ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 13, Issue 3, pp: (150-166), Month: July - September 2025, Available at: www.researchpublish.com

Entrepreneurial Innovations in AI-Driven Anomaly Detection for Software-Defined Networking in Critical Infrastructure Security

Chima Nwankwo Idika[1], Joy Onma Enyejo[2], Onuh Matthew Ijiga[3], Nonso Okika[4]

[1]Department of Computer Science, Prairie View A & M University, Prairie View Texas, USA.

[2]Department of Business Management, Nasarawa State University, Keffi, Nasarawa State, Nigeria.

[3]Department of Physics, Joseph Sarwaan Tarkaa University, Makurdi, Benue State, Nigeria.

[4]Network Planning Analyst, University of Michigan, USA.

DOI: https://doi.org/10.5281/zenodo.16408773

Published Date: 24-July-2025

Abstract: **The convergence of artificial intelligence (AI), software-defined networking (SDN), and cybersecurity has opened new avenues for protecting critical infrastructure systems against increasingly sophisticated cyber threats. This review explores how emerging entrepreneurial ventures are pioneering AI-driven solutions for anomaly detection within SDN architectures, particularly in sectors like energy, transportation, and healthcare. By decoupling control and data planes, SDN offers centralized programmability that enhances network agility but also introduces new vulnerabilities. AI techniques—such as machine learning, deep learning, and neural networks—have been adopted by cybersecurity startups to build scalable and adaptive anomaly detection frameworks that mitigate these vulnerabilities in real time. This paper examines the landscape of entrepreneurial innovation, highlighting case studies of startups that leverage AI to enhance threat detection, automate response mechanisms, and provide predictive security analytics in SDN environments. Emphasis is placed on the integration of zero-trust principles, edge intelligence, and decentralized detection architectures. Furthermore, the paper analyzes the commercial viability, scalability, and deployment challenges of these solutions, as well as their implications for regulatory compliance and cyber resilience. The findings highlight the growing significance of entrepreneurial ecosystems in driving technological advancements that safeguard critical infrastructure against evolving cyber risks.**

Keywords: **AI-Driven Anomaly Detection; Software-Defined Networking (SDN); Critical Infrastructure Security; Cybersecurity Entrepreneurship; Zero-Trust Architecture.**

1. INTRODUCTION

1.1 Background on Critical Infrastructure and Cybersecurity Challenges

Critical infrastructure (CI) encompasses vital systems and assets—such as power grids, water treatment facilities, healthcare systems, and transportation networks—whose disruption would significantly impact national security, economic stability, and public health. The increasing digitization and interconnectivity of these infrastructures, while promoting operational efficiency, simultaneously expose them to sophisticated cyber threats that exploit software vulnerabilities and complex network dependencies (Boyson, 2014). As traditional perimeter-based defenses prove inadequate, adversaries have shifted toward persistent, stealthy intrusion campaigns targeting programmable control systems, particularly through lateral movement and supply chain vectors.

Cyber-physical systems embedded in CI operate with tight real-time constraints and often lack basic encryption or access control, making them prime targets for ransomware, industrial sabotage, or state-sponsored attacks (Radanliev et al., 2020). The introduction of IoT and remote-access mechanisms for infrastructure management exacerbates these vulnerabilities, creating expanded attack surfaces. Complicating defense strategies is the heterogeneity of CI environments, which comprise legacy systems with poor update mechanisms, rendering standard patch management ineffective.

Resilience in this context is not only the ability to prevent attacks but also to detect, respond, and recover quickly with minimal downtime (Ijiga, O. M., 2024). This necessitates a robust, proactive cybersecurity posture that leverages intelligent anomaly detection models and dynamic threat intelligence (Pemmasani, 2023). Addressing these challenges requires scalable, adaptable, and entrepreneurial innovation across sectors to secure critical digital assets and maintain service continuity.

1.2 Role of SDN in Modern Network Architectures

Software-Defined Networking (SDN) represents a transformative shift in modern network architecture, enabling greater control, programmability, and agility through the decoupling of the control and data planes. Traditional networks rely on tightly integrated hardware and software components, making them rigid, expensive to upgrade, and difficult to manage (Idoko, et al., 2024). SDN, on the other hand, centralizes network intelligence in a programmable controller, allowing dynamic policy enforcement, fine-grained traffic engineering, and automated management through APIs and software interfaces (Kreutz et al., 2015). This architecture provides a fertile ground for innovation, particularly in security, as it facilitates real-time monitoring and swift reconfiguration of network paths in response to anomalies.

