DOI: https://doi.org

International Journal of Advanced and Innovative Research
Journal homepage :https://scholarclub.org/index.php/IJAIR/login

AI-Driven Cybersecurity Threat Detection Using Machine Learning and Data Analytics in Cloud Computing Environments

Altaf Mazhar Soomro (Coresponding Author)
altaf.m.soomro@alumini.uts.edu.au
University of Technology,Sydney,Australia

ARTICLE INFO: **ABSTRACT**

Received:
30 06 2026
Revised:
15 07 2026
Accepted:
15 08 2026

Keywords:
Artificial Intelligence, Machine Learning, Cybersecurity Threat Detection, Cloud Computing Security, Data Analytics, Explainable AI, Adaptive Security

Cloud computing has made its way into the daily operations of businesses, changing the way they store, manage and share data, and at the same time expanding the scope, complexity, and dynamism of cyber threats.Cloud computing has been adopted by many organisations and impacts the way in which organisations store, process and share information while growing the size, complexity and dynamism of cyber threats. Cloud environments feature distributed infrastructure, virtual resources, interdependent services, ever-evolving workloads, and massive amounts of data concerning security. These qualities are problematic for detection, often beyond the ability of traditional rules-based, signature-driven and/or manually monitored cybersecurity strategies. Targeted attacks can be hard to detect when they display new attack patterns, rapidly evolve, leverage legitimate cloud services or are introduced on multiple interconnected services. Within this context, artificial intelligence (AI), machine learning (ML) and data analytics have grown in importance as solutions to enhance intelligent and adaptive cybersecurity threat detection.The study focuses on qualitative analysis of the role of AI-based techniques, specifically machine learning and data analytics, in cybersecurity threat detection for cloud computing environments. The method used in the study is interpretive, exploratory, and documentary research method which is secondary evidence research. Relevant evidence is conceptually synthesized from peer reviewed scholarly literature, systematic and review studies, cybersecurity research, cloud-security publications, industry and security reports, standards, technical documents and authoritative institutional sources. Instead of building and testing a new machine-learning model, this study uses the existing knowledge to determine key patterns, challenges, opportunities, and practical implications of cloud threat detection using AI.The five areas identified using thematic analysis are interlinked. First, AI and ML can help detect more intelligently by detecting complex patterns of behavior and potentially even recognizing anomalies that might not be identified through traditional methods. Second, data analytics allows for analysis of diverse cloud-security data across networks, applications, devices, workloads, logs, and other distributed sources. Third, AI-powered solutions provide possibilities to deal with new and advanced threats using adaptive and behaviour-based detection. Fourth, they are affected by the quality of the data, false positive rates, explainability, privacy, security of training data, and organizational trust. Last but not least, when AI is integrated with other components of the cloud-security ecosystem, such as monitoring, incident-response, and security operations centers, it can enhance security operations in real time and adapt to the changing nature of threats.The study offers a conceptual analysis of how AI-enabled cybersecurity

detection is a more holistic socio-technical ability than an algorithmic one. In practice, the findings indicate that organizations and cybersecurity practitioners should assess different types of AI-based detection based on the quality and variety of data they have, the interpretability of security decisions, their ability to adapt to new threats, their privacy policies, their operational context, and how well they fit into their current security infrastructure. In summary, the success of AI-driven threat detection in cloud computing relies on a combination of advanced algorithms and reliable data sources, transparent decision-making processes, adaptability, privacy-focused measures, and seamless integration with cloud-security frameworks. This holistic view can help in creating more resilient, responsive, and intelligent cybersecurity strategies in today's more complex cloud environments.

INTRODUCTION

Cloud computing has significantly altered modern-day information infrastructures by providing access to scalable computing resources, distributed applications, virtualized services and data intensive platforms via inter-connected digital environments. This has also created an increased area for cybersecurity attacks. Cloud environments, in contrast to traditional infrastructures that might heavily depend on a single organization and a defined organizational boundary, are built on distributed resource pools, dynamically changing workloads, remote access, virtualization, application programming interfaces and more and more combinations of public, private, hybrid and multi-cloud services. As a result, cybersecurity has evolved from the concept of securing relatively remote networks to one of monitoring identities, workloads, applications, data flows, endpoints, and interactions on these interwoven networks. Security mechanisms need to be dynamic and flexible to adapt to the constantly evolving operational conditions and detect threats (Mell & Grance, 2011; ENISA, 2023).

The cyber security environment has also become more complicated. Cloud resources can be impacted by malware, ransomware, phishing, botnets, intrusion attempts, denial of service attacks, compromised accounts, insider threats, anomalous activity, and advanced persistent threats in various ways, and can be more and more sophisticated and adaptive. While these traditional security methods, which rely primarily on predefined rules, signatures, and known attack patterns are still significant, they can be limited in their effectiveness when dealing with novel, polymorphic, high-volume, distributed, and/or evolving threats. Static detection mechanisms can be good at detecting patterns that have already been encountered but have a poor ability to detect more subtle changes in behaviour or patterns that have not been seen before. The literature in the field of cybersecurity has thus appealed for more flexible solutions that can process cybersecurity information in large volumes and be able to detect complex patterns and signatures that do not exist in the current list (Khraisat et al., 2019; Buczak & Guven, 2016; ENISA, 2024).

Artificial Intelligence (AI) and Machine Learning (ML) have proven to be significant pillars of this shift towards intelligent cybersecurity. ML techniques can assist in threat detection by training models on security-related data and detecting anomalies that could signify suspicious behavior. Supervised learning, unsupervised learning, semi-supervised learning, deep learning, ensemble methods, and anomaly-detection methods are reviewed in existing works for the context of cybersecurity. It is particularly relevant to the world of cloud computing, as security events are created constantly throughout the distributed and heterogeneous infrastructure. However, the trend towards the use of ML doesn't mean that there is an automatic increase in the effectiveness of cybersecurity the more complex the algorithm becomes. The effectiveness of an AI-based detection approach will depend significantly on the types of data available, the security context, operational needs, and the ability to interpret and respond to alerts generated by the AI system (Apruzzese et al., 2023; Ferrag et al., 2020).

Data analytics is thus closely tied to threat detection using artificial intelligence. Cloud environments produce a variety of security information such as network traffic, authentication logs, access patterns, system events, application logs, behavioral signals, and other cloud telemetry. Combining and analyzing these sources may offer a more comprehensive picture of potentially suspicious activity than individual monitoring methods. However, the larger the data volume, the better the detection is not guaranteed. ML-based systems can also be unreliable and limited in their transferability due to incomplete or noisy information, class imbalance, inconsistent data sources, privacy issues, or evolving user behaviors. An interesting aspect of concept drift is that the relationships formed from the past security information could change as technology, users, infrastructures, and attack methods develop.

There are also important issues related to false positives, adversarial manipulation, explainability, computational requirements, privacy, and model generalizability mentioned in the literature. An algorithm could have been used to detect unusual activity but might not give security professionals a clear explanation of why an alert was triggered. Too many false positives can also add to analyst workload and decrease trust in automated systems. Likewise, the models can be tested by adverse conditions, and privacy concerns might limit access to critical security data. These problems illustrate that there is no algorithmic solution to effective cybersecurity, no model of choice. Alongside the concept of AI-driven security, there are emerging aspects of explainability, human oversight, organizational trust, and responsible data governance that are gaining significance (Machlev et al., 2022; Alsaigh et al., 2023).

