MANAGEMENT
2025, Vol. 29, No. 1
www.management-poland.com
DOI: 10.58691/man/200768

MARCIN PYCKA
MACIEJ ZASTEMPOWSKI

Machine learning and artificial intelligence techniques adopted for IT audit

Abstract

Research background and purpose: The rapid advancement of artificial intelligence (AI) and machine learning (ML) is reshaping IT audit practices by enhancing cybersecurity through improved risk management, technological integration, and data-driven strategies. Despite these advancements, there is a lack of comprehensive frameworks that fully integrate AI and ML into IT auditing, particularly for addressing complex threats like Advanced Persistent Threats (APTs). This study aims to explore these technologies' potential to transform IT audits.

Design/methodology/approach: A Systematic Literature Review (SLR) was conducted, analyzing studies from Scopus and Web of Science to identify trends and gaps in applying AI and ML in IT audits. Key areas of focus included risk management frameworks, cybersecurity methodologies, and emerging AI-driven audit techniques.

Findings: The review underscores AI and ML's pivotal roles in predictive analytics, anomaly detection, and real-time risk assessment. Frameworks like Transfer, Accept, Reduce, Avoid (TARA) and methodologies such as the Experimental Framework for Detecting Cyber-Attacks (ECAD) illustrate practical AI applications. The research also highlights the integration of blockchain, cloud computing, and game theory in enhancing cybersecurity audits. Nonetheless, challenges such as data quality and ethical considerations remain significant.

Value added and limitations: This study contributes to IT auditing literature by providing a structured analysis of AI and ML applications, highlighting emerging trends, and suggesting future research directions. Limitations include reliance on existing studies and the evolving nature of AI technologies. Future work should focus on empirical validation of AI-driven audit models and developing standardized frameworks to ensure robustness and reliability in IT audits.

Keywords: *IT security, artificial intelligence, machine learning, IT audit, cyber-security*

JEL
Classification: C19, M10, M42, O33

Received: 2024-06-14; **Final review:** 2024-12-12; **Accepted:** 2025-02-03

Marcin Pycka
Doctoral School of Social Science, Nicolaus Copernicus University, Poland,
ORCID: 0009-0007-4297-2675

Maciej Zastempowski ✉
Faculty of Economic Sciences and Management, Department of Enterprise Management, Nicolaus Copernicus University, Gagarina 13A, 87-100, Toruń, Poland;
email: mz@umk.pl, ORCID: 0000-0001-8196-3236

1. Introduction

In the rapidly evolving landscape of information technology (IT) security, the integration of Artificial Intelligence (AI) and Machine Learning (ML) techniques has emerged as a pivotal strategy for enhancing IT audit processes (Appelbaum et al., 2017; Ramamoorti et al., 1999; Omoteso, 2012). Although recent scientific literature presents a myriad of approaches to IT security and auditing, it is worth emphasising that it reveals both convergent and divergent methodologies (A. R. Hasan, 2022; Kokina & Davenport, 2017; Calderon and Cheh, 2002). Despite differing perspectives, several commonalities are evident across studies, particularly in the realms of risk management (AL-Dosari & Fetais, 2023; Cristea, 2021; Kure et al., 2022; Kedarya & Elalouf, 2023), technological integration (Mladenic et al., 2003; Thach et al., 2021), and data-driven strategies (Canada, 2020; Benzekri et al., 2019). However, despite the wealth of existing research, there remains a notable gap in fully integrating AI and ML into IT auditing frameworks to address modern, sophisticated cybersecurity threats such as Advanced Persistent Threats (APTs).

The issue of using AI and ML invariably arises in all these areas, yet a comprehensive, unified approach to applying these technologies in IT auditing—particularly for high-risk and complex environments—has not been sufficiently addressed. Current studies often focus on isolated aspects, such as anomaly detection, risk profiling, or compliance, but few explore the holistic application of AI and ML methodologies to strengthen IT audit processes comprehensively. Moreover, the literature lacks frameworks that adapt to dynamic, evolving cyber threats while ensuring robust risk management and effective technological integration.

Considering the diversity of approaches to defining these terms, the following definitions have been adopted for the purposes of this study:

- IT Audit: An information technology audit is defined as a systematic examination of the use, resources, and flow of information, evaluated through the analysis of both human and documentary sources, with the aim of determining their contribution to achieving organisational objectives (Buchanan and Gibb, 2008). For the purposes of this article, terms such as "technology audit," "system audit," and "network audit" are regarded as subcategories of IT audit.
- Artificial Intelligence (AI): Artificial intelligence refers to the science and engineering of designing and creating intelligent machines capable of performing tasks that typically require human intelligence (McCarthy et al., 2006).
- Machine Learning (ML): A subdomain of artificial intelligence, machine learning is concerned with the development of algorithms that enable computers to learn from data and make predictions or decisions without being explicitly programmed. This involves the training of computational models on datasets to perform specific tasks (Sarker, 2021).

The critical role of advanced technologies in enhancing IT security and auditing is widely acknowledged. For example, Lu (2022) examines the application of technologies such as cloud computing and blockchain in auditing processes. Mironeanu et al. (2021) focus on the use of ML methods for detecting cyber-attacks, while Saleem et al. (2020) propose models based on real attack analysis, and Khalili et al. (2018) utilise ML techniques for quantitative security assessments. These studies underscore the potential of AI and ML but stop short of offering integrated frameworks for IT auditing that address complex cybersecurity challenges such as APTs, which demand a multi-faceted, adaptive approach.

Advancements in AI and ML are transforming cybersecurity practices, particularly in auditing complex systems like those in the financial sector. Recent studies highlight the pivotal role of AI and ML in identifying and mitigating cyber threats through predictive analytics, anomaly detection, and adaptive defence mechanisms. For instance, a review of IoT-enabled smart airport infrastructures underscores the potential of AI-driven frameworks to safeguard critical systems through real-time risk profiling and automated monitoring, mitigating vulnerabilities introduced by heterogeneous and outdated technologies (Koroniotis et al., 2020). Similarly, game-theoretic approaches have emerged as a strategic tool for countering APTs, leveraging ML to simulate dynamic attacker-defender interactions and optimise resource allocation (Khalid et al., 2023). However, these contributions often remain domain-specific, highlighting the lack of generalisable strategies to incorporate AI/ML effectively into IT audit processes.

Also, in the field of data-driven strategies, the use of ML and AI is becoming more and more critical. For example, Mironeanu et al. (2021) and Khalili et al. (2018) emphasise the importance of data in improving IT security. Mironeanu et al. propose an Experimental Framework for Detecting Cyber-Attacks (ECAD) that heavily relies on data analysis. Similarly, Khalili et al. highlight data use for creating personalised insurance policies, demonstrating the significance of data-driven approaches in enhancing IT audit methodologies. Yet, the lack of a unified, adaptable framework remains evident, leaving organisations to piece together fragmented strategies for addressing increasingly sophisticated cyber threats.

This paper addresses this research gap by exploring the application of AI and ML methodologies to IT auditing, with a particular focus on risk management, technological integration, and data-driven approaches. By synthesising insights from contemporary research and proposing adaptable auditing frameworks, this study aims to bridge the divide between theoretical advancements and practical implementation in IT auditing. Such an exploration is critical to improving IT security audit outcomes and addressing the growing complexity of cyber threats.

