IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, December 2025

Impact Factor: 7.67

AI-Driven Threat Identification and Response: Implications for Secure and Scalable Telecom Infrastructure

Shiva Kumara
Independent Researcher
University of Washington
reachkumaras@gmail.com

Abstract: *Identity Threat Response and Detection based on AI has become a crucial facilitator in the case of secure and scalable telecom infrastructure as networks progress to 5G, B5G, and highly virtualized networks. The growing popularity of cloud-native architectures, the scale of connecting a large number of devices, and the evolving pattern of access have greatly increased the attack space of identity-based threats. In this paper, a detailed overview of AI-driven Identity and Access Management (IAM) models in telecom ecosystems is provided based on authentication, authorization, and adaptive access control. It discusses how machine learning (ML) methods, supervised, unsupervised, and reinforcement learning (RL), can be used to identify identity abuse, insider threats, and abnormal behavior using user and entity behavior analytics (UEBA). The survey also examines AI-based identity threat response, mitigation, such as anomaly detection, automated incident response, privacy-preserving monitoring, federated learning and integration with identity governance and administration (IGA) systems. The paper presents the role of AI-enhanced IAM in enhancing real-time threat detection, operational risk reduction and resilience and confidence in next-generation telecom networks.*

Keywords: AI-Driven Identity Threat Detection, Identity and Access Management (IAM), Telecom Security, 5G/B5G Networks, Machine Learning Privacy-Preserving Security, User and Entity Behavior Analytics (UEBA).

I. INTRODUCTION

The rapid evolution of telecommunication infrastructures from 4G to fifth-generation (5G) and beyond-5G (B5G) networks has enabled ultra-low latency, massive device connectivity, and extensive network virtualization. Although these developments enable coverage of various services and use cases, they have also greatly increased the attack surface of telecom ecosystems [1]. Specifically, credential theft, impersonation, privilege escalation, and insider attacks have become identity-based cyber threats that have become critical security issues. In telecommunication settings, hijacked identities may cause service failures, information leaks, and massive cascading failures of interconnected elements in the network [2]. The traditional rule-based and signature-based security tools are hence not adequate in curbing the dynamic, distributed, and sophisticated identity-based attacks.

Artificial Intelligence (AI) has also come to play as a successful enabler in development of these challenges by applying smart analytics and reactive threat detection. The AI-based security systems can identify minor anomalies and predict identity-threatening behavior through the rapid manipulation of vast quantities of authentication logs, access, and behavioral data prior to their escalation into significant incidents [3], [4]. As a result, AI is widely integrated into modern models of cybersecurity to simplify the process of detection, response, and mitigation through automating it, in addition to supplementing work of human security professionals [5]. Large advancements in identity threat detection, automated response, and resilience have also been achieved due to the growing overlap between AI and cybersecurity research.

Next-generation networks (NGNs) and 5G-based networks, in particular, are vital in the future of the telecom

DOI: 10.48175/IJARSCT-30567

infrastructure. The potential transformative 5G is additionally improved by the fact that it supports network slicing, cloud-native services and a high count of heterogeneous devices that can serve a strongly interconnected digital society [6], [7]. Nevertheless, these features pose great demands for scalable flexible and secure network management. A key issue is ensuring high identity security and data privacy in such dynamic business environments as a result of heightened interconnectivity and decentralization of service provision.

The two enabling technologies that NGNs had to employ to satisfy these requirements were Network Function Virtualization (NFV) and Software-Defined Networking (SDN). SDN also enables programmable and centralized control of network and therefore enables dynamic optimization of traffic flows and fast enforcement of security policy, whereas NFV enables flexible and cost efficient deployment of virtualized network functions [8], [9]. In this respect, identity threat detection and response mechanisms generated by AI are necessary in order to assure scalable telecom infrastructures, which prompts the necessity to carry out a comprehensive overview of the existing methods, issues, and research perspectives.

A. Structure of the Paper

The structure of the paper is as follows: Section II is devoted to IAM in telecom infrastructure, with the support of authentication, authorization, and AI-enhanced access control systems. Section III introduces three machine learning methods to detect identity threats, namely, unsupervised, supervised, and RF methods. Section IV is the analysis of AI-enhanced identity threat response and mitigation, such as anomaly detection, automated incident response. Lastly, Section V offers some knowledge on how the system can be integrated with IGA systems, and Section VI gives the conclusions and future research directions.

II. IDENTITY AND ACCESS MANAGEMENT (IAM) IN TELECOM INFRASTRUCTURE

The IAM of the telecom infrastructure is the first to offer secure authentication, authorization and access control over massive and extremely dynamic networks. The operators can already detect any form of identity-related threats within the network and at the same time modify the access policies to include AI-enhanced authentication, user behavior analytics, and automated access control. These smart IAM systems not only transform the industry but also reduce the risk posed by insiders and outsiders; in addition, they make the modern telecom ecosystems more sustainable and reliable.