Another challenge is how AI-powered detection fits into the wider scope of cloud-security architectures and Security Operations Centers (SOC). Finally, when the outputs of the detection can assist in the monitoring, investigation, incident response, access management, threat intelligence, and other security processes, ML-based detection becomes practically meaningful. This view is

different than the usual perception that cybersecurity ML is just a technical element that is assessed mainly by algorithmic performance. Rather, it should be viewed as a socio-technical capability consisting of algorithms, data, infrastructure, cybersecurity specialists, processes, and government.

Although significant work has been performed in the field of ML algorithms, intrusion detection, anomaly detection, datasets, and comparative modeling performance, there is an important gap in conceptualization. Most of the current literature focuses on a single technique or a specific technical evaluation, with relatively little attention paid to the comprehensive qualitative interrelationship between artificial intelligence, machine learning, data analytics, cloud architecture, adaptability, interpretability, privacy and human decision making in effective cloud threat detection. This is significant because the usefulness of AI for cybersecurity ultimately relies on the interplay of these aspects, rather than on the sophistication of the algorithms.

For this reason, this study uses a qualitative, interpretivist, exploratory, documentary and secondary-evidence approach to investigate the understanding and use of AI, ML and data analytics in cloud cybersecurity threat detection. Does not build or evaluate a fresh ML model, create an original dataset or perform quantitative statistical analysis. Rather, it is a critical synthesis of scholarly research, literature on cybersecurity, technical publications, standards, and authoritative institutional evidence.

How AI and ML are helping in the field of intelligent threat detection within cloud computing environments?How AI and ML are helping to make cloud environments intelligent threat detection systems? How will data quality, the diversity of security information, adaptability, explainability, privacy and trust influence the effectiveness of AI based detection? (3) How can AI-driven detection be incorporated into the wider Cloud-security and SOC environments in order to enable resilient cybersecurity?

The study is structured into five analytical themes: AI and machine learning for intelligent cloud-threat detection; data analytics and heterogeneous cybersecurity data; adaptive detection of evolving and sophisticated threats; explainability, reliability, privacy and trust; and integration of AI-driven detection into smart and resilient cloud-security architectures. The study delivers a more comprehensive picture of how AI can support cloud cybersecurity, while emphasizing that the success of the threat detection relies on not just powerful algorithms, but also on the quality of data, adaptability, interpretability of decisions, privacy-focused governance, human oversight, and the ability to integrate with broader security systems.

LITERATURE REVIEW

Evolution of Cybersecurity Threats in Cloud Computing

Cloud computing has revolutionized cyber security by moving relatively tightly controlled network environments into distributed structures with virtualization, remote access, cloud services, APIs, hybrid architectures and multi-cloud configurations. This growth makes the number of resources that are interconnected and require monitoring and protection rise. New configurations and legitimate services may be used as a basis for new threats, including ransomware, malware, credential compromise, botnets, insider misuse, denial-of-service (DOS) attacks, and advanced persistent threats (APT), which can make threat identification challenging (ENISA, 2023, 2024). While signature- and rule-based mechanisms are still useful for identifying known threats, they are limited in ability to detect attacks that are new, polymorphic, or act in a different way to the attack that they have seen before. Therefore, behavioral and anomaly detection methods have begun to receive more focus in the field of cybersecurity research because they can adapt to different types of threats (Khraisat et al., 2019; Buczak & Guven, 2016). The literature thus indicates a shift from static identification to adaptive intelligence, but new issues related to reliability, explainability, and complexity arise.

Machine Learning and AI for Cloud Threat Detection

The use of artificial intelligence and machine learning in cybersecurity has been growing in significance due to their ability to detect patterns and relationships that could otherwise be hard to define in a set of rules. If labeled examples of legitimate and malicious behavior can be found, supervised learning approaches would usually be useful, while unsupervised and semi-supervised learning approaches are more useful for attack labels that are missing or for new types of attacks that have not been encountered. Automated analysis is also advanced by deep learning and ensemble methods which process complex and high dimensional security information (Ferrag et al., 2020; Apruzzese et al., 2023).

But the literature does not lend itself to the notion that as the algorithms get more complex, they result in better cybersecurity. The effectiveness of ML relies on the training data, feature representation, the context of the environment, and the evolving attack behavior. Various results may also be obtained from research, depending on the data considered, the scenario posed, the processing done and the conditions used for the evaluation. Therefore, the performance of any algorithm in one environment does not necessarily carry over to another. This restriction highlights first of all the need to consider ML as not a technical solution, but a contextual cybersecurity capability.

Data Analytics, Security Telemetry, and Threat Intelligence

AI-powered threat detection is highly dependent on the quality and variety of security data. Cloud environments emit a lot of telemetry data as a result of network traffic, authentication events, access patterns, application logs, system logs, endpoint data, workload activity, and security-monitoring systems. Threat-intelligence feeds can also provide context to what is happening – when these events are detected, they can be correlated with data from other threat-intelligence sources, such as indicators of suspicious activity. Data analytics allows these disparate sources to be aggregated and analysed together to find patterns that are not evident in the individual data sources.

However, it is not always the case that more data equals better detection. Security data may have class imbalance, temporal changes, missing values, noisy and redundant features, and inconsistent formats. The choices of data-pre-processing and feature-selection can thus affect what ML systems are learning and which behaviors are identified. The significance of data sources and data quality in the usefulness of AI cybersecurity approaches has been highlighted in recent reviews by Ferrag et al. (2020) and by Apruzzese et al. (2023). This literature therefore suggests that analytical methods and the representativeness, integrity, and contextual relevance of the data are also shaping factors of cybersecurity intelligence.

Explainability, Reliability, Privacy and Trust

One of the challenges with AI tools in cybersecurity is the balance between predictive complexity and human interpretation. Advanced methods such as deep-learning can detect suspicious activities effectively but do not give much justification for their decisions. However, in an operational environment, security professionals must understand the reason for an alert before deciding just how important that alert is and what action should be taken. Explainable AI (XAI) is thus an important link between automated detection and human security decision-making (Machlev et al., 2022).

Other factors like false positives, false negatives, shift in data distribution and adversarial manipulation also affect reliability. Too many false alarms can drown out the analysts and not enough threats can have a very serious security impact. Another challenge is privacy, as there can be sensitive information about the user, the organization, or even behavior within the cloud security analytics. These concerns illustrate that such trust is not all about the technical sophistication. In order to achieve the meaningful adoption of operations, responsible data governance, transparency, robustness, accountability, and human oversight are required (Alsaigh et al., 2023). Trustworthy AI security is therefore increasingly viewed as a socio-technical, rather than just a computational, challenge.

Cloud-Security Architectures that are adaptive and intelligent

The real-world impact of AI-powered detection will rely on its ability to fit into the overall cybersecurity landscape. Real-time and near-real-time analytics can be used to assist in the continuous monitoring, anomaly detection, threat prioritization, and incident-response phases. In a Security Operations Center (SOC), AI can be used to help security analysts by analyzing vast amounts of security events and identifying potential highly unusual or malicious activities. A similar approach to the need for continuous identity, device, workload, application, and access behavior evaluations is needed for Zero Trust and Cloud Native architectures, which don't place any reliance on a defined perimeter.

The literature indicated that AI can boost adaptive security when combined with monitoring, threat intelligence, access control, incident response, and human intelligence. But automation shouldn't be seen as cybersecurity professionals becoming obsolete. Where there is a need for contextual judgment, accountability and investigation, human-AI collaboration is still important. Research on AI in cybersecurity, therefore, suggests that a resilient and holistic architecture that leverages AI capabilities along with existing cybersecurity processes is the future direction.