In the empirical layer, the paper employs the method of Systematic Literature Review (SLR), as proposed by Tranfield et al. (2003), to provide a robust foundation of evidence

to support scientific assumptions (Kitchenham, 2007). As previous research indicates (Kitchenham, 2004; Tranfield et al., 2003), this method allows for a thorough exploration of the research field, ensuring both breadth and depth of understanding.

The article's structure is as follows: Section 2 presents the method and scope of the conducted narrative SLR. The third part presents the obtained results and their discussion, and the last part presents conclusions.

2. Scope and Systematic Literature Review Methodology

The SLR method was used to determine the scope and depth of the research field, as proposed in the study by Tranfield et al. (2003). The literature review was conducted on March 14, 2024, based on two full-text databases - Scopus and Web of Science. The search string and inclusion and exclusion criteria are presented in Figure 1.

The decision to include only articles containing at least three specific keywords ensures thematic relevance and supports the study's objective of exploring the interconnectedness of IT audit, cybersecurity, and advanced technologies such as AI and APTs. This criterion helps filter out peripheral or tangential studies, prioritising those that provide meaningful insights into the multidisciplinary nature of the research. It aligns with the structured literature review methodology by balancing breadth and depth, capturing a focused dataset while maintaining rigour and relevance. By emphasising studies addressing multiple keywords, this approach facilitates a comprehensive yet manageable exploration of the field's complex intersections.

Two points are worth emphasising. Firstly, to focus on scientific articles describing at least three of the included criteria, items that contained at least three indicated keywords were selected. Secondly, the analysis of the 41 identified articles resulted in other research papers that were not initially revealed in the systematic literature review. Hence, eight additional articles were added to the research.

Integrating computer science with business management and accounting in the context of IT auditing is essential to address the interdisciplinary nature of modern auditing challenges (Canada, 2020). IT auditing requires technical expertise to assess complex systems and ensure cybersecurity, data integrity, and system reliability. At the same time, business management and accounting provide the necessary context for evaluating how these systems align with organisational goals, financial processes, and compliance requirements (Hasan, 2022). By combining these disciplines, auditors are equipped to analyse large volumes of data using advanced tools like artificial intelligence and machine learning, enabling more precise risk assessment and data-driven decision-making. This interdisciplinary approach ensures a comprehensive evaluation of both technical and strategic dimensions, enhancing the effectiveness and relevance of IT audits in today's dynamic business environments.

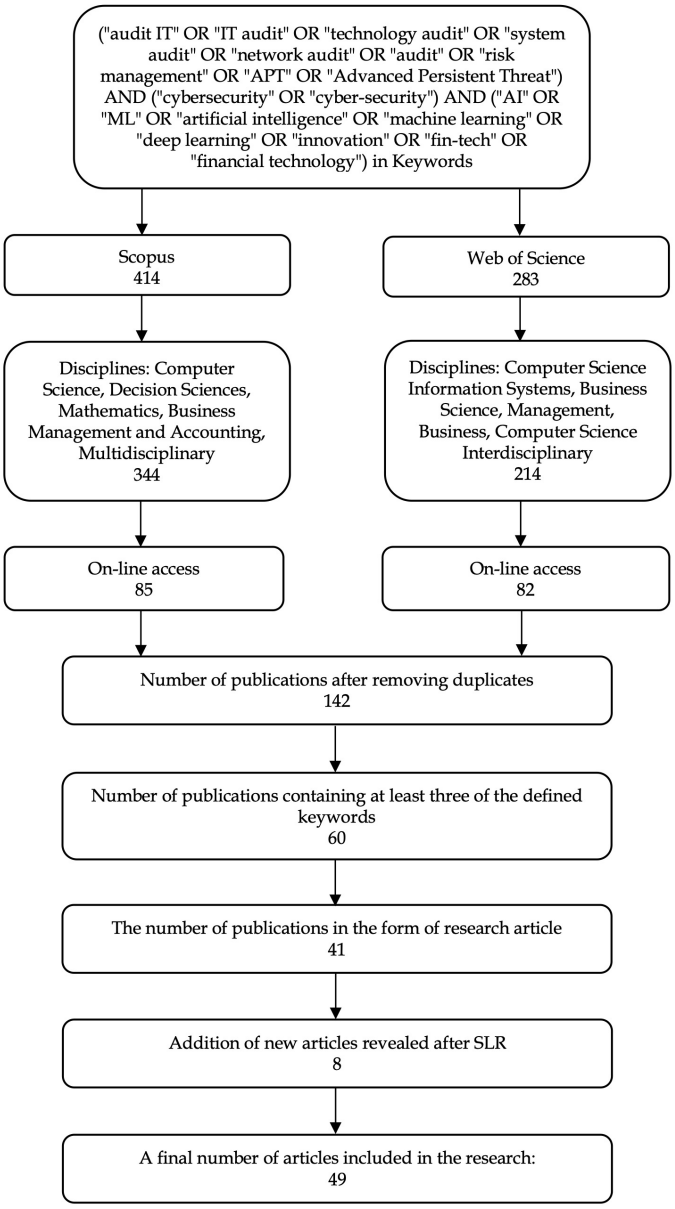

Figure 1. **Details of systematic literature review**

Source: own study

3. Results and discussion

IT audit plays a crucial role in providing reasonable assurance to the companies that cybersecurity risks are under control. Technology advancements require companies to look for more efficient means of providing this assurance. The following results of the narrative SLR present some of the approaches suggested and tested by researchers worldwide.

3.1. Suggested methodology to be applied

Some of the reviewed scientific papers present a variety of approaches to building methodology for IT security and auditing, indicating both similarities and differences in their methodologies, frameworks, and focal points.

Despite researchers presenting different perspectives, there are some similarities in the approaches presented. Lu (2022) and Khalili et al. (2018) both emphasise the importance of risk management in IT security. Mironeanu et al. (2021) also touch on risk management by addressing the need to effectively detect and prevent cyber-attacks to manage the risk posed by these threats.

All papers acknowledge the critical role of advanced technologies in enhancing IT security and auditing. For instance, Lu (2022) examines various technologies like cloud applications and blockchain, while Mironeanu et al. (2021) focus on ML methods for cyber-attack detection. Saleem et al. (2020) and Khalili et al. (2018) also integrate technology into their frameworks, with Saleem et al. (2020) proposing a model based on real attack analysis and Khalili leveraging ML techniques for quantitative security assessments.

Both Mironeanu et al. (2021) and Khalili et al. (2018) emphasise the importance of data in improving IT security. Mironeanu et al. propose an experimental framework for detecting cyber-attacks (ECAD) that relies heavily on data analysis. At the same time, Khalili et al. highlight the use of data to create personalised insurance policies.

The mentioned similarities are further supplemented by the authors' specific experience or research domains. Lu (2022) offers a comprehensive guide to IT auditing, covering various topics, including IT infrastructure, data usage, and management policies. This work balances theory and practice to provide a holistic view of IT audits. In contrast, Mironeanu et al. (2021) focus on real-time cyber-attack detection using a multi-layered framework. Their approach is more specialised, targeting specific threats in network security.

