-method detection to hybrid approaches that integrate multiple analysis modalities [9].

Resource and Scalability Constraints: Large-scale deployment must balance detection accuracy with latency, memory and energy constraints, particularly on mobile and IoT platforms. Security teams also face alert fatigue from false positives and limited expert capacity to triage complex cases, making it difficult to

ISSN 2277 – 8322

operationalize advanced models in production. Recent work points to explainable AI and tighter integration with threat intelligence as avenues to improve trust, reduce analyst workload and better prioritize responses [22].

4. LIMITATIONS OF THE CURRENT STUDY

This review acknowledges several methodological and practical constraints that bound its scope and conclusions. First, a significant gap exists in data availability. Proprietary industry datasets, closed threat reports, and vendor-specific telemetry are largely inaccessible to researchers, meaning emerging attack patterns observed only in operational environments may remain underrepresented in the literature reviewed [7][34].

Second, the methodological diversity across surveyed works presents a challenge to comparative analysis. The literature employs heterogeneous methodologies, platforms, datasets, and evaluation metrics spanning static, dynamic, hybrid, and deep learning approaches. Differences in dataset composition, feature extraction pipelines, and experimental protocols limit the ability to perform strict comparative evaluations of reported detection rates and robustness claims across studies [4][5][7]. Third, the rapid evolution of the threat landscape outpaces academic publication cycles. Although historical malware development is used to derive an evolutionary perspective, new polymorphic, metamorphic, IoT-oriented, and AI-assisted malware variants emerge faster than comprehensive academic analyses can be conducted and published, rendering some taxonomic classifications partially obsolete by the time they

appear in the literature [18][15].

Fourth, the study is limited by the absence of hands-on benchmarking experiments. No new implementations or comparative evaluations on a standardized reference dataset are conducted, which restricts the quantification of practical robustness against adversarial attacks and the assessment of cross-family generalization capabilities under consistent experimental conditions [9][22].

Fifth, the research relies primarily on existing taxonomies drawn from the literature rather than proposing or validating a novel empirical taxonomy through large-scale analysis of malware sample corpora. Finally, the review's platform coverage concentrates predominantly on executable-centric malware targeting general-purpose operating systems. Firmware, containerized workloads, mobile

ISSN 2277 – 8322

application ecosystems, and software supply chain attacks receive more limited treatment [13][14].

These constraints suggest avenues for future work, particularly in standardizing evaluation methodologies, accessing real-world threat intelligence, and expanding scope across diverse computing platforms.

5. FUTURE RESEARCH DIRECTIONS

The study identifies four key research priorities for advancing malware detection:

1) Ontology-Based Taxonomies: Developing context-aware taxonomies that encode semantic relationships between malware families, tactics, and target platforms, enabling continuous refinement and precise mapping between malware traits and detection methods.

2)Explainable AI Frameworks: Moving beyond opaque machine learning models by leveraging attention mechanisms, model-agnostic explanation tools and symbolic–neural hybrids to expose the features and behaviors underlying detection decisions, thereby increasing trust and supporting regulatory compliance.

i) Cross-Platform and IoT Detection: Addressing the failure of traditional desktop-centric solutions on embedded, mobile, and edge devices by designing lightweight, distributed models that leverage federated learning and blockchain-backed coordination mechanisms while preserving privacy.

ii) *Efficient Algorithms for Distributed Settings:* Creating robust, energy-efficient algorithms and communication protocols for collaborative detection across resource-constrained devices.

6. CONCLUSIONS

This study demonstrates that integrating historical malware taxonomy and evolution with contemporary machine learning approaches provides a robust foundation for modern cyber defense. Advances in machine learning and deep learning have substantially strengthened detection capabilities, particu-larly for handling obfuscated and previously unseen samples that evade traditional signature-based tools. However, these approaches face inherent limitations including dataset bias, adversarial examples, and difficulties in distinguishing benign anomalies from true attacks in complex environments.

Evidence indicates that combining static, dynamic and behavioral analyses within hybrid or layered architectures offers a more balanced trade-off between accuracy, robustness and operational efficiency. Beyond methodological advances,

improving transparency and standardization is critical for sus-tained progress. Explainable AI techniques can increase trust in automated detectors and facilitate forensic analysis, while harmonized malware taxonomies and benchmarks enhance reproducibility across academic and industrial communities. By aligning historically informed classification frameworks with state-of-the-art detection technologies, defense efforts can transition from primarily reactive mitigation toward more predictive and intelligence-driven security postures.