A. Authentication and Authorization Mechanisms

Access control is founded on authentication of identities of the users, network devices or other network entities to access data, applications and systems. The common authentication process involves users or devices registering with an authentication server, where they are issued unique identifiers and credentials (keys or certificates) that are stored on the server. For access requests, these credentials are authenticated to verify their authenticity and freshness before access is authorized based on established access control policies [10]. When authentication is successful, a secure session is established using session tokens, and subsequent interactions occur without re-authentication (as shown in Fig. 1). Encryption protocols like TLS are used to remove confidentiality risks and integrity breaches to the data involved in the session [11]. Credential revocation, renewal, and audit logging mechanisms are additional measures to enhance security and prevent misuse.

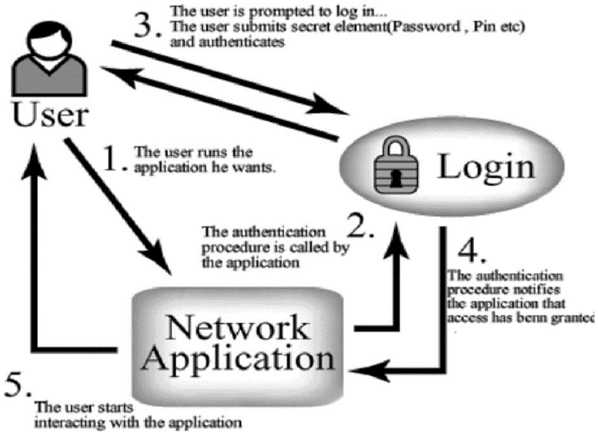
3. The user is prompted to log in...
The user submits secret element(Password , Pin etc)
and authenticates
User
1. The user runs the application he wants.
Login
The authentication procedure is called by the application
2.
4.
The authentication procedure notifies the application that access has benn grantec
Network Application
5.
The user starts interacting with the application

Fig. 1. Authentication Mechanisms.

In order to authenticate users and provide a security layer that may be used for further communication, authentication techniques define a challenge-response protocol in which information is transferred between the client and the server: biometric, token, or password-based authentication.

Password-Based Authentication

A list of names and passwords is kept on file on the server. The server provides access if a certain name is on the list and the user enters the right password. Authentication based on certificate. A component of the SSL protocol is client authentication via certificates.

Token-based Authentication

Token-based authentication is a kind of security where a server issues a security token that the server uses to verify a user's identity when they try to access a server, network, or other protected system [12]. After security token verification the application processes the request of the user.

Biometric-based Authentication

A security procedure called biometric authentication (BA) uses a person's distinct biological traits to confirm that they are who they say they are. BA is usually employed in regulating access to digital and physical resource such as computer, building and room.

Authorization: There is great variety in access control models of authorization (AuthZ). The Access Control Lists (ACLs) link the individual user identity to a given privilege of each resource in a centralized fashion which provides easy traceability but has scalability issues and single point of failure. Role-Based Access control (RBAC) enhances manageability through assigning permission to roles instead of users and is extensively used in enterprise and cloud systems, but it fails to work as well in highly dynamic systems because of role explosion [13]. Attribute-Based Access Control (ABAC) also has the added benefit of flexibilities since it depends on many attributes associated with users, resources, and contextual requirements when making authorization decisions, but is difficult and expensive to implement due to the overhead of attribute definition and maintenance [14]. Capability-Based Access Control (CapAC) uses capability tokens to grant access; these tokens contain authorization information and support decentralized authorization and peer-to-peer interactions. However, life cycle management of tokens is very difficult in these settings, mainly due to resource constraints or intermittent connections.

B. Identity and Access Management (IAM) in Telecom

IAM, which is one of the key elements of cybersecurity, is changing under the influence of AI. Credential theft and phishing is increasingly becoming a vulnerability of security tokens and passwords. Biometric identification systems based on AI utilize facial recognition, speech recognition or behavioral biometrics to be more secure. These systems authenticate users through unique physiological or behavioral attributes with help of ML algorithms and make it difficult to the attacker to masquerade as a legitimate user. Analyzing user behavior can also identify and prevent any

DOI: 10.48175/IJARSCT-30567

real-time attempts of unauthorized access by AI. The application of AI in cybersecurity has challenges even though it has numerous advantages. The key issue is adversarial attacks during which cybercriminals compromise AI models to avoid detection or to produce false positives [15]. Assailants may also alter the data inputs to make AI systems believe that a malicious action is innocent. As shown in Fig. 2, businesses must make sure AI-driven systems are ethical, transparent, and explicable in order to foster trust and accountability.