Lu (2022) proposes a methodological approach rooted in established standards and policies for IT auditing, aiming for a balanced view of theory and practice. Mironeanu et al. (2021) suggest a more experimental and real-time approach with their ECAD framework, emphasising the need for rapid detection and prevention.

Khalili et al. (2018) take a unique angle by addressing risk management through cyber insurance, an approach that transfers risk rather than solely focusing on prevention or detection, while Saleem et al. (2020) present a simplified, three-dimensional model focusing on the impacts of cyber-attacks on various aspects of data and system security.

Mironeanu et al. (2021), AL-Aamri et al. (2023) and Khalili et al. (2018) all utilise ML, but their applications differ. Mironeanu et al. and AL-Aaamri et al. apply ML for real-time cyber-attack detection within their ECAD framework. In contrast, Khalili et al. use ML to assess security profiles when designing insurance contracts.

Lu (2022) and Saleem et al. (2020) do not emphasise ML as heavily, with Lu providing a broader overview of technologies in IT audits and Saleem offering a conceptual model without a specific focus on ML.

Saleem et al. (2020) advocate for a straightforward approach to cybersecurity, emphasising basic security objectives and the impacts of attacks on data integrity and availability. Lu (2022) and Mironeanu et al. (2021) provide more detailed and context-specific frameworks addressing contemporary technologies and specific cyber threats.

The reviewed papers collectively underscore the evolving IT security and auditing landscape, each offering unique contributions. While there is a shared emphasis on risk management and integrating advanced technologies, the methodologies and specific focuses vary significantly. Lu (2022) provides a broad, balanced approach to IT audits, Mironeanu et al. (2021) specialise in real-time cyber-attack detection using ML, Khalili et al. (2018) explore risk transfer via cyber insurance, and Saleem et al. (2020) propose a simplified model based on real attack impacts. These diverse perspectives highlight the multifaceted nature of IT security and the need for varied strategies to address the complex challenges in this field.

3.2. Impact of risk management outcomes on IT audit

Another important aspect related to IT audits is properly managing cyber threat risk. One of the proposed approaches to managing cyber threat risk is an example of a method for automatically generating attack trees based on artificial intelligence, which can help assess cyber risk for critical infrastructure (Falco et al. (2018). This method uses the following techniques: 1) artificial intelligence planning, 2) definition of standard cybersecurity frameworks, and 3) system model description. The method aims to extract possible adversary strategies and attack paths. The method of automatically generating attack trees uses classical planning. Thanks to this, all possible attack paths that can achieve the goal the attacker sets can be calculated based on a set of attack rules. Attack rules are based on the combination of various existing security frameworks, e.g. the cyber kill chain, Internet of Things (IoT) attack surface,

Common Attack Pattern Enumeration and Classification (CAPEC), Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), Kali Linux, Common Vulnerabilities and Exposures (CVE) and others. As an example of an application, a sample ransomware attack (e.g., SamSam) is given, which can paralyse urban infrastructure and extort a ransom from local authorities.

Irshad and Basit Siddiqui (2023) propose an interesting approach to risk management from a broader perspective by linking cyber threats with information from cyber intelligence reports. Cyber intelligence is defined as a knowledge base that contains the context, behaviour, actions taken, and implications of cyber-attacks. The authors distinguish three levels of attribute identification: tools, tactics, techniques, and procedures (TTP) used by the attacker, the country behind the attack, and the specific person who carried out the attack. The last level is the most difficult to determine, as the attacker uses various hiding and disinformation techniques. The authors use various reference standards, such as ATT&CK, developed by MITRE corporation, APT Groups and Operations, and CAPEC. The data sources are unstructured cyber threat reports, which are published in various formats, such as text and PDF, by various entities, such as law enforcement agencies, security service providers, and bloggers. The aim of such research is to develop a mechanism for attributing or profiling cyber threats by extracting features from unstructured cyber threat reports. The authors propose a new embedding model known as "Attack2vec", which is trained on domain-specific embeddings from the cyber intelligence area. Irshad and Basit Siddiqui compare the results of their model with other methods and use machine learning algorithms, such as decision trees, random forests, and support vector machines, for cyber threat classification. During tests, the model achieved high results in terms of accuracy, precision, sensitivity, and F1 measure (also known as the F1 score, which is a statistical metric used to evaluate the performance of a classification model). A similar approach resulting in clustering attacks based on risk assessment results is proposed by Haddadpajouh et al. (2020).

Rosenberg (2018) proposes a somewhat controversial approach to attributing threats to specific countries. The author presents the first method of automatic attribution of advanced threats (APT) to specific countries, using deep neural networks (DNN) and dynamic analysis. An APT classifier has been developed that achieves high accuracy in identifying different APT families, which was developed in the past by the governments of specific countries. Based on this analysis, the model is able to attribute a given threat to a specific country. Another suggested possibility is to base on survey results (Zipperle et al., 2022) to learn more about experienced attacks.

It's worth mentioning that separate risk-management approaches are developed specifically for the banking industry (Kedarya & Elalouf, 2023; Thach et al., 2021).

Some authors (Ghanem et al., 2023) describe one aspect of risk management, in this case, compliance risk management. The article discusses the global pressure

exerted on an organisation to comply with cybersecurity standards and policies. Mentioned are methods of ensuring security compliance, such as Vulnerability Assessment (VA) and Penetration Testing (PT), which are used to identify gaps in security systems. A method called Expert-System Automated Security Compliance Framework (ESASCF) is presented, which allows for the automation of the SC process by extracting and reusing expert knowledge. The results of ESASCF tests on various networks showed significant time and effort savings. The document discusses various methods of using artificial intelligence for penetration testing and malware detection, with an emphasis on their effectiveness and degree of automation. Other authors (Koroniotis et al., 2019) suggest using survey results analysis to understand more about the threats coming from botnets operating in the IoT environment. There is the specific SHARKS model developed by Brown et al. (2022) and made available to discover unknown vectors of attacks in IoT environments and present it in a graphical way (Sarhan & Spruit, 2021; H. Kim et al., 2023). IoT environment is also a good playground for testing and adapting machine learning techniques for analysing traffic data (Chen et al., 2022).

Researchers also indicate that the threat landscape is continuously evolving (Kuppa & Le-Khac, 2022), requiring the security domain to constantly adapt and modify approaches to make them capable of hitting the moving target of emerging APTs.

In summary, although all four studies address aspects of cyber threat risk management, each adopts a distinct focus and methodology. Falco et al. (2018) emphasize the use of AI-generated attack trees, while Irshad and Basit Siddiqui 2023 concentrate on linking cyber threats with cyber intelligence reports. Rosenberg et al. (2018) explore the attribution of threats to specific countries, and Ghanem et al. (2023) examine compliance risk management. Each approach presents unique strengths and potential limitations, with their applicability and effectiveness varying depending on the specific context and objectives of the IT audit.

3.3. Security of solutions based on ML and AI

Many considerations regarding auditing ML solutions begin with the security analysis of using such solutions. One such consideration is presented in the work by Falco (2021). The article describes how the interdependence between the growing number of automated management systems and their security is becoming increasingly visible with the emergence of new incidents in the area of data access security. Falco proposes an independent audit of AI systems to ensure security and increase trust in these systems. The audit would be based on three principles: 1) prospective risk assessment, 2) operation tracking, and 3) adapting the system to the requirements of individual jurisdictions.