Literature synthesis and research gap

The literature across the five themes shows that there are interrelated technological, data, organizational and governance aspects to AI-enabled detection of threats in the cloud. There are many existing studies that offer a significant amount of knowledge about ML algorithms, anomaly detection, security datasets, deep learning, and automated detection. Most of the literature is however still technically oriented towards individual algorithms, datasets or performance evaluations. Much less has been discussed about the interaction between AI/ML, diverse security data, adaptability, explainability, privacy, human oversight and cloud-security architecture and how they all contribute to trustworthy and resilient threat detection.

This gap calls for the present qualitative, interpretivist and exploratory kind of documentary study. Instead of testing another ML model, this study combines the existing scholarly and authoritative information to decipher the relationships between these dimensions. Its value is in knowing how to use AI for cybersecurity as much as it is in knowing how to detect the problem with algorithms. It is using AI as a capability that needs to be integrated into the security strategy using reliable data, adaptive intelligence, interpretable decisions, privacy aware governance and effective integration into a wider cloud security framework.

RESEARCH METHODOLOGY

Research Philosophy

The employ of the interpretivist research philosophy is suitable for this study because it is used to explore the constructions of knowledge, meaning, challenges and possibilities associated with the use of AI in cybersecurity threat detection, as found in the current scholarly and professional literature. Interpretivism acknowledges that in many cases technological and organisational phenomena cannot be fully grasped without taking into account their social, contextual and institutional context. The definition and value of AI-driven detection is influenced by the organization's practices, human decision-making, governance, privacy, trust, and evolving threat landscape as much as by the capabilities of the computers. The study therefore does not aim to draw general causal inferences nor to provide an objective assessment of the performance of a specific algorithm. Rather, it engages with previous knowledge to develop an understanding of the ways in which scholars and authoritative institutions have conceptualized AI, machine learning (ML), data analytics, and cybersecurity in complex cloud contexts (Creswell & Poth, 2018).

Research Design

This study is qualitative research with exploratory and documentary research approach using secondary data only. Documentary research is appropriate when the intention is to critically analyze and discuss what has already been known and to uncover patterns, relationships, debates, or conceptual progressions in a collection of documents. The exploratory approach is especially fitting, as AI-driven cybersecurity is a constantly evolving landscape, with new architectures on the cloud, novel attack surfaces, new analysis methods, and ongoing discussions about the trustworthiness of automation. Instead of building and testing a new ML model, the study combines available evidence to build an integrated cloud-threat detection model that addresses technological, operational, organizational, and ethical aspects of cloud threat detection.

Evidence Base and Selection

The evidence base comprises authentic peer-reviewed journal articles, systematic reviews and critical review studies, relevant scholarly books, cybersecurity standards, technical reports, publications about cloud security, and authoritative institutional sources. Recent articles on the history of AI, cloud computing, and modern cybersecurity practices are given preference and covered with articles published between 2020 and 2026. Previous seminal sources are included if they provide needed methodological and/or conceptual background.

The topical relevance, scholarly authenticity, methodological transparency, authority, and contribution to the understanding of AI/ML-enabled cybersecurity threat detection of sources were determined. Literature reviewed included specific focus on cloud-security threats, machine learning, anomaly detection, cybersecurity data analytics, threat intelligence, explainable AI, privacy, adaptive security and security operations. The selection was an interpretive process and not numerical sampling. No subjects, data sets, or sampling procedures used quantitative sampling were involved.

Documentary analysis and thematic analysis

The collected literature was analyzed by qualitative documentary analysis and thematic analysis. Documentary analysis helps develop a critical approach to documents as a means of knowledge and in the consideration of context, purpose, assumption and limitation. Thematic analysis was followed by the approach of Braun and Clarke (2006, 2021) that offered the flexibility to identify, review, organise and interpret common themes in qualitative data.

The analysis process included multiple revisiting of the selected evidence, uncovering of concepts and themes that emerged, comparing similar findings, and creating more encompassing interpretations. This analysis did not focus on a statistical aggregation of results, but rather on the convergence, divergence, or qualification of the results from various sources. Five analytical themes were used to guide the synthesis:

1. AI & ML for intelligent cloud-threat detection;

2.data analytics and heterogeneous security data;

3. Adaptive detection of changing threats;

4 Explainability, reliability, privacy and trust;

5.intelligent and resilient cloud-security integration.

These themes were not considered separately. But their relationships were studied to analyse the influence of data characteristics on AI-driven detection, the issues of evolving threats and model reliability, the role of explainability in enhancing human trust and the integration of AI capabilities into broader cloud-security frameworks.

Analytical Interpretation

The research focuses is critical comparison and conceptual synthesis, not on quantitative measurement. Research context, technological assumptions, methodological orientation and the cybersecurity problem addressed were explored through the lens of the evidence of the various studies. Agreements across sources were identified, contradictions and limitations were preserved as analytically significant, but not eliminated. This method acknowledges that the nature of cloud architecture, data characteristics, type of threats, operational needs, and organizational context can cause different conclusions about the use of AI in cybersecurity. Thus, the analysis separates out claims from empirical studies from those of a more general conceptual or theoretical nature.

Quality and Trustworthiness

Credibility, transparency, consistency, source triangulation, and reflexive interpretation, were used to deal with trustworthiness. Authoritative, peer-reviewed evidence was emphasised and claims across a range of source types compared to enhance credibility. The scholarly research, standards, technical publications and institutional cybersecurity evidence were taken into account for source triangulation. The research orientation, evidence criteria and thematic structure were clearly defined to ensure analytical transparency. Systematic comparison of the ideas presented repeatedly in the literature was used to provide consistency. Qualitative interpretation also was important, as it always includes the judgment of the researcher, and interpretations were made based on documented evidence and not based on unsupported assumptions (Creswell & Poth, 2018).

Ethical Issues and Restrictions

The study is based on secondary literature that are public data or data that can be accessed legally without the involvement of human participants, interviews, questionnaires, personal data collection and experimental interventions. Ethical practice, then, is about the accurate representation of sources, appropriate citation, avoiding plagiarism, and responsible interpretation of published evidence. As the study is not directly related to data collection from human subjects, no ethics approval or consent of participants were necessary.

There are some caveats to keep in mind, however. Documentary research relies on the quality, quantity and availability of existing evidence available and can be affected by publication bias and methodological differences. Comparisons can be tricky because of variations in terms, cloud environments and the definitions of threats and research goals. In addition, cyber security technologies and attack methods change quickly and some findings may no longer be applicable as technologies change. These constraints further emphasize the importance of interpreting existing literature with criticality and sensitivity to context, instead of assuming that all of that literature is equivalent, or that it will remain definitive.

FINDINGS and DISCUSSION

Through the literature review, the researcher finds that the current literature is focused on a problem of selecting the most advanced machine learning algorithm in the context of implementing AI solutions for detecting cyber threats in cloud computing systems. Rather, the literature reveals that complexity in cloud infrastructures is leading to an ever-expanding data landscape of security data, characterized by high volume, variety in sources, quantity and types, and that machine learning and data analytics can provide tools and methods to extrapolate patterns that might not be apparent using traditional techniques. In the meantime, data quality and contextualisation, explainability, privacy, governance, and human-centric security operations are key elements to relying on AI-driven detection. In addition, recent developments in the field of cybersecurity demonstrate that cloud environments continue to be vulnerable to new threats, such as ransomware, threats to availability, data-related threats, and more advanced evasion methods (ENISA, 2024, 2025). (ENISA)

The outcome is thus organized around five themes that are interrelated: (1) AI and machine learning as foundations for intelligent cloud threat detection; (2) data analysis and heterogeneous cloud-security data; (3) adaptive detection of evolving and sophisticated threats; (4) explainability, reliability, privacy and trust; and (5) intelligent and resilient cloud-security integration. These themes all point to the fact that the role of AI in cloud security is not limited to the complexity of the algorithms, but to the combination of the algorithms, security data, infrastructure and processes, as well as human expertise.