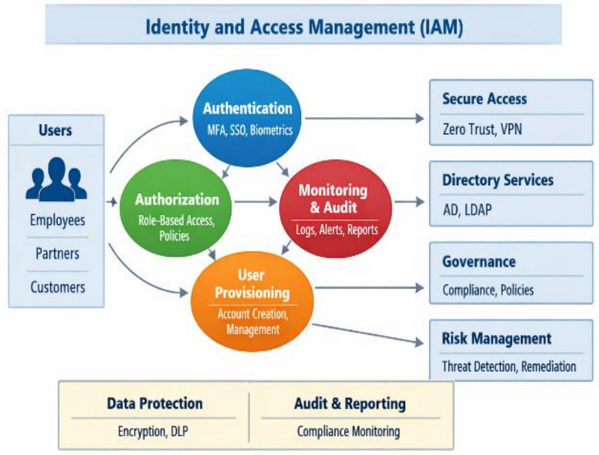

Fig. 2. Identity and Access Management.

Zero-trust architecture (ZTA) improves the use of AI in cybersecurity. The idea of zero-trust emphasizes the authentication of users and devices and strict access controls. ZTA implementation through AI and ML is mainly focused on the real-time monitoring, assessing the risk, and managing the access on an adaptive basis. AI algorithms can use the location, device type, and history of access by the users to dynamically modify access permissions. This limits the area of attack and prevents insider attacks and horizontal network movement. Cybersecurity loses its identity to federated learning, quantum ML and edge AI. Federated learning allows a number of businesses to cooperate in the training of models without revealing sensitive information, enhancing the safety and confidentiality of such information [16]. Quantum ML applies quantum computing to solve difficult cybersecurity issues, including the process of factoring large integers to do cryptography. Edge AI, that is processed on the devices and not in data centers, minimizes latency and bandwidth consumption, allows detecting a threat faster. The AI and blockchain technology also provide new opportunities to protect online transactions and provide networks [17]. The impartiality and decentralization of blockchain supplement the analytics of AI, allowing sharing data safely and detecting fraud. The AIs are able to identify anomalies and fraudulent activities in blockchain transactions patterns and enhance the integrity of the system.

C. User Behavior Analytics and Automated Access Control

The identity AI-based IAM systems rely on the User Behavior Analytics (UBA). UBA observes user actions so that they can develop operational patterns that are likely to occur due to which an organization can identify security threats that do not comply with the expected pattern(s). The detection system informs the security team of investigation requirements whenever the user links to any external resources out of areas that are not within their customary territories. The predictive approach reduces illegal access to the system and security gaps.

IAM systems are automated to control access by use of AI. IAM systems use security mechanisms which are based on strict, set rules that do not keep up with changes in the user accounts. The real-time access assessment of AI-supported systems takes advantage of the operating parts that assess user activities, device security measures, and the environmental factors (Garcia, 2023). Users have greater security and improved authentications due to flexible IAM system design.

D. Identity-Based Threats in Telecom Ecosystems

The modern telecommunications business environment is more hectic than ever before, thus requiring instant threat detection. Telecom networks have become the foundation of contemporary communication that links billions of hardware devices and enables them to exchange sensitive data. As the problem of advanced cyber threats emerges, telecom companies are confronted with an uphill task: how to secure their networks and offer good quality service to their customers. The real-time threat detection enables telecom operators to detect and act on possible security breaches in real time, and not after they have been detected. Such active strategy is necessary in the environment when cybercriminals are actively developing their strategies to take advantage of vulnerabilities [18]. Failure to initially detect a threat can have dire outcomes in the form of data breaches, loss of services, and loss of money. An example of this is the collapse of the network performance due to a successful Distributed Denial of Service (DDoS) attack which impacts millions of users. Telecom companies can minimize risk factors and offer the timely response to any irregularity in network traffic and enhance the security of a network infrastructure and customers confidence with the help of real-time detection systems.

This practice has been successful in the case of a number of telecom firms that succeeded in integrating AI-based real-time threat detection into their security measures. The most dominant one is that of AT&T that has employed ML algorithms to process the patterns of network traffic in real-time. Using AI technologies, AT&T could detect abnormal behavior automatically, such as abnormal spikes in the data traffic or abnormal logins [19]. This has helped them to detect and answer to threat in a more efficient way, reducing the average time to detect and confine the possible breaches [20]. The other one is Vodafone, which implemented an AI-based threat intelligence platform to enhance its cybersecurity stance. Vodafone can gather and process data in various locations, including network equipment, customer interactions, and third-party threat feeds, through the advanced analytics. A holistic approach would enable the company to detect the threat on a real-time basis and possibly forecast the potential vulnerability based on the previous information. As a result, there is a significant decrease in the amount of successful attacks, and Vodafone demonstrates the potential of AI to enhance telecom security [21]. In a similar vein, Telefonica has used AI tools to manage problems and identify dangers. In order to identify risks, their system scans hundreds of data sources, including those from social media and the dark web, using NLP (natural language processing). Telefonica can stay ahead of dangers as they arise thanks to this innovative technique, which also helps them with their security policy. The adoption of AI in their security capabilities has enabled Telefonica to be faster in threat detection, which allows the company to make decisions faster and respond more promptly to the threat.