An independent audit of AI systems represents a pragmatic approach to the challenge of ensuring the security of automated systems, which, in the case of using traditional audit methods, would be cumbersome and impossible to enforce due to the costs associated with such a traditional approach.

The reviewed papers present five distinct approaches to managing cyber threat risk in the context of IT audits. Each approach utilises different methodologies and focuses on various aspects of cyber threat risk management. Comparison and contrast of these approaches highlight potential impacts on IT audit practices.

All approaches aim to manage cyber threats, emphasising the importance of identifying, analysing, and mitigating cyber-attack risks.

Both Falco et al. (2018) and Irshad and Basit Siddiqui (2023) incorporate AI and machine learning techniques in their methodologies. Falco et al. use AI to generate attack trees, while Irshad and Basit Siddiqui employ machine learning to classify and profile cyber threats.

The approaches leverage established cybersecurity frameworks. For instance, Falco et al. (2018) use frameworks such as the cyber kill chain and MITRE ATT&CK, while Irshad and Basit Siddiqui (2023) also reference MITRE ATT&CK, along with APT Groups and CAPEC.

Each method relies on data to drive its analysis. Falco et al. (2018) use attack rules derived from various security frameworks, Irshad and Basit Siddiqui (2023) analyse cyber intelligence reports, and Rosenberg et al. (2018) use data to attribute APTs to specific countries.

It's worth emphasising that the researchers also point out some important differences in perspectives on the solution's security.

Falco et al. (2018) focus on generating attack trees using AI planning to identify possible attack paths. Irshad and Basit Siddiqui (2023) link cyber threats with cyber intelligence reports using an embedding model (Attack2vec) for profiling and classification, and Rosenberg et al. (2018) attribute threats to specific countries using deep neural networks and dynamic analysis. As a supplement, Ghanem et al. (2023) emphasise compliance risk management through methods like Vulnerability Assessment and Penetration Testing, incorporating an automated compliance framework (ESASCF).

Falco et al. (2018) try to determine the suitable context for assessing risks in critical infrastructure scenarios, exemplified by a ransomware attack. Irshad and Basit Siddiqui (2023) look at broader applicability in profiling cyber threats and understanding attacker behaviour. In turn, Rosenberg et al. (2018) focused on the geopolitical implications of cyber threats, attributing attacks to specific nations. Ghanem et al. (2023) analysed the other interesting perspective, which aimed to ensure organisational compliance with cybersecurity standards, focusing on automation and efficiency.

Regarding the depth of analyses presented, there are also differences in the approaches suggested. Falco et al. (2018) empirically analyse potential attack paths using AI-generated

models. Irshad and Basit Siddiqui (2023) promote in-depth profiling of attackers based on unstructured cyber intelligence reports. Rosenberg et al. (2018) present a controversial focus on the attribution of sophisticated APTs to nations, requiring extensive data and deep learning models.

Falco et al. (2018) promote the use of classical AI planning and standard cybersecurity frameworks, while Irshad and Basit Siddiqui (2023) successfully implement a new embedding model (Attack2vec) and machine learning algorithms like decision trees, random forests, and SVM. Rosenberg et al. (2018) present a more ambitious approach by employing deep neural networks and dynamic analysis for APT attribution. Conversely, Ghanem et al. (2023) utilise the ESASCF framework for automating security compliance processes. The studies mentioned above provide significant input for consideration of the impact on IT Audit.

The AI-generated attack trees Falco et al. (2018) and the profiling of cyber threats Irshad and Basit Siddiqui (2023) provide comprehensive tools for assessing potential risks and understanding attacker strategies. This can enhance the depth and accuracy of IT audits.

The methodologies by Rosenberg et al. (2018) and Irshad and Basit Siddiqui (2023) contribute to better attribution and profiling of cyber threats, which is crucial for understanding the origin and nature of attacks. This knowledge can inform audit strategies and responses.

Ghanem et al. (2023) approach to compliance risk management ensures that organisations meet cybersecurity standards efficiently. This focus on compliance is vital for IT audits, which often include evaluating adherence to regulatory requirements.

Mirsky et al. (2023) take different perspectives from ethics and discuss how cyber adversaries can use AI maliciously to enhance attacks and expand campaigns against organisations. They identify 32 offensive AI capabilities that adversaries can use, such as deepfake creation, automated spear phishing, and lateral movement in networks.

All approaches recognise the evolving nature of cyber threats and incorporate techniques to adapt to new attack vectors. This adaptability is essential for IT audits, which must remain relevant in a rapidly changing threat landscape.

Each of the five approaches to risk management in IT auditing offers unique methodologies, each emphasizing distinct aspects of cyber threat risk. While they share the common objective of identifying and mitigating cyber risks through advanced technologies and frameworks, their specific techniques and applications differ significantly. Integrating these diverse approaches can enable IT auditors to conduct more comprehensive and robust assessments of cyber threat risks, thereby enhancing the overall security posture of the organizations under evaluation.

3.4. Analytic techniques adopted

The various approaches to IT audit analytic techniques presented in the reviewed papers can be grouped based on their primary focus areas: network traffic analysis, code analysis, and attacker behaviour analysis.

Approaches and techniques proposed for Network Traffic Analysis are the following:

- Ahmed et al. (2021) propose a method using the Cyber Kill Chain (CKC) and machine learning to detect Advanced Persistent Threats (APT). They utilise a publicly available dataset, reconstruct data according to CKC stages, and apply five machine learning algorithms to classify attack stages;
- Neuschmied et al. (2022) use multi-stage autoencoders for unsupervised learning and dimensionality reduction to detect APTs in network systems, employing various statistical techniques for feature reliability;
- Kumar (2020) combines multi-objective genetic algorithms (MOGA) and neural networks (NN) in a hybrid model for intrusion detection, using majority voting to combine ensemble solutions;
- Saini et al. (2023) focus on detecting APT attacks using a hybrid ensemble model that combines random forest and XGBoost with feature selection techniques like Pearson correlation, information gain, and SHAP;
- Alsanad and Altuwaijri (2022) apply feature reduction using principal component analysis on the CSE-CIC-IDS2018 dataset and compare five machine learning classifiers;
- Fernandez Maimo et al. (2018) propose an anomaly detection system for 5G networks using deep learning techniques that adapt to changes in network load;
- Campazas-Vega et al. (2020) present an approach to detecting malicious network traffic using supervised learning models. Several models that have achieved high detection accuracy using datasets like UNSW-NB15 are mentioned;
- Myneni et al. (2023) discuss the creation of 'Unraveled,' a semi-synthetic dataset designed to capture Advanced Persistent Threat (APT) attacks, addressing the lack of realistic cybersecurity datasets for sophisticated and persistent cyber-attack features.

All methods utilise machine learning and statistical techniques to analyse and classify network traffic data. They aim to detect anomalies and threats in network systems, emphasising the need for accurate feature extraction and selection. Several approaches, like those by Ahmed et al. (2021), Alsanad and Altuwaijri (2022), and Saini et al. (2023), employ ensemble methods to improve detection accuracy.

There are also some differences pointed out by the authors. Ahmed et al. (2021) focus specifically on classifying attack stages using the CKC framework, while Saini et al. (2023) and Kumar (2020) use hybrid models combining multiple algorithms for broader intrusion detection.