The integration of SDN in critical infrastructure, such as smart grids and industrial IoT networks, allows for scalable, adaptive, and resilient communication frameworks. However, this centralization also introduces a potential single point of failure, elevating the importance of robust security mechanisms (Lara et al., 2014). The dynamic nature of SDN traffic and flow rules necessitates the deployment of intelligent anomaly detection systems capable of operating in real time and understanding contextual traffic behaviors. As entrepreneurial innovations harness SDN's flexibility, startups are building modular, scalable AI-based solutions tailored for multi-domain environments, balancing openness with stringent access controls (Idoko, et al., 2024). Thus, SDN plays a pivotal role in reshaping the cybersecurity posture of modern critical systems.

1.3 Importance of Anomaly Detection

Anomaly detection is an indispensable component of modern cybersecurity frameworks, particularly in safeguarding dynamic and mission-critical environments such as Software-Defined Networks (SDNs). Unlike signature-based detection methods, which rely on predefined patterns of known attacks, anomaly detection identifies deviations from established baseline behaviors, making it particularly suited to recognizing novel, zero-day threats and subtle policy violations (Chandola et al., 2009). This capability is crucial in SDN environments, where network behavior evolves rapidly and where centralized controllers can become high-value targets for cyberattacks.

The real-time identification of anomalies ensures that threats such as Distributed Denial of Service (DDoS), man-in-the-middle attacks, or lateral movements are detected before significant damage occurs. Effective anomaly detection frameworks must handle high-dimensional, high-volume data streams with minimal false positives. Recent entrepreneurial advances leverage deep learning, time-series modeling, and unsupervised learning to refine detection accuracy in complex, evolving networks (Ahmed et al., 2016). In particular, startups are developing context-aware, AI-enhanced solutions that adaptively learn from traffic patterns and autonomously recalibrate thresholds based on evolving risk profiles.

These intelligent systems enhance situational awareness and shorten the mean time to detect (MTTD) and respond (MTTR) to security incidents. As the SDN paradigm becomes ubiquitous across critical infrastructure, anomaly detection will remain central to operational resilience, data integrity, and the prevention of catastrophic system failures.

1.4 Emergence of Entrepreneurial Innovation in AI-Based Security

The emergence of entrepreneurial innovation in AI-based security reflects a strategic realignment of cybersecurity development away from monolithic institutions toward agile, venture-driven ecosystems. Startups and innovation-driven enterprises have begun to dominate the cybersecurity landscape by commercializing cutting-edge AI technologies designed to detect and mitigate sophisticated threats in real time (Gans & Stern, 2017). These entrepreneurs harness cloud-native architectures, federated learning, and blockchain-integrated security mechanisms to build intelligent detection and response systems capable of securing dynamic infrastructures like Software-Defined Networks (SDNs).

Unlike traditional enterprises burdened by legacy infrastructure, AI-focused startups benefit from lean R&D processes, faster deployment cycles, and a culture of rapid prototyping. This agility enables them to react to emerging threats and regulatory changes more swiftly than conventional vendors (Imoh, & Enyejo, 2025). For instance, startups leveraging reinforcement learning and graph neural networks are redefining anomaly detection by modeling evolving attack patterns and network topology shifts (Lee et al., 2013). Moreover, the proliferation of Internet of Things (IoT) devices across critical infrastructure has created new markets for privacy-preserving AI innovations, including secure multi-party computation and encrypted model training (Zubaydi, et al., 2023).

Entrepreneurial ecosystems, supported by accelerators, venture capital, and government-backed innovation hubs, now serve as critical incubators for next-generation cybersecurity tools (Idoko, et al., 2024). These environments enable the translation of advanced academic research into deployable AI solutions that proactively protect national critical infrastructure in an era of escalating digital risk.

1.5 Objectives and Scope of the Review

This review aims to investigate how entrepreneurial innovations are transforming AI-based anomaly detection within Software-Defined Networking (SDN) environments to enhance the cybersecurity of critical infrastructure systems. The core objectives are to analyze the technical integration of AI in SDN anomaly detection, assess the contributions of emerging startups in this space, and evaluate their role in addressing evolving cyber threats through scalable, adaptive solutions. The scope encompasses both foundational and applied perspectives, including the architecture of SDN, types of AI models employed, and sector-specific implementations across energy, healthcare, and transportation. The review also considers the commercial viability, deployment challenges, and policy implications of these entrepreneurial technologies. By synthesizing insights from high-impact literature and real-world case studies, the paper seeks to offer a comprehensive understanding of how AI-driven startups are reshaping the cybersecurity landscape for critical infrastructure protection.