III. MACHINE LEARNING TECHNIQUES FOR IDENTITY THREAT DETECTION

This section discusses improvements of ML methods to identity threat detection because it allows a dynamic analysis of authentication history, access history, and user behavior unlike the classic rule-based system. With the help of behavioral and anomaly-based analytics, reinforcement learning, and supervised and unsupervised learning, the AI-driven models can be used to detect compromised identities, insider threats, and new attack patterns in real time.

A. Role of Artificial Intelligence in Identity Threat Detection.

The accelerated pace of interoperability, IoT gadgets, and cloud services has boosted identity-driven cyber-crime like credential stealing, account compromise, identities, and privilege misuse considerably. Because they cannot be dynamically deployed to address dynamically changing attack patterns, traditional rule-based and signature-based security solutions are becoming less effective against such emerging threats. ML and its manifestations in the form of AI instrumental in the identity threat detection process by providing constant processing of authentication procedures, access requests, and user actions. Models of AI can handle high amounts of identity-related data in real-time to determine the behavioral baseline and detect minor deviations that signal identity compromise. The systems that are AI-centered also have the capability to evolve with the dynamic user behavior and security measures unlike the traditional security approaches.

Machine Learning in Cybersecurity

In field of modern cybersecurity, one of the most potent technologies is ML, that is also a type of AI. The algorithms of ML allow learning systems to learn automatically without a specific program, and therefore these algorithms are quite efficient in dynamic conditions of complex environments including cybersecurity [22]. The ML methods are widely classified into three paradigms that are the supervised, unsupervised and reinforcement learning. The applications and benefits of each paradigm in cybersecurity are different.

Supervised Learning

In supervised learning, the ML model is trained with a labeled dataset that provides input-output pairs to teach the model how to make predictions. This is very useful for classifying and identifying malware in the field of cybersecurity. As an example, a trained ML model could be fed with a set of known malware signature files and safe software and trained to then classify new files based on the learned patterns as malicious or safe. In intrusion detection systems (IDS), supervised learning is common in detecting known attack signatures and notifying security personnel when an analogous activity is discovered. Nevertheless, its performance can be restricted by the quantity and quality of the labeled data, which may be problematic when there are novel and unidentified hazards.

Unsupervised Learning

Unlike supervised learning, which depends on labeled data, unsupervised learning does not. The data's inherent shape is broken down to reveal hidden patterns and anomalies instead. The paradigm lends itself particularly to the business of anomaly detection, in which it is the objective to identify abnormal activities that are out of the ordinary and do not require prior information on particular attack signatures [23]. Network monitoring systems frequently employ unsupervised learning approaches to find zero-day vulnerabilities, insider assaults, and advanced persistent threats. These algorithms are able to mark suspicious behavior that may have been indicative of an intrusion even when the type of attack is unknown by analyzing the network traffic patterns continuously. Security teams may better comprehend and categorize novel attack vectors by using unsupervised learning to cluster similar types of cyberthreats.

Reinforcement Learning

A more developed type of ML is reinforcement learning (RL), where a model is able to learn through its interactions with the immediate surroundings and comments in the form of a reward or a penalty. Reinforcement learning in cybersecurity has potential in adaptive defense. The RL model would then over time improve its defense strategies by being more efficient in autonomously preventing or incurring intrusions depending on its history of interaction with attackers. In automated pentating, AI systems look for network vulnerabilities and learn how to exploit or defend against them in a simulated environment. Reinforcement learning is another use of this topic. Combining these machine learning paradigms offers a variety of techniques to enhance cybersecurity.

B. Behavioral and Anomaly-Based Identity Threat Detection

Continuous observation and measurement of user and entity behavior on authentication, access, and use events is used to identify identity abuse by identity threat detection based on behavioral and anomaly-based identity threats that builds on AI. The models of User and Entity Behavior analytics (UEBA) set dynamic behavior thresholds based on normal behavior patterns of logins, frequency of access, resource utilization, and sequence of interactions in order to identify deviations in real time, which could be used to signal compromised credentials or unauthorized access. The systems are especially efficient in detecting insider threats, where malicious or careless activities are launched by legitimate identities, and also in detecting sneaky account takeovers that circumvent conventional security measures. Through the correlation of behavioral anomalies with contextual factors, including the posture of the device, its location, and sensitivity to access, AI-based risk scoring mechanisms give continuous trust scores to identities, which can be used to actively mitigate the risk, e.g., step-up authentication, access control, or session termination.