Neuschmied et al. (2022) and Fernandez Maimo et al. (2018) emphasise unsupervised learning and adaptation to network changes, whereas Ahmed et al. (2021) and Alsanad and Altuwaijri (2022) rely on supervised machine learning techniques.

Fernandez Maimo et al. (2018) specifically target 5G networks, highlighting a specialised application area not covered by the other approaches.

Approaches and techniques suggested for Code Analysis are the following:

- Lacombe et al. (2023) focus on reducing potential injection points for malicious software using heuristics based on dependency analysis, occurrence limitation, limiting, and unfolding strategies;
- Li et al. (2020) analyse PHP source code sequences to detect potential XSS attacks by building a model to extract relevant information from data streams;
- Mosa et al. (2023) developed a machine-learning model to detect phishing websites, considering URL features, source code, and threat intelligence.

All approaches focus on analysing source code to detect vulnerabilities and potential malware injections. They aim to enhance existing security measures by identifying points of weakness that traditional techniques might overlook.

There are also some differences pointed out by the authors. Lacombe et al. (2023) emphasise heuristics to reduce injection points in the software development process, providing a broad set of strategies for various scenarios. Li et al. (2020) concentrate on detecting specific types of attacks (XSS) in PHP code, offering a more targeted approach to code analysis.

Approaches and techniques suggested for Attacker Behavior Analysis are the following:

- Xiao et al. (2018) apply the cumulative theory of perspective (CPT) to study interactions between cyber systems and APT attackers, considering psychological effects and decision-making under uncertainty;
- Y. Kim et al. (2023) propose the Bayesian ATT&CK Network (BAN) model, which uses Bayesian networks and the MITRE ATT&CK template to predict APT attack techniques and corresponding defensive measures;
- Ghafir et al. (2019) propose a novel intrusion detection system for APT detection and prediction, utilising two main phases: attack scenario reconstruction and attack decoding using Hidden Markov Models (HMM).

All approaches analyse the behaviour and strategies of attackers to improve threat detection and prediction. They utilise advanced theoretical frameworks (CPT and Bayesian networks) to model interactions and predict attack patterns.

There are also some differences pointed out by the authors. Xiao et al. (2018) focus on the psychological aspects of attacker decision-making and its impact on detection performance, incorporating game theory and decision-making under uncertainty, while Y. Kim et al. (2023) use Bayesian networks and expert knowledge to predict attack techniques, offering a more structured and data-driven approach to behaviour analysis.

In contemporary IT audit practices, a comparative analysis between traditional methodologies and AI-enhanced techniques highlights a transformative shift in addressing modern cybersecurity challenges. Traditional IT audit methodologies rely heavily on predefined control frameworks and manual inspection processes, often limiting their ability to adapt dynamically to evolving cyber threats such as APTs (Canada, 2020). These conventional methods, while systematic, often face challenges in scalability and precision when processing vast, complex datasets typically seen in large-scale IT environments.

In contrast, AI-enhanced techniques introduce a paradigm shift by leveraging machine learning algorithms and data-driven insights. These approaches, as evidenced by recent studies, integrate advanced anomaly detection models, such as hybrid ensemble learning, clustering algorithms, and graph neural networks, to proactively identify and respond to threats (Ramamoorti et al., 1999). AI-based methodologies can analyse intricate behavioural patterns and uncover hidden correlations in real-time, providing auditors with actionable intelligence that traditional methods might overlook. This integration fosters not only enhanced accuracy in detecting irregularities but also significant improvements in efficiency by automating routine audit tasks and focusing human expertise on higher-order decision-making.

By juxtaposing these approaches, the analysis underscores the necessity of embracing AI to address the limitations of traditional methods, particularly in areas requiring agility, scalability, and predictive capabilities, thereby fortifying IT audit processes against contemporary cybersecurity risks.

Other Approaches suggested by some researchers:

- Zhen and Gao (2023) present the Robustly optimised BERT approach-Whole Word Masking-Residual Dilated Convolutional Neural Network-Conditional Random Field (RoBERTa-wwm-RDCNN-CRF) model for recognising proper names in the Chinese cyber threat environment;
- M. M. Hasan et al. (2023) use several boosting methods and an explainable AI tool based on Shapley values (SHAP) for predicting APT attacks and visualising model results;
- Javed et al. (2023) introduce a new approach using Graph Attention Network (GAN), a multi-dimensional algorithm that captures behavioural features to detect hidden APT attacks in I-IoT-enabled CPS with high accuracy and real-time performance. Graph usage is also analysed by Rabzelj et al. (2023);
- Khalid et al. (2023) highlight the adoption of game theory as a strategic approach to understanding and analysing the interactions between attackers and defenders in the context of APTs, optimising defensive performance and anticipating countermeasures. Wan et al. (2023) discuss the use of defensive deception in cyber security, employing information asymmetry to mislead attackers and protect systems;

- Kim et al. (2021) propose a machine learning-based method that does not rely on domain experts' knowledge for feature extraction. The method preserves sequential information of log data, which is crucial for identifying anomalies;
- Koroniotis et al. (2020) highlight the security threats posed by the integration of IoT devices in smart airports, emphasising the need for advanced cybersecurity measures;
- Qiu et al. (2019) propose a method to predict the impact of Android malware on security and privacy.

From a major perspective, all methods present ready models that utilise machine learning and AI for specific cybersecurity tasks, and they emphasise the importance of model interpretability and feature analysis for effective threat detection. However, Zhen and Gao (2023) focus on a linguistic model tailored to the context of the Chinese language and cyber threat. M. M. Hasan et al. (2023) employ general machine-learning techniques for broader APT attack prediction. Hasan et al. also emphasise the use of explainable AI to interpret and visualise model outcomes, enhancing the transparency and understanding of AI-driven predictions.

The approaches to IT audit analytic techniques exhibit diverse methodologies and focal points. While network traffic analysis remains a predominant focus, code analysis and attacker behaviour analysis offer valuable insights into specific aspects of cybersecurity. Each method brings some strengths, from machine learning and statistical techniques to psychological theories and heuristic strategies. Understanding these similarities and differences helps in selecting the appropriate analytic technique for specific IT audit and cybersecurity needs.

3.5. New research areas suggested by the literature

Future research directions in IT auditing and cybersecurity highlight several critical areas, offering fertile ground for researchers seeking to advance this field. Below are the suggested topics and actionable insights for researchers interested in building upon these studies:

- Automatic Detection and Classification of APTs: Researchers could focus on developing AI-driven systems capable of independently detecting and classifying APTs. Exploring the use of unsupervised learning algorithms, transfer learning, and reinforcement learning can help reduce the reliance on human intervention. Collaborations with cybersecurity firms to access real-world datasets would enhance the applicability of such systems (Ahmed et al., 2021).
- Blockchain Technology and 5G/6G Networks in IoT: Investigating blockchain's potential for securing 5G/6G communication infrastructures and IoT ecosystems can pave the way for secure, decentralised frameworks. Researchers should explore integrating blockchain with quantum-safe cryptography to address future threats.

Testing these systems in controlled environments simulating smart cities or healthcare networks could yield valuable insights (Ali et al., 2023).