Theme 1: AI and Machine Learning as Foundations of Intelligent Cloud-Threat Detection

Thematic Finding

The first big discovery is that AI and machine learning are increasingly becoming key enablers in shifting cybersecurity from primarily static and rules-based detection to more adaptive and behavioral ones. The literature suggests that ML-based systems can help in detecting unusual patterns, classify suspicious activity, detect relationships in security data and assist in detecting a threat that may not be part of a known signature. In summary, reviews of AI based intrusion detection (Al-Yaseen et al., 2023; Hamed et al., 2023) cite machine learning, deep learning and ensemble methods as important advances to enhance the development of intelligent cybersecurity detection.

The discovery is significant in cloud environments in which resources are distributed, workloads are dynamic, remote access is in play, virtualization is commonplace, resources are interdependent and user and system behavior is in constant flux. The traditional security models continue to be important but a reliance on a unique set of rules or attack patterns might be restrictive if attack payloads are less obvious or new, or originating from multiple sources. A recent survey of cloud attack prevention also documents the shortcomings of traditional intrusion-prevention methods when it comes to unknown attacks and stresses the increased importance of machine-learning methods (Ledesma et al., 2023). (ScienceDirect)

The study involved a review of the existing literature

In the literature, there exist few classes of Machine learning approaches. If enough information is available in terms of labelled security data that can be used to represent the security patterns, and a list of known threat categories is provided, relationships between security patterns and known threat categories can be learned, and supervised learning is helpful. Unsupervised learning is more relevant to anomaly oriented detection as this type does not require samples to be labeled beforehand. A small percentage of security events are “labeled,” and semi-supervised methods lie somewhere between supervised and unsupervised and can be useful. Deep-learning techniques can handle complex representations and massive security info, and ensemble approaches create a collection of various learning mechanisms to mitigate weaknesses of single learning mechanisms (Al-Yaseen et al., 2023; Hamed et al., 2023).

There is thus no simple hierarchy in the literature with one learning paradigm being universally superior. Rather, the suitability of the model is determined by security problem and operational environment. If there are data that have been labeled for the supervised approach, it may be more attractive, or if there are new or inadequate labeled behaviours, the anomaly-oriented or semi-supervised approach may be more suitable. Deep models can provide representation benefits, but also add interpretive and computational complexity. The reason for this is because it has been a focus of the previous ML cybersecurity literature to focus on model performance and benchmark datasets instead of the context needed for a sustainable deployment.

This is seen in an extensive analysis of the literature that showed that there is a significant amount of literature focused on ML, deep learning and ensemble learning, and there are still research questions regarding attack classification and practical detection requirements (Hamed et al., 2023). Similarly, a broader view of the intelligent cloud defenses highlights an increasing focus on ML and deep learning as alternatives or supplements to the traditional security mechanisms, as well as some ongoing challenges concerning the cloud attacks, datasets, and deployment (Alazab et al., 2022). (ScienceDirect)

Interpret and compare

These results have more of an interpretationist meaning than just technical algorithms. The whole literature shows a trend to move from the question of detecting known attacks to the question of detecting meaningful deviations from normal behavior in an evolving environment. That's a significant change in thinking about cyber security.

But there is a point to be noted, the flexibility of machine learning – as it seems – doesn't mean it's without constraints. The information that a ML system receives is what it learns. If this data is incomplete and biased or it is out-of-date, not representative, or poorly labeled, sophisticated algorithms can exacerbate the problem of the underlying security data. The intelligence an AI-powered detection system has, in other words, depends on the quality and context of the information that is used in the creation of that intelligence.

There is also a big gap between what can be shown on research platforms and what works in operational cloud platforms. In the real world, there can be numerous services, identities, applications, devices and geographically distributed resources at any one time.There can be a multitude of services, identities, applications, devices and geographically distributed resources available at any one time in the real world, and benchmark datasets can help to simplify the complex nature of cloud infrastructures. So a model that is successful in one research context does not necessarily translate to other cloud providers, organizations, threat context, or architectural configuration.

Significance and Implications

That is the key theoretical view point that the use of AI for threat detection is not a replacement for traditional security products, and it is context specific. It is true that traditional controls are still relevant as machine learning is not a solution to solving the need for authentication, authorization, encryption, access management, network controls, vulnerability management, and investigation by humans.

Therefore, organizations need to consider using the ML-based detection as a component of layered cybersecurity, in reality. Which model to employ will rely on security objectives, data available, computer resources, type of cloud architecture, experience of the organization, and the consequences or costs of false or lost alerts.

The connection between the research questions is therefore obvious: AI and ML can help the cloud threat detection principally by boosting its ability to understand intricate and shifting security patterns, as proposed in the literature. They are only effective if the algorithmic capabilities do meet the data conditions and operational requirements, however.

Theme 2: Data Analytics and Heterogeneous Cloud Security Data

Thematic Finding

The second theme illustrates the data information backbone of AI based cyber security detection. Machine-learning algorithms depend on the data environment that they are applied to. Cloud systems are constantly generating different types of information with relevance to security including authentication information, access logs, network activity, application events, system telemetry, endpoint data, identity behaviour information and threat-intelligence information. The lesson learnt is that volume of data alone is not sufficient to make successful AI-based detection, it needs to be able to transform the many data types into relevant and contextually understandable security signals.

This is further complicated by cloud computing with information spread out across services, applications, identities, virtual resources and administrative domains. The relationships between events that may appear insignificant when they are considered individually but are meaningful when considered together may be important for threat detection.

Use of existing literature to inform research

Security datasets and data characteristics have been mentioned as crucial aspects in the evolution of ML-based security solutions in various studies on intelligent cloud security (Alazab et al., 2022). Some of the other findings of AI-based Intrusion Detection, as reported by the reviewers, also show a variation in methodology and the type of security data used depending on the type of intrusion detection (Hamed et al., 2023). In addition to the issue of availability of security information, which strongly relates to the issue of unknown attacks (Ledesma et al., 2023), the literature on cloud attack prevention also brings this topic to the fore. (ScienceDirect)

Based on this evidence, some challenges arise relating to data. First of all, there's data volume. Manual review can be difficult in cloud environments due to the potential for a large number of events. Second, data velocity which is information that can occur suddenly and rapidly, and can only be acted upon in a timely manner if it is a security metadata event. Third, data variety: Data like logs, network data, identity events, application telemetry, endpoint data, threat intelligence, and more can be of different types

and carry different meanings. Four is data quality, data that is missing, data that is noisy, data that is duplicated, data that is in different formats, and possibly some strange observations.

Therefore, the concept of feature selection and preprocessing is of significance. The objective is not to collect as much data as possible, but to obtain information that can be implemented in a meaningful way to help in security interpretation. Too much information or too much irrelevant information can overload the computer processing and difficulty to analyze the information, too much reduction can lead to some important information which needs to be picked up the subtle threat washed out.