IV. AI-DRIVEN IDENTITY THREAT RESPONSE AND MITIGATION

Identity threat response and mitigation, including anomaly detection, automated incident response, and privacy-preserving learning, are all highly advanced, and require only limited human effort to swiftly identify and isolate identity-based attacks. The technologies are premised on the combination of federated learning, privacy by design tracking as well as automated response systems, that not only protects data in a manner that is scalable and real time, but also protects sensitive identity information.

A. AI Approaches for Anomaly Detection and Response Automation.

The identification of the potential cybersecurity vulnerabilities is needed to provide a successful safeguarding against cyber threats. By using AI, companies can have access to more advanced features that cannot be achieved through a conventional approach, which enables them to improve their security.

Anomaly Detection

AI systems are highly useful in detecting abnormalities in behavior, which constitutes a significant protection against cyberattacks. This approach is predicated on the active process of baseline construction, which enables AI to continuously collect data and track system behavior and the intricate user network in the cloud environment. It requires one to develop the foundations correctly with the inclusion of shared behavior in the cloud ecosystem in a way that influences the unnatural functionality of AI [24]. Through continuous observation and learning, AI is capable of detecting similarities and interactions between people, systems, and applications. Therefore, comprehension enables prompt identification of deviations that can indicate possible security risks. Moreover, ongoing analysis of user behaviors, network activity, and system processes enables AI systems to improve and modify their conception of normalcy, guaranteeing that the baseline continues to be applicable even when user patterns and system configurations change.

Response Automation

AI is a security component because it can quickly identify and respond to threats, which speeds up recovery times and reduces damage by simplifying incident response methods. AI can reduce damage and speed up recovery times by simplifying incident response processes since it can quickly identify and respond to threats, therefore making this component of security automation and incident response more effective and enabling smooth, advanced threat detection and response in cloud security. In addition, the rapid threat detection and response of AI reduces the impact of security issues without requiring human involvement. AI, for instance, may swiftly and effectively respond to new threats by automatically quarantining infected devices or undoing modifications initiated by cyber criminals [25]. AI-driven automation relieves the teams of these tedious activities, which speeds up response times and lowers the chance of mistakes, resulting in a more flexible and effective security framework and promoting ongoing security improvement.

B. Data Privacy in AI-Driven Monitoring

The pipeline is based on privacy-by-design: sensitive pseudonymized (format-preserving tokenization or salted hashing), and separated by field-level encryption such that models are presented with the minimal data needed. Impose tiered data paths a limited raw archive to audit/replay and privacy-filtered stream to analytics with schema registry guards which reject unexpected PII. Sessionization and featurization provide k-anonymity style bucketing on the rare values, and apply differential privacy to aggregate metrics that are to be reported on dashboards in order to avoid identity re-identification. ABAC/RBAC with short-lived credentials, customer-managed keys (CMKs) within HSM-based KMS, and auditable audit trails control access to raw signals, model outputs include lineage and privacy tags such that SOAR playbooks can automatically mask or redact evidence in a ticket. Lastly, retention is finite (e.g. 90/180 days), and deletions via the feature store and model caches are propagated to maintain training/serving parity without re-creating deleted datariables are reduced to a minimum at collection, strongly.

C. Federated Learning for Identity Threat Models

Federated learning (FL) trains anomaly encoders and risk scorer tenants or regions by transmitting model updates and not data to an aggregator guarded with secure aggregation together by attested orchestration. Every location calculates gradients on the local features, which are clipped and perturbed with noise to provide different privacy and then takes part in aggregation rounds, which consider the heterogeneous datasets and stragglers through FedProx-like targets. Model cards monitor both per-site performance and drift to allow reweighting or holding back underperforming cohorts and a privacy budget (e, d) is monitored to limit cumulative exposure. Due to the variability of identity semantics

DOI: 10.48175/IJARSCT-30567

because identity semantics are often local, Jointly train global FL backbones with local adapters (fine-tuned heads, calibration layers) to maintain accuracy, data locality, whereas encrypted checkpoints and signature prevent model poisoning, and server-side anomaly detectors monitor malicious updates (e.g., sign-flip or backdoor gradients).

D. Integration with Identity Governance Systems (IGA)

AI-powered access management systems are capable of changing their authorization rules by taking into account various risk factors occurring at the moment such as the activity of the user, the condition of the device, and the quality of the network [26]. AI policy enforcement is not limited to the static setting of rules and adapts the access rights in real-time, thus guaranteeing the minimum access required but without disrupting the provision of the service. Such an approach strengthens the resistance of the credential abuse and insider attack.