1.6 Structure of the Paper

The paper is structured into six main sections to systematically explore the topic. It begins with an introduction that establishes the context, defines key terms, and outlines the significance of anomaly detection in SDN for critical infrastructure. The second section reviews the technical fundamentals of AI and SDN integration, followed by a third section that explores entrepreneurial trends and innovative startups in the field. The fourth section delves into practical applications across various infrastructure domains. The fifth section discusses existing challenges, limitations, and future research directions. The final section concludes with a synthesis of key findings and implications for stakeholders.

2. FUNDAMENTALS OF AI AND SDN FOR ANOMALY DETECTION

2.1 Overview of SDN Architecture and Components

SDN redefines traditional networking by decoupling the control plane from the data plane, enabling centralized, programmable network management and facilitating dynamic policy enforcement. At its core, the SDN architecture comprises three key components: the application layer, where user-defined policies and network services reside; the control plane, represented by the SDN controller that translates policies into flow rules; and the infrastructure layer, consisting of forwarding devices such as switches and routers that execute instructions received from the controller (Nunes et al., 2014) as represented in figure 1. This separation allows network administrators to manage traffic flows programmatically and in real time, reducing operational complexity and increasing scalability (Enyejo, et al., 2024).

Communication between these layers is facilitated through standardized interfaces: the Northbound API enables communication between the control plane and application layer, while the Southbound API (most notably OpenFlow) connects the control plane to the data plane (Ononiwu, et al., 2023). SDN's logically centralized control architecture enhances network agility, policy abstraction, and rapid deployment of services, making it a promising platform for critical infrastructure networks (Feamster et al., 2014). However, this programmable flexibility also mandates enhanced security considerations, especially in contexts requiring fine-grained access control and integrity verification. As the architecture matures, SDN is increasingly being integrated with AI to enable intelligent traffic management, anomaly detection, and automated threat mitigation in dynamic network environments.

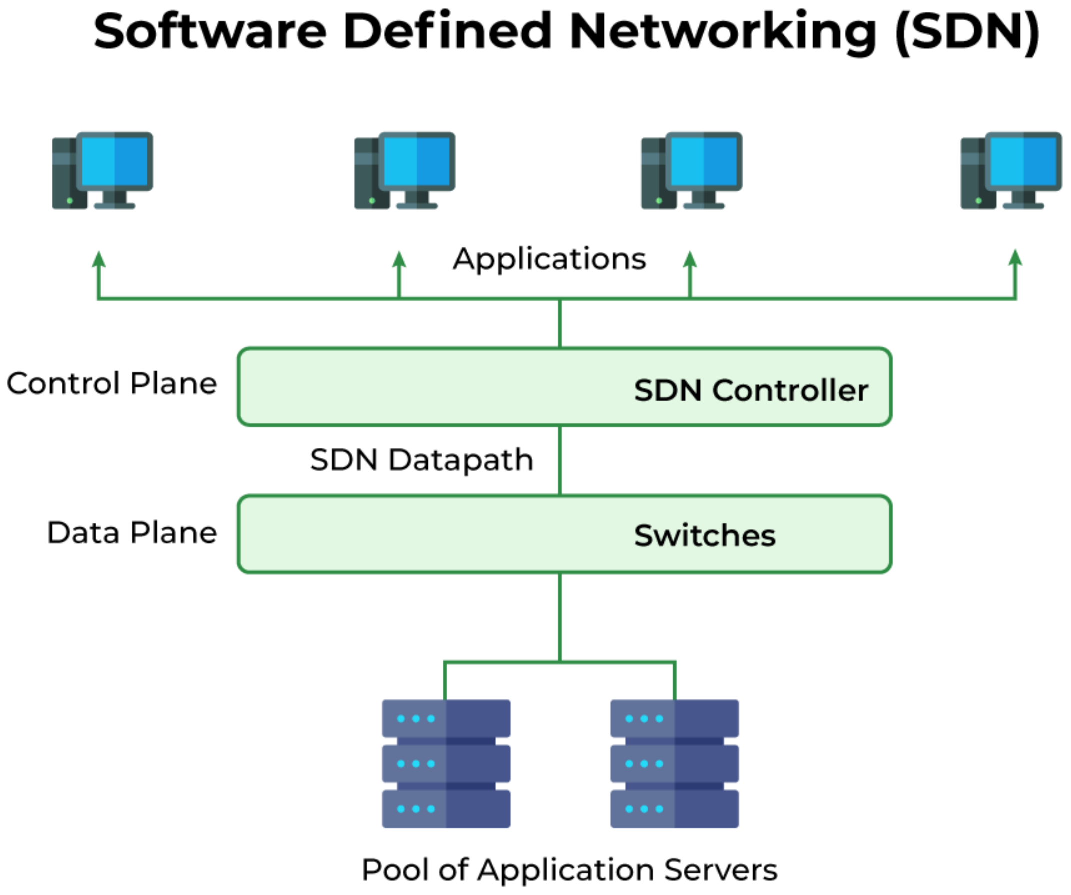

Figure 1: Picture of Layered Architecture of Software Defined Networking (SDN) Illustrating Control and Data Plane Separation (geeksforgeeks, 2025).