The student will interpret and compare texts.

The literature indicates that the most important paradox: more security data available doesn't necessarily mean more cyber security intelligence. The more data you have, the more analysis options you have, but you also have the possibility of more noise, more complexity, more storage space, more privacy issues and more misdirection.

This means that the technology assumption that cloud security problems can be solved with a large stack of telemetry and more advanced algorithms is wrong. The more convincing side is that data governance and analytical design are to be taken on par with algorithm selection. For artificial intelligence security, the process involves several transformations, in which data needs to be collected, contextualized, normalized (if applicable), interpreted, analyzed, and then translated to security information.

Data imbalance is yet another critical issue. In the normal cybersecurity universe, there are lots of more mundane events than detectable malicious events. Therefore, there could be many mundane activities that are not of interest to the detection system, but a few of the specific types of threats. This creates conceptual problems with the learning systems because most of the events in the data are not the most security relevant ones.

Constant changing of cloud environments adds to the problem. A normal behaviour in one organisation or at one time may not be considered as normal in another organisation or time. With remote working, new applications, new services, application migration from one cloud to another, changes in access policies, etc., the distribution of security events can change.

Significance and Implications

The theory behind it is that data analytics has to be regarded as a mediation layer between the complexity of the cloud and the machine intelligence. This implies that the two are correlated as:

The data analytics, machine intelligence and threat interpretation stages are all located within cloud environments and heterogeneous security data.

This also reminds us of the need to not consider AI a panacea for truth and why security organizations need to be careful not to equate an AI system with truth. Their output is in response to the quality, structure, coverage and context of their data.

In reality, organizations must take a holistic view of data management to ensure that cloud logs, identity data, network telemetry, endpoint data and threat intelligence can be connected together, while maintaining privacy and not introducing undue centralization of sensitive information. Thus, data governance should not be a back-office problem, but rather a part of the cybersecurity architecture.

The discovery is directly related to the larger research problem of the central role of the availability of data and the meaning of the data in threat detection using AI as the core. The objective is not to collect tons of security information, but to provide analytical environments to help detect and interpret meaningful patterns in security data in a responsible manner.

Theme 3 Emerging and sophisticated threats in an adaptive

Thematic Finding

The third theme has to do with the requirement for flexibility. The cybersecurity landscape is dynamic, with cloud infrastructure and threats constantly evolving, as evidenced in the literature. Modern day threats include ransomware, availability attacks, threats to data and ways to avoid known defenses. The recent threat assessments conducted by ENISA highlight the ongoing significance of big threats, as well as growing sophistication in evasion techniques such as the exploitation of trusted services and legitimate tools to hide malicious activity (ENISA, 2024, 2025). (ENISA)

A general issue that arises for detection systems is that the model trained/configured from historic activities will start to lose the representation of the current activities over time. AI and ML are then useful not just for the ability to identify known patterns, but for some methods that help facilitate identifying deviations and new and changing relationships in security data.

Make inferences from previous reading(s).

Well, known and unknown attacks continue to be a problem as recognized in existing cloud-security reviews. For example, Ledesma et al. (2023) point to the limitations of traditional detection techniques to identify unknown attacks, and discuss how ML can play a part in a broader response. Likewise, in (ScienceDirect), reviews encompass intelligent cloud defense and emphasize the necessity to research ML/DL based solutions for addressing the emerging cloud threats in the future. (ScienceDirect)

This is particularly an issue of concept drift! In the real world it is the changes in such patterns that a model should learn from. A cloud environment can change due to new applications, changing user behavior, migration, architectural redesign or organizational changes. Meanwhile, the competition can adjust accordingly to beat the detection measures set up.

The literature that comes from this as a result suggests adaptive learning, anomaly detection, behavioural analytics, continuous monitoring and more that can be adapted to change. However, risks are associated with adaptation. A highly adaptive system may learn unwanted patterns and/or deem a valid change a threat. Lack of adaptation can lead to out of date detection mechanisms.

Interpretation & Critical Comparison

The outcome indicates their stability as well as adaptability, indicating a dialectic of stability and adaptability. It is important that security systems have adequate rules and controls that are stable enough to ensure a predictable protection, but remain responsive to evolving environments. AI/ML systems can help to navigate through the tension, but they don't extirpate it.

This can be especially crucial in the context of adversarial machine learning. Adversarial methods can be used to manipulate AI systems, and there is no way to prevent the manipulation of AI systems entirely (NIST, 2024). Likewise, NIST and ENISA identify threats to ML systems, and charge that security controls need to be considered from the inception of an ML-based system to its disposal (NIST, ENISA 2021). (ENISA)

That is, what makes machine learning attractive for the cybersecurity community can also be a new source of security. But securing cloud infrastructure is not the only thing that organisations need to do; they might also have to consider securing the data, models, pipelines and decision processes that power AI in security.

This results in a significant change of concepts. AI isn't a panacea for threat detection, and shouldn't take the place of any other action. Rather, the use of AI in cybersecurity is seen as an ongoing monitoring, assessment, adaptation, validation, and human review cycle.

Significance and Implications

The lesson learned: Model lifecycle management should be a component of the cybersecurity governance framework. The architecture, data distribution, threat patterns and behavior of the cloud can evolve, requiring changes to the detection systems as well.

However, the ramifications of this theory are even more significant: effective threat detection is not only a classification problem, it's also a temporal and contextual interpretation problem. Security systems need to determine if the change is an attack, the normal evolution or an indeterminate state that needs to be investigated by people.

The discovery further bolsters the conceptual link:

Cloud Threat Complexity → Changing Security Data → Adaptive Analytics and ML → Continuous Detection → Human Validation.

This perspective is different from the technologically deterministic one that more powerful AI results in more secure systems, but rather recognizes that as AI develops, the security measures need to adapt.This perspective isn't that more complex aI models will necessarily provide better security, but rather that as aI models get more sophisticated, so too must the security measures. Instead, it's about knowing how to be contextually relevant without losing reliability or control that matters in the value of AI in the literature.

Theme 4 reliability, privacy and trust.Explainability, Reliability, Privacy, and Trust are themes of this.

Thematic Finding

The fourth theme shows that the utility of AI to cybersecurity can't be fully evaluated by its ability to identify suspicious activity. Trustworthiness, explainability, privacy, robustness and accountability are additional attributes that are all equally important. When a security analyst receives an AI-generated alert they may want to know the reason for the behaviour to decide what action to take.

This is important even more so because there can be a lot of alerts that can be generated in some of the cloud-security environments. Explainable AI (XAI) research highlights the potential of interpretability tools for security practitioners to deal with the AI-generated output and reduce problems like alert overload and false positive alerts (Kaur et al., 2023). (Springer)

Quotes from current books (EFL)

The literature underlines the increased interest in Explanable AI (XAI) for cybersecurity, particularly in intrusion detection, malware classification, and various other security applications. However, the same literature admits that transparency without oversimplification is difficult to obtain in the decision making of complex models, and that the security of the XAI is also not guaranteed.On the other hand, the challenges of making complex models transparent while keeping the decision-making process intact and making sure that XAI itself was secure are recognized in the same literature (Kaur et al., 2023). (Springer)

The NIST AI Risk Management Framework also highlights important concepts from the NIST definition of trustworthy AI (NIST, 2023), such as validity and reliability, safety, security and resilience, accountability and transparency, explainability and interpretability, privacy enhancement, and fairness. (NIST)

These are key rules that directly apply to cyber security. A model that generates a lot of false triggers can lead to analyst fatigue. If the model is not able to identify meaningful threats, it can result in false confidence. Without a model that provides some comprehensible explanations of the model decisions, investigations and accountability can be difficult. In the meantime, security analytics might need to process user, device, behavior and organizational activity data, which could pose privacy and governance issues.