Further alignment of ITDR and IGA can turn the findings of detecting into long-lasting cuts in the standing privilege. Instead of increasing the ticket price, ITDR might be able to suggest least-privilege role redesigns, entitlement cleanups, and candidates of access re-certification, and IGA workflows could offer approvals, segregation-of-duty checks and audit trails. The research to be done should be on translating behavioral risk into governance artifacts, learning policies that suggest safe patterns of JIT elevation, and closed-loop studies that measure months of blast-radii reduction. By aligning ITDR signals with business context in HR and ERP systems, over-revocation is likely to be avoided, as well as compliance constraints considered.

V. LITERATURE REVIEW

Recent research indicates an increasing level of efficacy of AI-based cybersecurity solutions to improve threat detection and prompt response, and resilience across 5G/B5G networks, enterprise applications, national infrastructure, and telecom environments. All of these works highlight progressive AI methods and architectural frameworks, define the main problems associated with scalability, explainability, privacy, and real-time processing. The key contributions, methods, and research gaps identified in the existing literature are summarized and compared in Table I.

Nirdhar (2025) offers a thorough examination and comparison of AI-based methods, for example ML, DL, RL, and hybrid AI, for identifying and thwarting cyberthreats in 5G/B5G networks. An AI-security architecture's layers are shown, and each approach is assessed according to many criteria, including complexity, scalability, accuracy, and real-time viability. The study offers a path for secure, intelligent next-generation networks and explores potential future developments for example explainable AI (XAI), edge AI, federated learning, and quantum AI [27].

Joshua and Mylavarapu (2025) analyze the concept of artificial intelligence (AI), its use in cybersecurity, the history of cyberthreats, and the advantages and disadvantages of AI-based security techniques. Another aspect that is evaluated by them is the future of AI-based cybersecurity, the experience of AI failures, and their successful uses by large corporations. The discovery highlights importance of automation and human controls to establish scalable and strong security systems which are capable of keeping abreast with the continuously evolving cyber threat landscape. To become successful in digital safety measures, it is necessary to balance the two. Increased interconnection in the digital world has seen organizations being overwhelmed by more advanced cyberattacks that cannot easily be averted using conventional security practices [28].

Akinloye, Anwansedo and Akinwande (2024) found that accuracy and speed of threat assessment and response are significantly increased by AI-driven solutions. Automation potential of AI might expedite threat mitigation and eliminate the need for human analysts. Additionally, AI's industry applicability indicates that it may be applied in a range of settings and adapt to new threats. Protecting national infrastructure networks is another significant cybersecurity trend made possible by AI-enabled threat detection and response systems. Therefore, these technologies eventually make a country's whole infrastructure more robust when they are improved with the capacity to identify and counteract intrusions [29].

Dhanushkodi and Thejas (2024) show that in order to ensure the dependability and legitimacy of AI-based security solutions, explainability and resilience in AI models are essential. The papers being examined include a broad range of sectors and businesses, including driverless vehicles, 5G networks, Industry 5.0, and the Internet of Things. These articles can show how AI is adaptable in tackling particular security issues in the sector. Transformer-based frameworks, blockchain implementation, and federated learning are some of the current advancements in threat detection systems that continue to improve the development of a more reliable and real-time system. However, real-time processing, privacy, security, and managing enormous volumes of data continue to present challenges [30].

Azambuja et al. (2023) Provide a systematic study of the literature to find publications about cyberattacks powered by AI and analyze them to determine cybersecurity solutions. In order to give the research community, the knowledge they need to create defenses against similar risks in the future, this study uses literature analysis to investigate the impact of this novel threat. The findings may be applied to conduct studies on AI-assisted cyberattacks [31].

Manda (2023) explains the most recent advancements in next-generation firewalls (NGFWs), which incorporate intrusion protection systems and deep packet inspection, and application knowledge to provide enhanced security capabilities. By evaluating these technologies, the study shows how important they are for protecting telecom networks from online threats such as Distributed Denial-of-Service (DDoS) assaults, ransomware, and zero-day attacks. Additionally, it describes how NGFWs use AI and ML to improve threat detection and response and adopt a more proactive security strategy [32].