- Service Scaling and Attack Prevention: The scalability of cybersecurity solutions, such as using Docker containers, can be enhanced by focusing on dynamic resource allocation methods and vulnerability detection mechanisms. Researchers might develop tools for detecting MAC address spoofing and proactive defence systems based on anomaly detection using real-time data streams. Modelling novel attack patterns and conducting red-team simulations can prepare organisations for external threats (Mironeanu et al., 2021).
- Deep Learning for DNS Data Analysis: Advancing deep learning methods, particularly focusing on large-scale DNS traffic data, could significantly improve threat detection. Researchers should experiment with transformer models for sequence data and contrastive learning for anomaly detection. Partnering with internet service providers for diverse and large datasets can further validate findings (Alsanad & Altuwaijri, 2022).
- Knowledge Graphs for Cyber Threats: A flexible, context-aware approach to identifying cyber threats using system kernel audit records and knowledge graphs can enhance detection accuracy. Researchers could explore combining graph neural networks (GNNs) with domain-specific ontologies to model complex dependencies in cybersecurity events. Open-source tools like Neo4j or GraphDB might support this research direction (Yang et al., 2022).
- Advanced Source Code Analysis: Developing methodologies to analyse multiple execution branches and detect vulnerabilities in source code is critical. Researchers could employ symbolic execution combined with ML-based pattern recognition to address this gap. Expanding these techniques to cover programming languages beyond PHP and focusing on supply chain security risks could add value (Li et al., 2020).
- Language-Specific Cybersecurity Models: Tailored linguistic models, such as one for recognising proper names in Chinese cyber threat environments, are vital for region-specific applications. Researchers could adapt pre-trained natural language models like BERT or GPT to cybersecurity-specific tasks, ensuring accurate threat representation in diverse linguistic contexts (Zhen & Gao, 2023).
- Hybrid Cyber Threat Detection: Developing hybrid models that combine rule-based systems with ML for effective threat detection can enhance reliability. Researchers should investigate ensemble approaches that leverage the strengths of decision trees, neural networks, and probabilistic models. Testing these models in controlled attack scenarios will validate their robustness (M. M. Hasan et al., 2023).
- Cyber Defense for 5G Networks: Exploring new analytical technologies for robust defence architectures tailored to 5G networks can address emerging challenges. Researchers might focus on anomaly detection for edge computing nodes, network

slicing security, and adaptive AI-driven intrusion detection systems (Fernandez Maimo et al., 2018).
- Solutions for SMEs: Tailored cybersecurity solutions for small and medium-sized enterprises (SMEs) could address resource constraints. Researchers could focus on lightweight, cost-effective tools that integrate with existing SME infrastructures. Designing user-friendly interfaces and scalable models will improve adoption rates (Ilca et al., 2023).

4. Conclusion

Integrating AI and ML techniques in IT auditing signifies a paradigm shift in enhancing cybersecurity measures. This comprehensive review highlights these technologies' critical role in advancing IT audit methodologies through improved risk management, technological integration, and data-driven approaches.

A central theme across the analysed literature is the emphasis on risk management, with frameworks like TARA playing a critical role in guiding organisations toward strategic responses to cyber risks. The integration of AI into real-time risk assessment aligns closely with the TARA framework, as AI enhances the ability to detect, assess, and respond to threats dynamically. For instance, AI-driven predictive analytics can identify potential vulnerabilities, enabling organisations to decide whether to transfer risks through cyber insurance, accept residual risks, reduce exposure via mitigation measures, or avoid risks entirely by reconfiguring systems. Advanced technologies, including cloud computing, blockchain, and machine learning, further bolster the implementation of TARA by providing scalable, automated, and data-driven capabilities. These innovations enable IT audit frameworks to evolve into proactive and adaptive systems capable of real-time threat assessment and decision-making, effectively operationalising the principles of the TARA framework to address the complex landscape of cybersecurity challenges.

Data-driven approaches are fundamental in enhancing IT security. The use of Experimental Frameworks for Detecting Cyber-Attacks (ECAD) and data analysis for personalised insurance policies exemplify the significance of leveraging data in audit processes. The diversity in focus among studies – from broad overviews of IT infrastructure to specialised frameworks for real-time threat detection – reflects the multifaceted nature of IT security and the necessity for adaptable audit strategies.

ML's application in IT auditing is a recurring and significant theme. Its use in real-time cyber-attack detection and quantitative security assessments showcases its potential to improve audit effectiveness substantially. Additionally, integrating ML with traditional audit techniques allows for more comprehensive and accurate evaluations.

The methodologies reviewed reveal varied perspectives on cybersecurity. While some advocate for straightforward approaches, others propose detailed, context-specific

frameworks addressing contemporary technologies and cyber threats. This diversity in approaches highlights the need for flexible and adaptive auditing frameworks to address the evolving landscape of IT security.

For IT audit practitioners, the integration of AI and ML offers practical tools to enhance audit efficiency and effectiveness. These technologies can be employed to automate routine audit tasks, such as data classification, anomaly detection, and compliance verification, thereby allowing auditors to focus on higher-level strategic assessments. Machine learning models, like those used for detecting APTs or profiling attacker behaviour, enable practitioners to identify vulnerabilities and risks in real-time, facilitating a proactive approach to cybersecurity. Additionally, AI-driven frameworks, such as automated attack tree generation or embedding models like "Attack2vec," can simplify complex risk assessments and threat attribution processes. By adopting these advanced techniques, IT auditors can provide more robust assurance of security controls, improve incident detection and response strategies, and align audit findings with organisational risk management objectives. Ultimately, these tools empower auditors to deliver more comprehensive and actionable insights, supporting organisations in mitigating risks and enhancing their cybersecurity posture.

Despite their potential, integrating AI and ML into IT audits comes with limitations that practitioners must consider. These technologies often require significant computational resources, specialised expertise, and high-quality data to deliver accurate and reliable results, which can be a barrier for smaller organisations or those with limited budgets. Additionally, machine learning models are inherently susceptible to biases present in the training data, which may lead to inaccurate or unfair outcomes. There is also a risk of over-reliance on automated systems, which could undermine critical human judgment in nuanced audit scenarios. Furthermore, the lack of standardised frameworks for auditing AI and ML systems themselves raises concerns about transparency, interpretability, and accountability, particularly when errors occur. Addressing these limitations is crucial to ensuring the effective and ethical application of AI and ML in IT audits.

The evolving threat landscape necessitates continuous adaptation and innovation in auditing methodologies. AI and ML provide powerful tools to enhance the accuracy, efficiency, and comprehensiveness of IT audits. By incorporating these technologies, IT auditors can better identify, analyse, and mitigate cyber risks, thereby significantly improving organisations' overall security posture.

In conclusion, integrating AI and ML into IT auditing is not merely a technological advancement but a fundamental shift in how audits are conducted. These technologies enable a more proactive, data-driven, and comprehensive approach to managing cyber threats. We believe that the insights from this SLR offer valuable guidance for researchers, practitioners, and policymakers in leveraging AI and ML to enhance IT audit methodologies and ensure robust cybersecurity measures.

Authors' contribution

M.P.: article conception, theoretical content of the article, research methods applied, conducting the research, data collection, analysis and interpretation of results, draft manuscript preparation. **M.Z.:** article conception, theoretical content of the article, analysis and interpretation of results, draft manuscript preparation review & editing.