Discuss the meaning and compare the various interpretations of the text

Hence, a trade-off between complexity and interpretability can be found in literature. Very sophisticated models can detect complex relationships, but it may be difficult to gain an understanding of the logic of these models from the security practitioners' perspective. Earlier models are simpler and potentially more easily understood, but not necessarily as complex as earlier.

This does not imply that always an explanation is the selection of a simpler model. Rather, it implies that organisations need to figure out how to strike the appropriate equilibrium between the sophistication of predictions, their interpretability, their operational characteristics, and their risk.

It is necessary to take a contextual understanding of reliability. A detection system functions in the context of a larger system. The interpretation of the alert must be based on the organizational policies, criticality of the assets, role of the user and current events, as well as the overall security environment. A technical indicator can thus have varying interpretations in different cases.

The privacy is an added aspect. Cloud security has a wide variety of monitoring and can create conflicts with data minimisation and responsibilities for privacy. Monitoring is however a challenge not only in terms of the monitoring itself, but also in terms of making a legitimate and proportionate use of security information.

Threats of being a part of a hostile group create additional challenges to trust. The adversarial machine learning project by NIST also demonstrates that AI systems can be manipulated, too (NIST, 2024). This means cybersecurity companies must not only safeguard the cloud system they are monitoring but also the AI mechanisms themselves that are monitoring these systems.

Significance and Implications

At the heart of the theoretical result is that trust is not an “after-thought” that is merely “plugged” in. It's a component of sound AI-powered cybersecurity.

In practice, AI systems should be assessed across various aspects, including detection, robustness, interpretability, privacy, accountability, usability, and manipulation resistance. AI-based recommendations should not be used to negate the skill of security experts asking questions, probing and interpreting the generated recommendations.

Their need for human oversight, however, is no indication of a failure of the AI. Rather, it is a crucial aspect of good security architecture. AI can handle large volumes of data and extract insights, human professionals can offer context, organise knowledge, think ethically and take responsibility for the impactful decisions.

The ease of linking to the research questions is clear; the effectiveness of how AI tools can contribute to cybersecurity intelligence relies on the trustworthiness, learnability, comanagement, and actionability of the outputs that they produce.

Theme 5: The smart, resilient adoption of Cloud Security.

Thematic Finding

The fifth theme builds on the previous themes by demonstrating the value of threat detection capabilities enabled by AI in the context of a comprehensive cloud-security ecosystem. No literature indicates that machine learning should be considered as a separate level of technology to be implemented. Rather, the key is the interdependencies of AI-powered detection, identity management, access control, security monitoring, incident response, threat intelligence, zero trust principles, organizational governance, and human expertise.

This discovery is particularly important since the traditional perimeter assumptions of security are being undermined by the use of cloud computing. The NIST Zero Trust Architecture recognizes a shift in security strategy, which moves beyond a network-centric defense to focus on assets, users and resources (Rose et al., 2020). (NIST)

Data obtained from books and other published sources.Information taken from the current literature.

The NIST cloud-native zero-trust guidance also highlights the need for identity-centric security in multi-cloud and hybrid scenarios, such as application and service identities and granular access policies (Chandramouli & Butcher, 2023). The principles are much the same as those of AI based detection; contextual information about users, services, devices and interactions with resources may be provided by behavioral analytics and ML.

In the literature, ML and deep learning are also being increasingly integrated into a larger cloud-defense solution, instead of being used as standalone classifiers (Alazab et al., 2022). The assessment also reflects the need for an integrated security strategy in the face of the capabilities of threat actors to leverage on legitimate services, distributed environments and defence vulnerabilities (ENISA, 2024, 2025). (ENISA)

A place where such integration is critical is in the Security Operations Centers. Although AI can identify and prioritize security data, it's essential that analysts respond to vague security alerts, ask questions about the security situation of the organization, and decide on responses. Likewise, threat intelligence can be used to give context in explaining an anomaly, as opposed to using the anomaly intelligence as the only foundation for detection.

The results reveal that the most significant change is from using AI as a detection system to integrating AI into an intelligent security system.

This distinction is important as detection is only one aspect of cybersecurity. Suspicions of activity does not equate to prevention of damage, containment of an incident, restoration of service or enhancement of organizational resiliency. The result of a detection process must therefore go to the appropriate investigation, authorisation, response, recovery and learning processes.

To support this integration, zero-trust architecture is a useful paradigm to consider, as it is not a perimeter-only security approach, but a continuous monitoring of identities, resources, and access. Additionally, NIST's guidance for multi-cloud environments recognizes the necessity to provide security controls that support distributed service architectures, such as for cloud-based applications (Chandramouli & Butcher, 2023). (NIST Computer Security Resource Center)

However, there are challenges that come with integration. Linking AI systems with the security operations may lead to a dependency on the automated recommendations. Inconsistent systems can cause alert fatigue and over-automated systems may respond to partial data, resulting in inaccurate responses. So, the degree of certainty and potential consequences of decision should also be considered for automation purposes.

The literature therefore corroborates the model of human-AI collaboration and not human replacement. AI has limitations in providing context and judgment, as well as ethical review and accountability, but it is much better equipped to process large sets of patterns and conduct constant analysis.

Significance and Implications

This theme provides the theoretical contribution of the integration of the previous four findings in a bigger socio-technical model.

Cloud Complexity to Security Data, AI/ML Analytics, Adaptive Detection, Explainable and Trustworthy Interpretation, Integrated Security Response, Organizational Resilience.

This model is clearly not a mere selection of a model, but a demonstration of the power of AI to help with cybersecurity. The final security result is dependent on the relationships among technological, informational, organizational and human elements.

For a practitioner, it is also critical to think about investments in AI-powered detection as well as data governance, cloud architecture, identity management, security operations, workforce skills, model governance, and incident-response capabilities. Thus, the most effective security architecture will not always be the most sophisticated AI model, but rather one that combines the right amount of AI with the needs of the organization, while still being able to withstand threats and disturbances while remaining secure.

Integrated Thematic Synthesis

In all five themes the evidence shows that the threat detection in cyber security in cloud computing is a socio-technical and architectural challenge as well as a computation problem. In Theme 1 it was demonstrated how the machine learning approach could be used to complement the detection of complex and abnormal security activity. In Theme 2, it was highlighted as a crucial ability to be supported by good quality cloud security data, characterized by quality, variety, contextualization and governance. Theme 3 demonstrated that the adaptive detection strategies and the dynamic and continuous evaluation of them need to be revised with changing threats and changing cloud environments. In Theme 4, it has been agreed explainability, reliability, privacy, robustness and trust are the criteria for the use of the security information produced by AI in a responsible way. Finally, Theme 5 revealed that detection doesn't have an operational meaning unless combined with cloud-security architectures, identity controls, zero-trust approaches, security operations, incident response, threat intelligence and finally, with human expertise.

The results, however, contradict a purely technologicalist understanding of the improvement of cyber security as a direct effect of the use of machine learning. The evidence does speak for a more conditional interpretation, however. The power of AI can enhance the analytical capabilities of cybersecurity systems, but it is limited by the quality of the data, the data's relevance in context, the robustness of the model, its governance, interpretability and integration into the company.