Table 1: Comparative Analysis of Recent Studies on CRM and Digital Transformation in Banking

Authors	Focus Area	AI Techniques Used	Key Contributions	Evaluation Dimensions / Findings	Limitations & Future Directions
Nirdhar et al. (2025)	Identifying and reducing cyber threats in 5G and B5G networks	ML, DL, RL, Hybrid AI	Provides a thorough comparison of AI methods for next-generation networks and suggests a layered AI-security architecture	Assessed techniques for computational complexity, real-time viability, scalability, and accuracy.	Emphasizes how secure networks in the future will require Explainable AI (XAI), Edge AI, Federated Learning, and Quantum AI.
Joshua and Mylavarapu (2025)	AI sin enterprise cybersecurity	AI-driven automation, decision-support systems	Analyzes evolution of cyber threats, AI fundamentals, real-world implementations, and failures	Demonstrates improved scalability and adaptability through AI-driven security frameworks	Emphasizes balancing automation with human oversight to avoid over-reliance on AI
Akinloye et al. (2024)	Cybersecurity for national infrastructure networks	AI-driven systems for danger detection and reaction	Shows AI significantly improves speed and accuracy of detection and mitigation	Automation reduces human workload and accelerates incident response	Calls for further validation across diverse infrastructure environments
Dhanushkodi et.al. (2024)	Security of Industry 5.0, IoT, 5G, and self-driving vehicles	Blockchain-integrated AI, federated learning, and transformer models	Emphasizes explainability and resilience as core requirements for trustworthy AI security systems	Demonstrates AI adaptability across heterogeneous domains	Large-scale data management, real-time processing, and privacy protection are among the difficulties
Azambuja et al. (2023)	AI-enabled cyberattacks and defenses	AI-assisted attack modeling and analysis	Systematic literature review identifying AI-based cyberattack patterns	Provides insights for anticipating and defending against future AI-supported attacks	Lacks empirical validation; primarily literature-driven analysis
Manda, et al.	Telecom	ML and AI-	Evaluates NGFWs	Effective against	Highlights need for

(2023)	network security using NGFWs	enhanced firewalls	integrating DPI, IPS, and application awareness	DDoS, ransomware, and zero-day attacks	tighter AI integration for real-time, proactive defense

VI. CONCLUSION AND FUTURE WORK

The threat identity response and detection, which is through AI-based, in contemporary telecom infrastructures in telecom have been deeply discussed. As the telecom networks are being migrated to 5G, B5G, and cloud-native architecture, identity-based attacks have become dynamic and more advanced and can no longer be easily monitored as was done by an old-fashioned regulation rule-based security architecture. With addition of ML and AI to IAM, the dynamically changing environment can be monitored, auto-authentication and authorization can be carried out, and decisions regarding authorization can be made dynamically as well as be context-aware. Among the most important techniques for improving the real-time identification are automated incident response, anomaly detection, user and entity behavior analytics (UEBA), and federated learning, insider threat, and privilege abuse detection capacity. Additionally, by enforcing least-privilege and optimizing policies, the convergence of AI-driven Identity Threat Detection and Response (ITDR) and Identity Governance and Administration (IGA) can ensure the absence of hazards over the long run. Altogether, AI-enabled IAM systems enhance scalability, resiliency, and reliability, which serve a critical role in ensuring next-generation telecom ecosystems in the context of providing a balance between operational effectiveness, privacy, and regulatory adherence.

It should be researched the future of explainable AI in identity risk decisions, high resistance to adversarial attack, and the federated and edge AI models should be widely implemented. The use of quantum resistant cryptography with standardized ITDR-IGA models will enhance security of identity in telecom networks.

REFERENCES

[1] A. S. Yesuf, "A Review of Risk Identification Approaches in the Telecommunication Domain," in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, SCITEPRESS - Science and Technology Publications, 2017, pp. 389–396. doi: 10.5220/0006197603890396.

[2] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[3] R. Kaur, D. Gabrijelcic, and T. Klobucar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.

[4] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[5] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 09, no. 03, pp. 205–212, 2025, doi: 10.47001/IRJIET/2025.903027.

[6] A. Agrawal, G. Dubey, M. Dubey, P. Narwaria, and D. P. Khatri, "Next Generation Networks: Advancements, Challenges, and Opportunities for Scalable and Secure Infrastructure," in *Futuristic Trends in Network & Communication Technologies Volume 3 Book 2*, 2024, pp. 58–71. doi: 10.58532/V3BGNC2P2CH2.

[7] V. Shewale, "Demystifying the MITRE ATT & CK Framework: A Practical Guide to Threat Modeling," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 3, pp. 182–186, May 2025, doi: 10.32996/jcsts.2025.7.3.20.

[8] O. Afolalu and M. S. Tsoeu, "Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions," *Futur. Internet*, vol. 17, no. 4, p. 133, Mar. 2025, doi: 10.3390/fi17040133.

[9] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 3, pp. 6–18, Mar. 2025, doi: 10.48175/IJARSCT-23902.

[10] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A Review of the Authentication Techniques for Internet of Things Devices in Smart Cities: Opportunities, Challenges, and Future Directions," *Sensors*, vol. 25, no. 6, p.