References

Ahmed, Y., Asyhari, A. T., & Rahman, MdA. (2021). A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Computers, Materials and Continua*, *67*(2), 2497–2513. https://doi.org/10.32604/cmc.2021.014223

AL-Aamri, A. S., Abdulghafor, R., Turaev, S., Al-Shaikhli, I., Zeki, A., & Talib, S. (2023). Machine Learning for APT Detection. *Sustainability (Switzerland)*, *15*(18). https://doi.org/10.3390/su151813820

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173629

Ali, A., Al-rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors*, *23*(15). https://doi.org/10.3390/s23156762

Alsanad, A., & Altuwaijri, S. (2022). Advanced Persistent Threat Attack Detection using Clustering Algorithms. *International Journal of Advanced Computer Science and Applications*, *13*(9), 640–649. https://doi.org/10.14569/IJACSA.2022.0130976

Appelbaum, D. (2017). *Public Auditing, Analytics, and Big Data in the Modern Economy* [Doctoral dissertation, The State University of New Jersey]. RUcore: Rutgers University Community Repository. https://doi.org/doi:10.7282/T3R49TQ2

Benzekri, A., Laborde, R., Oglaza, A., Rammal, D., & Barrere, F. (2019). Dynamic security management driven by situations: An exploratory analysis of logs for the identification of security situations. *2019 3rd Cyber Security in Networking Conference, CSNet 2019*, 66–72. https://doi.org/10.1109/CSNet47905.2019.9108976

Brown, J., Saha, T., & Jha, N. K. (2022). GRAVITAS: Graphical Reticulated Attack Vectors for Internet-of-Things Aggregate Security. *IEEE Transactions on Emerging Topics in Computing*, *10*(3), 1331–1348. https://doi.org/10.1109/TETC.2021.3082525

Buchanan, S., & Gibb, F. (2008). The information audit: Theory versus practice. *International Journal of Information Management*, *28*(3), 150–160. https://doi.org/10.1016/j.ijinfomgt.2007.09.003

Calderon, T. G., & Cheh, J. J. (2002). A roadmap for future neural networks research in auditing and risk assessment. *International Journal of Accounting Information Systems*, *3*(4), 203–236. https://doi.org/10.1016/S1467-0895(02)00068-4

Campazas-Vega, A., Crespo-Martínez, I. S., Guerrero-Higueras, Á. M., & Fernández-Llamas, C. (2020). Flow-data gathering using netflow sensors for fitting malicious-traffic detection models. *Sensors (Switzerland)*, *20*(24), 1–13. https://doi.org/10.3390/s20247294

Chartered Professional Accountants of Canada. (n.d.). The Data-Driven Audit: How Automation and AI are Changing the Audit and the Role of the Auditor. Retrieved June, 04, 2024 from: https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/data-driven-audit-ai-automation-impact?utm_source=chatgpt.com

Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine Learning Enabled IoT Security: Open Issues and Challenges under Advanced Persistent Threats. *ACM Computing Surveys*, *55*(5). https://doi.org/10.1145/3530812

Cristea, M. A. (2021). Operational risk management in banking activity. *IBIMA Business Review*, *2021*. https://doi.org/10.5171/2021.969612

Falco, G., Shneiderman, B., Badger, J., Carrier, R., Dahbura, A., Danks, D., Eling, M., Goodloe, A., Gupta, J., Hart, C., Jirotka, M., Johnson, H., LaPointe, C., Llorens, A. J., Mackworth, A. K., Maple, C., Pálsson, S. E., Pasquale, F., Winfield, A., & Yeong, Z. K. (2021). Governing AI safety through independent audits. In *Nature Machine Intelligence*, *3*(7). https://doi.org/10.1038/s42256-021-00370-7

Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities. *IEEE Access*, *6*, 48360–48373. https://doi.org/10.1109/ACCESS.2018.2867556

Fernandez Maimo, L., Perales Gomez, A. L., Garcia Clemente, F. J., Gil Perez, M., & Martinez Perez, G. (2018). A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *IEEE Access*, *6*. https://doi.org/10.1109/ACCESS.2018.2803446

Ghafir, I., Kyriakopoulos, K. G., Lambotharan, S., Aparicio-Navarro, F. J., Assadhan, B., Binsalleeh, H., & Diab, D. M. (2019). Hidden markov models and alert correlations for the prediction of advanced persistent threats. *IEEE Access*, *7*. https://doi.org/10.1109/ACCESS.2019.2930200

Ghanem, M. C., Chen, T. M., Ferrag, M. A., & Kettouche, M. E. (2023). ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance. *IEEE Access*, *11*, 129840–129853. https://doi.org/10.1109/ACCESS.2023.3332834

Haddadpajouh, H., Azmoodeh, A., Dehghantanha, A., & Parizi, R. M. (2020). MVFCC: A Multi-View Fuzzy Consensus Clustering Model for Malware Threat Attribution. *IEEE Access*, *8*, 139188–139198. https://doi.org/10.1109/ACCESS.2020.3012907

Hasan, A. R. (2022). Artificial Intelligence (AI) in Accounting & Auditing: A Literature Review. *Open Journal of Business and Management*, *10*(01), 440–465. https://doi.org/10.4236/ojbm.2022.101026

Hasan, M. M., Islam, M. U., & Uddin, J. (2023). Advanced Persistent Threat Identification with Boosting and Explainable AI. *SN Computer Science*, *4*(3). https://doi.org/10.1007/s42979-023-01744-x

Ilca, L. F., Lucian, O. P., & Balan, T. C. (2023). Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. *Sensors*, *23*(15). https://doi.org/10.3390/s23156757

Irshad, E., & Basit Siddiqui, A. (2023). Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal*, *24*(1), 43–59. https://doi.org/10.1016/j.eij.2022.11.001

Javed, S. H., Ahmad, M. B., Asif, M., Akram, W., Mahmood, K., Das, A. K., & Shetty, S. (2023). APT Adversarial Defence Mechanism for Industrial IoT Enabled Cyber-Physical System. *IEEE Access*, *11*, 74000–74020. https://doi.org/10.1109/ACCESS.2023.3291599

Kedarya, T., & Elalouf, A. (2023). Risk Management Strategies for the Banking Sector to Cope with the Emerging Challenges. *Foresight and STI Governance*, *17*(3), 68–76. https://doi.org/10.17323/2500-2597.2023.3.68.76

Khalid, M. N. A., Al-Kadhimi, A. A., & Singh, M. M. (2023). Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review. *Mathematics*, *11*(6). https://doi.org/10.3390/math11061353

Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security*, *13*(9), 2226–2239. https://doi.org/10.1109/TIFS.2018.2812205

Kim, C., Jang, M., Seo, S., Park, K., & Kang, P. (2021). Intrusion Detection Based on Sequential Information Preserving Log Embedding Methods and Anomaly Detection Algorithms. *IEEE Access*, *9*, 58088–58101. https://doi.org/10.1109/ACCESS.2021.3071763

Kim, H., Hwang, E., Kim, D., Cho, J. H., Moore, T. J., Nelson, F. F., & Lim, H. (2023). Time-Based Moving Target Defense Using Bayesian Attack Graph Analysis. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3269018