This is consistent with the overall cybersecurity environment ENISA is monitoring, as threats constantly change and responses must evolve to new techniques and infrastructure (ENISA, 2024, 2025). It also highlights NIST's ideas of trustworthy AI and the zero-trust paradigm, which includes two or more systems of governance, identity, risk management, and organizational responsibility management (NIST, 2023; Rose et al., 2020). (NIST)

Thus, the main result of this qualitative synthesis is that the most useful role of using AI for cybersecurity is to be an intelligent complement to a larger cybersecurity ecosystem, not a substitute for existing security controls or cybersecurity experts. Patterns can be captured by machine learning at a scale that could be beyond human ability, and data analysis can bridge the gaps of information scattered across the security environment. Adaptivity can be applied to adjust to changes in conditions, and explainability can be applied to help humans understand. But governance processes that can address privacy, accountability, adversarial manipulation and organizational risk must be enveloped by such capabilities.

The results also show that future development should be beyond isolated instances of algorithmic capabilities to models for research and implementation that explore the aspects of generalizability, lifecycle security, data governance, explainability, adaptive learning, cloud-native integration and human-AI collaboration. It's particularly important in a world where the threat level keeps changing along with the protection technologies.

The future of cloud cyber security, then, will not be defined by any one, big algorithm. It is more realistically characterised as a new breed of adaptive intelligent systems, which are explainable, data-driven, aware of privacy issues, and which are integrated within the organisational context, and support cybersecurity decision-making continuously while keeping a meaningful human check.

Table 1

Thematic Synthesis of AI Driven Cybersecurity Threat Detection in Cloud Computing

Theme	Central Finding	Key Challenges	Major Implications
1. AI and ML for intelligent detection	ML and AI expand the capacity to identify anomalies, suspicious behavior, and complex threat patterns	Data dependence, generalizability, model complexity, contextual limitations	Model selection should be context-sensitive rather than based on universal algorithmic superiority
2.Data analytics and heterogeneous security data	Security intelligence depends on integrating diverse cloud telemetry and security information	Volume, velocity, variety, noise, missing data, imbalance, interoperability	Data governance and analytical quality are foundational to AI-driven detection
3.Adaptive detection of evolving threats	AI can support detection in changing and uncertain threat environments	Concept drift, adversarial manipulation, changing architectures, continuous adaptation	Detection systems require lifecycle management and ongoing evaluation
4.Explainability, reliability, privacy, and trust	Responsible AI requires interpretable, robust, privacy-conscious, and accountable detection	False alerts, opacity, privacy risks, adversarial attacks, bias	Human oversight and trustworthy AI principles should be integrated into security design
5.Intelligent and resilient security	AI becomes	Automation risks,	AI should

integration	most valuable when embedded within cloud-security architecture and operations	integration complexity, organizational readiness	augment rather than replace cybersecurity professionals and established controls

1. AI and ML for intelligent detection ML and AI expand the capacity to identify anomalies, suspicious behavior, and complex threat patterns Data dependence, generalizability, model complexity, contextual limitations Model selection should be context-sensitive rather than based on universal algorithmic superiority

2. Data analytics and heterogeneous security data Security intelligence depends on integrating diverse cloud telemetry and security information Volume, velocity, variety, noise, missing data, imbalance, interoperability Data governance and analytical quality are foundational to AI-driven detection

3. Adaptive detection of evolving threats AI can support detection in changing and uncertain threat environments Concept drift, adversarial manipulation, changing architectures, continuous adaptation Detection systems require lifecycle management and ongoing evaluation

4. Explainability, reliability, privacy, and trust Responsible AI requires interpretable, robust, privacy-conscious, and accountable detection False alerts, opacity, privacy risks, adversarial attacks, bias Human oversight and trustworthy AI principles should be integrated into security design

5. Intelligent and resilient security integration AI becomes most valuable when embedded within cloud-security architecture and operations Automation risks, integration complexity, organizational readiness AI should augment rather than replace cybersecurity professionals and established controls

Concluding Discussion

The thematic highlights that AI-based Cyber Security threat detection is a major paradigm shift in the manner in which complex and volatile Cyber Security information can be interpreted in cloud-security environments. Yet, there is no justification in the literature for technological determinism. The application of machine learning does not bring any solution to the problems caused by cloud computing alone, and it is not a replacement for the reliance on traditional security controls, governance or expert judgment.

Rather, the evidence suggests a holistic approach: Cloud complexity creates varying security signals, data analytics processes the signals into meaningful information, AI and ML aid detection and adaptation, explainability and governance build trust, and integrated security architectures translate detection to organizational resiliency. This relationship offers the best theoretical implications of the current qualitative synthesis.

With this implication, it is also crucial for organisations transitioning to increasingly distributed and cloud-native infrastructures. Security strategies need to shift from perimeter protection to continuous, contextual, identity-aware, data-driven and adaptive security. Meanwhile, smart cybersecurity needs to go hand-in-hand with privacy, accountability, robustness, transparency, and human control measures.

So, the role of AI in cloud cybersecurity should not be considered as a battle between humans and machines. It should be interpreted as the evolution of safe and responsible ecosystems between humans and AI where AI provides enhanced analytical capabilities and humans remain in charge of interpretation, governance and consequential decision-making.

CONCLUSION

The growing complexity, spread, and dynamism of cloud computing environments have introduced scenarios with cybersecurity problems that can't be solved with only static detection mechanisms. The present study is a qualitative, interpretivist, and exploratory documentary study that explores how artificial intelligence (AI), machine learning (ML), and data analytics can help with more intelligent cloud-threat detection. The thematic synthesis highlights the necessity of AI-based cybersecurity solutions not being merely an application of a high-tech algorithm, but of complex interplay between data, adaptability, interpretability, human expertise, governance and cloud security architecture.

The initial theme confirmed the potential of AI and ML technologies to enhance threat detection, especially regarding identifying abnormal patterns, unusual activities, and intricate connections within cloud systems. But AI is not meant to replace the need for traditional security measures or security personnel. Rather, intelligent detection should be used in conjunction with existing security controls like access control, monitoring, threat intelligence, incident response, and security governance. The second theme was the importance of data analytics in the Central theme. Cloud infrastructures produce a variety of information in the form of logs, network traffic, authentication events, access patterns, workloads, and more security telemetry. AI's value therefore

hinges crucially on the availability of the data that it exploits, which must be relevant, reliable, representative, and responsibly managed.

The third theme showed the importance of being able to adapt, as the cloud infrastructures and cyber threats are always evolving. Threat behaviour, technologies, or operational environments may shift and pose a risk to models and detection mechanisms that rely strongly on past patterns. Persistent monitoring, adaptation to the context and human intervention are thus required to ensure meaningful detection capabilities. The fourth theme also highlighted that technical abilities do not create trust. Explainability, transparency, reliability, privacy, robustness, and human oversight are all critical as these AI alerts and decisions must be understood and critically assessed by security professionals. This is consistent with the general discussion that there is a role for explainable AI in responsible security operations (Machlev et al., 2022).

The fifth theme was the need to complement AI-driven detection with wider and more robust cloud-security architectures for practical value. Operational context can be provided by Security Operations Centers, cloud-native monitoring, threat intelligence, incident-response processes and human expertise to help turn automated detection into actionable cybersecurity. AI should thus serve as a tool to supplement security skills, not supplant them.