REFERENCES

[1] Robert David, ”understanding Malware: A comprehensive Guide to Types,Risks and Prevention Strategies” REVISTA DE INTELIGENCIA ARTIFICIAL EN MEDICINA, Volume: 15 Issue: 01 (2024), Available Online: https://redcrevistas.com/index.php/Revista

[2] Priya Arora, Rashmi Gupta, Nidhi Malik and Anil Kumar ”Malware Analysis Types & Techniques : A Survey”, ICIMMI ’23: Proceedings of the 5th International Conference on Information Management & Machine Intelligence, Article No.: 135, Pages 1 – 6, May 2024, DOI: 10.1145/3647444.3652439.

[3] Jannatul Ferdous, Rafiqul Islam, Arash Mahboubi and Md. Zahidul Islam, ”A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms” Journals & Magazines IEEE Access Volume:11, Page(s): 121118 - 121141, October 2023, Electronic ISSN: 2169-3536, DOI: 10.1109/ACCESS.2023.3328351.

[4] Faitouri A. Aboaoja, Anazida Zainal, Fuad A. Ghaleb, Ban-der Ali Saleh Alrimy, Taiseer Abdalla Elfadil Eisa and Asma Abbas Hassan Elnour “Malware Detection Issues, Challenges, and Future Directions: A Survey” Appl. Sci. 2022, 12(17), 8482;https://doi.org/10.3390/app12178482.

[5] O.A.Aslan,R.Samet, “A Comprehensive Review on Malware Detection Approaches”,IEEE Vol 8, ISSN:2169-3536,2022.

[6] Jeff Chandy, ”Review on Malware, Types, and its Analysis”, In-ternational Journal for Research in Applied Science & Engineer-ing Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538, Volume 10 Issue XII Dec 2022, https://doi.org/10.22214/ijraset.2022.

47887.

[7] Harjeevan Gill, ”Malware: Types, Analysis and Classifications”, June 2022, DOI:10.31224/2423.

[8] M Parekh,GKulkarni “A Survey on Malware Analysis Techniques,its Detection and Mitigation” International Research Journal on Engineering & Technology, Vol.08, ISSN:2395-0072,2021.

[9] Nagababu Pachhala, S. Jothilakshmi and Bhanu Prakash Battula, ”A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques”, Published in: 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), IEEE, DOI: 10.1109/ICOSEC51865.2021.9591763.

[10] Ishant Yadav, Gagandeep kaur, Sukhwinder Kaurand Anshu Vashisth ”A Complete Study on Malware Types and Detecting Ransomware Using API Calls” Conference: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), DOI:10.1109/ICRITO51393.2021.9596085.

[11] C Rohith and G. Kaur, ”A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus,” 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 429-434. DOI: 10.1109/ICIEM51511.2021.9445322.

[12] Tibra Alsmadi and Nour Alqudah ”A Survey on malware detection techniques” Published in: 2021 International Conference on Information Technology (ICIT). DOI: 10.1109/ICIT52682.2021.9491765.

[13] Hector Menendez, “Malware: The Never-Ending Arms Race”, Published: Sep 8, 2021, DOI: https://doi.org/10.46723/ojc.1.1.3.

[14] Adel Abusitta, Miles Q. Li and Benjamin C.M. Fung, “Malware classification and composition analysis: A survey of recent developments”, Journal of Information Security and Applications, Volume 59, June 2021, 102828, DOI: 10.1016/j.jisa.2021.102828.

[15] Mohammed N. Alenezi , Haneen Alabdulrazzaq, Abdullah A. Alshaher and Mubarak M. Alkharang, “Evolution of Malware Threats and

Tech-niques: A Review" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 12, No. 3, December 2020.

[16] Sajedul Talukder1 and Zahidur Talukde, "A SURVEY ON MALWARE DETECTION AND ANALYSIS TOOLS", International Journal of Network Security & Its Applications (IJNSA) Vol. 12, No.2, March 2020.

[17] Omer Aslan Aslan and Refik Same, "A Comprehensive Review on Malware Detection Approaches" Published in: IEEE Access (Volume: 8). Page(s): 6249 – 6271 (2020), Electronic ISSN: 2169-3536. DOI:10.1109/ACCESS.2019.2963724.

[18] Vignau B, Khoury R and Halle´ S, "10 years of IoT malware: A feature-based taxonomy" In: 2019 IEEE 19th international conference on software quality, reliability and security companion. IEEE; 2019, p. 458–65.

[19] Sanjay K. Sahay, Ashu Sharma and Hemant Rathore, "Evolution of Malware and Its Detection Techniques" Conference paper, First Online: 26 June 2019, Part of the book series: Advances in Intelligent Systems and Computing (AISC,volume 933).