1649, Mar. 2025, doi: 10.3390/s25061649.

[11] M. Kokila and S. Reddy K, “Authentication, access control and scalability models in Internet of Things Security–A review,” *Cyber Secur. Appl.*, vol. 3, p. 100057, Dec. 2025, doi: 10.1016/j.csa.2024.100057.

[12] S. Rajarajeswari and A. M. Stella, “A Review of Authentication and Authorization Methods,” *Int. J. Comput. Sci. Inf. Technol. Res.*, vol. 7, no. 3, pp. 78–83, 2019.

[13] Y. Wang, P. Castillejo, J.-F. Martínez-Ortega, and V. Hernández Díaz, “A survey on Identity and Access Management for future IoT services,” *Comput. Networks*, vol. 272, p. 111718, Nov. 2025, doi: 10.1016/j.comnet.2025.111718.

[14] S. Narang and A. Gogineni, “Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment,” *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[15] D. Patil, “Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Prevention Mechanisms Through Machine Learning and Data Analytics,” *SSRN*, pp. 39–43, 2024.

[16] D. Patel, “Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity,” *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, 2023, doi: 10.56975/tijer.v10i6.158517.

[17] S. S. U. Hasan, A. Ghani, A. Daud, H. Akbar, and M. F. Khan, “A Review on Secure Authentication Mechanisms for Mobile Security,” *Sensors*, vol. 25, no. 3, p. 700, Jan. 2025, doi: 10.3390/s25030700.

[18] J. K. Manda, “AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations,” *SSRN Electron. J.*, vol. 6, no. 2, pp. 333–340, 2024, doi: 10.2139/ssrn.5003638.

[19] S. Amrale, “A Novel Generative AI-Based Approach for Robust Anomaly Identification in High-Dimensional Dataset,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, pp. 709–721, Oct. 2024, doi: 10.48175/IJARSCT-19900D.

[20] N. Ahmed *et al.*, “Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction,” *Sensors*, vol. 22, no. 20, p. 7896, Oct. 2022, doi: 10.3390/s22207896.

[21] Y. Ding, “Research on Network Security Threat Detection and Defense Mechanism Based on Artificial Intelligence,” in *2024 International Conference on Information Technology, Comunication Ecosystem and Management (ITCEM)*, IEEE, Dec. 2024, pp. 119–123. doi: 10.1109/ITCEM65710.2024.00030.

[22] N. Mohamed, “Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms,” *Knowl. Inf. Syst.*, vol. 67, no. 8, pp. 6969–7055, Aug. 2025, doi: 10.1007/s10115-025-02429-y.

[23] R. Q. Majumder, “Machine Learning for Predictive Analytics: Trends and Future Directions,” *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3557–3564, May 2025, doi: 10.38124/ijisrt/25apr1899.

[24] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, “Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data,” in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[25] V. N. Satyam, D. Mishra, and B. G. Mahapatra, “AI-Driven Identity Threat Detection and Response Systems for Modern Cloud Security Operations Centers,” *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 4, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P112.

[26] P. Chandrashekar and M. Kari, “Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System,” vol. 11, no. 4, pp. 901–907, 2024.

[27] K. Nirdhar, “AI-Driven Cyber Threat Detection and Mitigation in 5G and Beyond: Enhancing Security in the Telecom Industry - A Survey and Comparative Analysis,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 7, pp. 1613–1616, Jul. 2025, doi: 10.22214/ijraset.2025.73249.

[28] E. Joshua and P. Mylavarapu, “AI-driven threat detection: Enhancing cybersecurity automation for scalable security operations,” *Int. J. Sci. Res. Arch.*, vol. 14, no. 3, pp. 681–704, Mar. 2025, doi:

10.30574/ijsra.2025.14.3.0615.

[29] A. Akinloye, S. Anwansedo, and O. T. Akinwande, "AI-Driven Threat Detection and Response Systems for Secure National Infrastructure Networks: A Comprehensive Review," *Int. J. Latest Technol. Eng. Manag. Appl. Sci.*, vol. 13, no. 7, pp. 82–92, Aug. 2024, doi: 10.51583/IJLTEMAS.2024.130710.

[30] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access*, vol. 12, pp. 173127–173136, 2024, doi: 10.1109/ACCESS.2024.3493957.

[31] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," *Electronics*, vol. 12, no. 8, p. 1920, Apr. 2023, doi: 10.3390/electronics12081920.

[32] J. K. Manda, "Next-Generation Firewall Technologies for Telecom: Evaluating Advanced Firewall Technologies and Their Role in Protecting Telecom Networks from Evolving Cyber Threats," *SSRN Electron. J.*, vol. 10, no. 3, pp. 860–871, 2023, doi: 10.2139/ssrn.5136748.