Theoretically, the study is expected to add by proposing the problem of cloud-threat detection as a socio-technical and architectural problem instead of an algorithm-selection problem. In the real world, organizations can assess AI security solutions based on the characteristics of data quality, context appropriateness, explainability, privacy, adaptability, governance, and security infrastructure compatibility.

Some caveats are in order. The study is reliant on pre-existing documentary evidence which introduces the risk of publication bias and source quality, potentially context specific differences, inconsistent cybersecurity terminology and the ever evolving AI and cloud technologies. The following areas should be explored in future research: context-sensitive evaluation, explainable and privacy-preserving AI, adaptive threat detection, human-AI collaboration, cloud-native security integration, and responsible AI governance.

But through all of this, the responsible application of adaptive intelligence, quality data, explainable decision-making, privacy, human skills and resilient security architectures will all play a crucial role in delivering trustworthy cloud cybersecurity that cannot be achieved by ever-completer AI solutions. AI-powered cybersecurity solutions are the key to the future of security, but only if they are intelligent and transparent, context-aware and accountable, and are able to adapt to the ever-changing nature of threats.

REFERENCES

Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications, 195, 346–361. https://doi.org/10.1016/j.comcom.2022.09.012 (ScienceDirect)

Aiyanyo, I. D., Samuel, H., & Lim, H. (2020). A systematic review of defensive and offensive cybersecurity with machine learning. Applied Sciences, 10(17), 5811. https://doi.org/10.3390/app10175811 (MDPI)

Alsaigh, R., Mehmood, R., & Katib, I. (2023). AI explainability and governance in smart energy systems: A review. Frontiers in Energy Research, 11, 1071291. https://doi.org/10.3389/fenrg.2023.1071291

Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57, 132. https://doi.org/10.1007/s10462-024-10776-5 (Springer)

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Burdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), Article 8, 1–38. https://doi.org/10.1145/3545574 (DOI)

Belal, M. M., & Sundaram, D. M. (2022). Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends. Journal of King Saud University—Computer and Information Sciences, 34(10), 9102–9131. https://doi.org/10.1016/j.jksuci.2022.08.035 (Directory of Open Access Journals)

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502 (DOI)

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in CyberSecurity: A survey. IEEE Access, 10, 93575–93600. https://doi.org/10.1109/ACCESS.2022.3204171 (DBLP)

Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P.-F., Han, Y., Jmila, H., Blanc, G., Takahashi, T., & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: A literature survey. Annals of Telecommunications, 77, 789–812. https://doi.org/10.1007/s12243-022-00926-7 (Springer)

Dina, A. S., & Manivannan, D. (2021). Intrusion detection based on machine learning techniques in computer networks. Internet of Things, 16, 100462. https://doi.org/10.1016/j.iot.2021.100462 (University of Kentucky)

European Union Agency for Cybersecurity. (2022). ENISA threat landscape 2022. ENISA.

European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. ENISA. (ENISA)

European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. ENISA. (ENISA)

Fedorchenko, E., Novikova, E., & Shulepov, A. (2022). Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges. Algorithms, 15(7), 247. https://doi.org/10.3390/a15070247 (MDPI)

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419 (Colab)

Guo, Y. (2023). A review of machine learning-based zero-day attack detection: Challenges and future directions. Computer Communications, 198, 175–185. https://doi.org/10.1016/j.comcom.2022.11.001 (NIST Computer Security Resource Center)

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595 (MDPI)

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804 (DOI)

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2, 20. https://doi.org/10.1186/s42400-019-0038-7 (Springer)

Li, G., Sharma, P., Pan, L., Rajasegarar, S., Karmakar, C., & Patterson, N. (2021). Deep learning algorithms for cyber security applications: A survey. Journal of Computer Security, 29(5), 447–471. https://doi.org/10.3233/JCS-200095 (Sage Journals)

Liu, Z., Xu, B., Cheng, B., Hu, X., & Darbandi, M. (2022). Intrusion detection systems in the cloud computing: A comprehensive and deep literature review. Concurrency and Computation: Practice and Experience, 34(4), e6646. https://doi.org/10.1002/cpe.6646 (Wiley Online Library)

Machlev, R., Heistrene, L., Perl, M., Levy, K. Y., Belikov, J., Mannor, S., & Levron, Y. (2022). Explainable artificial intelligence (XAI) techniques for energy and power systems: Review, challenges and opportunities. Energy and AI, 9, 100169. https://doi.org/10.1016/j.egyai.2022.100169

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, 10, 2823–2836. https://doi.org/10.1007/s13042-018-00906-1 (ResearchGate)

Oprea, A., Singhal, A., & Vassilev, A. (2022). Poisoning attacks against machine learning: Can machine learning be trustworthy? Computer, 55(11), 94–99. https://doi.org/10.1109/MC.2022.3190787 (NIST)

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29 (NIST)

Phillips, P. J., Hahn, C., Fontana, P. C., Yates, A. N., Greene, K. K., Broniatowski, D. A., & Przybocki, M. A. (2021). Four principles of explainable artificial intelligence (NIST Interagency/Internal Report 8312). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8312 (NIST)

Qayyum, A., Ijaz, A., Usama, M., Iqbal, W., Qadir, J., & Al-Fuqaha, A. (2020). Securing machine learning in the cloud: A systematic review of cloud machine learning security. Frontiers in Data Science, 3, 587139. https://doi.org/10.3389/fdata.2020.587139 (PubMed Central (PMC))

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207 (NIST)

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2, 173. https://doi.org/10.1007/s42979-021-00557-0 (DOI)

Vassilev, A., Oprea, A., Fordyce, A., & Andersen, H. (2024). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (NIST AI 100-2 E2023). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2023 (NIST)

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. IEEE Access, 8, 146598–146612. https://doi.org/10.1109/ACCESS.2020.3013145 (DBLP)

Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEE Access, 10, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051 (ZU Scholars)

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Chen, K. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. Artificial Intelligence Review, 55(1), 129–161. https://doi.org/10.1007/s10462-021-09976-0 (ResearchGate)

National Institute of Standards and Technology. (2016). Guide to cyber threat information sharing (NIST Special Publication 800-150). https://doi.org/10.6028/NIST.SP.800-150 (NIST Computer Security Resource Center)

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1 (NIST)

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource & overview guide (NIST Special Publication 1299). https://doi.org/10.6028/NIST.SP.1299 (NIST)

National Institute of Standards and Technology. (2024). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations. https://doi.org/10.6028/NIST.AI.100-2e2023 (NIST)

Broniatowski, D. A. (2021). Psychological foundations of explainability and interpretability in artificial intelligence (NIST Interagency/Internal Report 8367). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8367 (NIST)

NIST. (2022). Towards a standard for identifying and managing bias in artificial intelligence (NIST Special Publication 1270). National Institute of Standards and Technology.

NIST. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. (NIST Computer Security Resource Center)

NIST. (2025). Implementing a zero trust architecture: High-level document (NIST Special Publication 1800-35). National Institute of Standards and Technology. (NIST Computer Security Resource Center)

Yaich, R., Balondrade, A., Sicard, A., Fouquiau, C., Giraud, G., Amokrane-Ferka, K., & Arbaretier, E. (2025). Symbiotic human–AI collaboration for augmented cybersecurity operations. Proceedings of the AAAI Symposium Series, 6(1), 350–358. https://doi.org/10.1609/aaaiss.v6i1.36072 (AAAI Publications)

Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57, 132. https://doi.org/10.1007/s10462-024-10776-5 (Springer)