[20] R. Tahir, "A Study on Malware and Malware Detection Techniques," Int. J. Educ. Manag. Eng., vol. 8, no. 2, pp. 20–30, 2018.

[21] Anitta Patience Namanya; Andrea Cullen; Irfan U. Awan; Jules Pagna Disso, "The World of Malware: An Overview", Published in: 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), DOI: 10.1109/FiCloud.2018.00067.

[22] A. Souri and R. Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," Hum-Centric Comput. Inf. Sci., vol. 8, no. 1, p. 3, 2018.

[23] Pai S, Di Troia F, Visaggio CA, Austin TH and Stamp M. "Clus-tering for malware classification". J Comput Virol Hacking Tech 2017;13(2):95–107.

[24] Mohd Faizal Ab Razak, Nor Badrul Anuar, Rosli Salleh and Ahmad Fir-daus, "The rise of "malware": Bibliometric analysis of malware study", Journal of Network and Computer Applications, Volume 75, November 2016, Pages 58-76, https://doi.org/10.1016/j.jnca.2016.08.022.

[25] LiangG. et al., ”A behavior-based malware variant classification technique”, Int J Inf Educ Technol (2016).

[26] GhiasiM. et al., ”Dynamic VSA: a framework for malware detection based on register contents” Eng Appl Artif Intell, (2015).

[27] MohaisenA. et al., Amal: High-fidelity, behavior-based automated mal-ware analysis and classification, Comput Secur (2015).

[28] S. Alam, R. Horspool, I. Traore, and I. Sogukpinar, “A framework for metamorphic malware analysis and real-time detection,” Comput. Secur., vol. 48, pp. 212–233, Feb. 2015.

[29] Gandotra, E., Bansal, D. and Sofat, ”Malware analysis and classification: a survey” Journal of Information Security Vol.5 No.2(2014), Article ID:44440,9 pages DOI:10.4236/jis.2014.52006.

[30] IslamR. et al. ”Classification of malware based on integrated static and dynamic features”, J Netw Comput Appl 2013.

[31] Z. Bazrafshan, H. Hashemi, S. M. H. Fard, and A. Hamzeh, “A survey on heuristic malware detection techniques,” in Proc. 5th Conf. Inf. Knowl. Technol., May 2013.

[32] R. Islam, R. Tian, L. M. Batten and S. Versteeg, “Classification of malware based on integrated static and dynamic features,” J. Netw. Comput. Appl., vol. 36, no. 2, pp. 646–656, Mar. 2013.

[33] Imtithal A. Saeed, Ali Selamat and Ali M. A. Abuagoub, ”A Survey on Malware and Malware Detection Systems”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.16, April 2013.

[34] Kirti Mathur and Saroj Hiranwal, ”A Survey on Techniques in Detection and Analyzing Malware Executables”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 4, April 2013.

[35] Ammar Ahmed E. Elhadi, Mohd Aizaini Maarof and Ahmed Hamza Osman, ”Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph”, American Journal of Applied Sciences 9 (3): 283-288, 2012, ISSN 1546-9239, 2012.

[36] ChenZ. et al., ”Malware characteristics and threats on the internet ecosystem”, J Syst Softw (2012).

[37] Pham Van Hung, ”An approach to fast malware classification with machine learning technique”, Keio University,5322 Endo Fujisawa Kanagawa 252-0882 JAPAN, 2011.

[38] Ronghua Tian, ”An Integrated Malware Detection and Classification System”, Changchun University of Science and Technology, Thesis, August, 2011.

[39] J. Kinder, S. Katzenbeisser, C. Schallhart and H. Veith, “Proactive detection of computer worms using model checking,” IEEE Trans. Depend. Sec. Comput., vol. 7, no. 4, pp. 424–438, Oct. 2010.

[40] P. Beaucamps and J. Marion, “On behavioral detection,” in Proc. EICAR, vol. 9, 2009.

[41] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda and C. Kruegel, “A view on current malware behaviors,” in Proc. USENIX Workshop, 2009.

[42] G. Wagener, R. State and A. Dulaunoy, “Malware behaviour analysis,” J. Comput. Virol., vol. 4, no. 4, pp. 279–287, Nov. 2008.

[43] M. Christodorescu, S. Jha, D. Maughan, D. Song and C. Wang, Malware Detection. Springer Science & Business Media, 2007.

[44] N. Idika and P. Mathur, “A survey of malware detection techniques,” Purdue Univ., West Lafayette, IN, USA, Tech. Rep., vol. 48, 2007.

[45] A. Holzer, J. Kinder and H. Veith, “Using verification technology to specify and detect malware,” in Proc. Int. Conf. Comput. Aided Syst. Theory. Berlin, Germany : Springer, 2007.