Kim, Y., Lee, I., Kwon, H., Lee, K., & Yoon, J. (2023). BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework. *IEEE Access*, *11*, 91949–91968. https://doi.org/10.1109/ACCESS.2023.3306593

Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews*. Keele University Technical Report TR/SE-0401. https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Kitchenham, B. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Keele University and Durham University. https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, *14*(1), 115–122. https://doi.org/10.2308/jeta-51730

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access*, *8*, 209802–209834. https://doi.org/10.1109/ACCESS.2020.3036728

Koroniotis, N., Moustafa, N., & Sitnikova, E. (2019). Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions. In *IEEE Access*, *7*, 61764–61785. https://doi.org/10.1109/ACCESS.2019.2916717

Kumar, G. (2020). An improved ensemble approach for effective intrusion detection. *Journal of Supercomputing*, *76*(1), 275–291. https://doi.org/10.1007/s11227-019-03035-w

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

Lacombe, G., Feliot, D., Boespflug, E., & Potet, M. L. (2023). Combining static analysis and dynamic symbolic execution in a toolchain to detect fault injection vulnerabilities. *Journal of Cryptographic Engineering, 14,* 147–164. https://doi.org/10.1007/s13389-023-00310-8

Li, C., Wang, Y., Miao, C., & Huang, C. (2020). Cross-site scripting guardian: A static XSS detector based on data stream input-output association mining. *Applied Sciences (Switzerland)*, *10*(14). https://doi.org/10.3390/app10144740

Lu, W. (2022). Cybersecurity Data Science: Concepts, Algorithms, and Applications. In I., Woungang, S.K. Dhurandher, (Eds.). 4th International Conference on Wireless, Intelligent and Distributed

Environment for Communication. *94* (pp. 21-30). Springer, Cham. https://doi.org/10.1007/978-3-030-89776-5_2

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence. *AI Magazine*, *27*(4), 12–14.

Mironeanu, C., Archip, A., Amarandei, C. M., & Craus, M. (2021). Experimental cyber-attack detection framework. *Electronics (Switzerland)*, *10*(14). https://doi.org/10.3390/electronics10141682

Mirsky, Y., Demontis, A., Kotak, J., Shankar, R., Gelei, D., Yang, L., Zhang, X., Pintor, M., Lee, W., Elovici, Y., & Biggio, B. (2023). The Threat of Offensive AI to Organizations. In *Computers and Security*, *124*, 103006. https://doi.org/10.1016/j.cose.2022.103006

Mladenic, Dunja., Lavrač, Nada., Bohanec, Marko., & Moyle, Steve. (2003). *Data Mining and Decision Support Integration and Collaboration*. Springer US. https://doi.org/10.1007/978-1-4615-0286-9

Mosa, D. T., Shams, M. Y., Abohany, A. A., El-Kenawy, E.-S. M., & Thabet, M. (2023). Machine Learning Techniques for Detecting Phishing URL Attacks. *Computers, Materials and Continua*, *75*(1), 1271–1290. https://doi.org/10.32604/cmc.2023.036422

Myneni, S., Jha, K., Sabur, A., Agrawal, G., Deng, Y., Chowdhary, A., & Huang, D. (2023). Unravelled — A semi-synthetic dataset for Advanced Persistent Threats. *Computer Networks*, *227*, 109688. https://doi.org/10.1016/J.COMNET.2023.109688

Neuschmied, H., Winter, M., Stojanović, B., Hofer-Schmitz, K., Božić, J., & Kleb, U. (2022). APT-Attack Detection Based on Multi-Stage Autoencoders. *Applied Sciences (Switzerland)*, *12*(13), 6816. https://doi.org/10.3390/app12136816

Omoteso, K. (2012). The application of artificial intelligence in auditing: Looking back to the future. In *Expert Systems with Applications*, *39*(9), 8490-8495. https://doi.org/10.1016/j.eswa.2012.01.098

Rabzelj, M., Bohak, C., Juznic, L. S., Kos, A., & Sedlar, U. (2023). Cyberattack Graph Modeling for Visual Analytics. *IEEE Access*, *11*, 86910-86944. https://doi.org/10.1109/ACCESS.2023.3304640

Ramamoorti, S., Bailey Jr, A. D., & Traver, R. O. (1999). Risk assessment in internal auditing: a neural network approach. *International Journal of Intelligent Systems in Accounting, Finance & Management*, *8*(3), 159–180. https://doi.org/10.1002/(SICI)1099-1174(199909)8:3<159::AID-ISAF169>3.0.CO;2-W

Rosenberg, I., Sicard, G., & David, E. (2018). End-to-end deep neural networks and transfer learning for automatic analysis of nation-state malware. *Entropy*, *20*(5), 390. https://doi.org/10.3390/e20050390

Saini, N., Bhat Kasaragod, V., Prakasha, K., & Das, A. K. (2023). A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection. *Concurrency and Computation: Practice and Experience*, *35*(28), e7865. https://doi.org/10.1002/cpe.7865

Saleem, D., Sundararajan, A., Sanghvi, A., Rivera, J., Sarwat, A. I., & Kroposki, B. (2020). A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems. *IEEE Systems Journal*, *14*(1), 17–27. https://doi.org/10.1109/JSYST.2019.2919464

Sarhan, I., & Spruit, M. (2021). Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph. *Knowledge-Based Systems*, *233*, 107524. https://doi.org/10.1016/j.knosys.2021.107524

Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

Thach, N. N., Hanh, H. T., Huy, D. T. N., Gwoździewicz, S., Nga, L. T. V., Huong, L. T. T., & Nam, V. Q. (2021). Technology quality management of the industry 4.0 and cybersecurity risk man-

agement on current banking activities in emerging markets - the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. In *British Journal of Management*, *14*(3), 207-222. https://doi.org/10.1111/1467-8551.00375

Wan, Z., Cho, J.-H., Zhu, M., Anwar, A. H., Kamhoua, C. A., & Singh, M. P. (2023). Resisting Multiple Advanced Persistent Threats via Hypergame-Theoretic Defensive Deception. *IEEE Transactions on Network and Service Management*, *20*(3), 3816–3830. https://doi.org/10.1109/TNSM.2023.3240366

Xiao, L., Xu, D., Mandayam, N. B., & Poor, H. V. (2018). Attacker-Centric View of a Detection Game against Advanced Persistent Threats. *IEEE Transactions on Mobile Computing*, *17*(11), 2512-2523. https://doi.org/10.1109/TMC.2018.2814052

Yang, F., Han, Y., Ding, Y., Tan, Q., & Xu, Z. (2022). A flexible approach for cyber threat hunting based on kernel audit records. *Cybersecurity*, *5*, 11. https://doi.org/10.1186/s42400-022-00111-2

Zhen, Z., & Gao, J. (2023). Chinese Cyber Threat Intelligence Named Entity Recognition via RoBERTa-wwm-RDCNN-CRF. *Computers, Materials and Continua*, *77*(1), 299–321. https://doi.org/10.32604/cmc.2023.042090

Zipperle, M., Gottwalt, F., Chang, E., & Dillon, T. (2022). Provenance-based Intrusion Detection Systems: A Survey. *ACM Computing Surveys*, *55*(7), 1-36. https://doi.org/10.1145/3539605