Figure 1 titled *"Software Defined Networking (SDN)"* illustrates the layered architecture and core components of an SDN environment, providing a clear representation of how control and data planes are decoupled to enhance network programmability and flexibility. At the *top layer*, a series of computing devices represent applications, which interact with the *control plane* via northbound APIs to define traffic policies and routing logic. The *control plane* is centrally managed by an *SDN Controller*, which serves as the network's brain—translating high-level application requirements into low-level forwarding rules. These rules are communicated to the *data plane*, which comprises *Switches* responsible for actual packet forwarding across the network based on the SDN datapath. Below the data plane lies a *pool of application servers*, which receive, process, and respond to traffic as directed by the flow rules managed by the controller. This architecture enables real-time traffic management, dynamic resource allocation, and centralized policy enforcement across distributed environments. It also allows for intelligent monitoring and anomaly detection when integrated with AI-based security tools. By abstracting the control logic from the hardware and consolidating it in the SDN controller, administrators can manage the entire network programmatically, leading to more agile, scalable, and secure networking infrastructures.

2.2 AI Techniques Used in Anomaly Detection (ML, DL, XAI)

Artificial Intelligence (AI) has revolutionized anomaly detection in cybersecurity, particularly within programmable frameworks such as SDN. Machine Learning (ML) techniques, including decision trees, k-means clustering, support vector machines (SVM), and random forests, are widely adopted to model normal network behaviors and detect deviations that suggest potential intrusions (Buczak & Guven, 2016). These algorithms excel in handling structured network data and identifying outliers in large-scale traffic logs. Deep Learning (DL) approaches—such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) models—are increasingly favored for capturing complex temporal patterns and multi-dimensional correlations in dynamic traffic environments.

As SDNs continue to generate high-volume, heterogeneous data streams, the need for transparent and trustworthy decision-making has given rise to Explainable AI (XAI). XAI frameworks aim to demystify model predictions, offering interpretability tools such as SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-Agnostic Explanations), and attention-based mechanisms that help network operators understand the rationale behind flagged anomalies (Ghosh & Saha, 2021). This transparency is critical for reducing false positives and building operator confidence in automated detection systems (Ijiga, A. C., 2024). Together, ML, DL, and XAI provide a multi-layered defense model capable of learning evolving attack vectors, adapting to new network topologies, and aligning with real-world operational requirements in critical infrastructure security.

2.3 Challenges of Securing SDN Environments

While Software-Defined Networking (SDN) offers operational efficiency and programmability, it simultaneously introduces novel security vulnerabilities that challenge its deployment in critical infrastructure. Central to these risks is the centralization of control, which creates a single point of failure. If compromised, the controller could grant adversaries unfettered access to network-wide traffic flows and configurations. Additionally, the communication channel between the controller and switches—primarily via OpenFlow—lacks robust default encryption or authentication mechanisms, rendering it susceptible to man-in-the-middle attacks, spoofing, and flow rule manipulation (Klöti et al., 2013) as shown in table 1.

Moreover, SDN's dynamic nature invites policy inconsistencies, especially in multi-tenant or federated architectures where conflicting rule sets can be injected. The modularity of SDN also presents an expanded attack surface, including APIs, northbound applications, and third-party software libraries that may harbor exploitable bugs (Scott-Hayward et al., 2016). Another critical challenge lies in maintaining real-time visibility and trust across distributed SDN domains, particularly when integrating with legacy systems that lack native SDN support.

Effective security for SDNs requires a shift from static rule enforcement to context-aware, behavior-driven models, often powered by AI. However, deploying such models at scale introduces its own set of challenges, including data scarcity, model drift, and adversarial manipulation (Ononiwu, et al., 2024). Thus, securing SDN environments demands a holistic, multi-layered approach that integrates robust protocols, AI-enhanced analytics, and continuous monitoring mechanisms.

Table 1: Summary of Challenges of Securing SDN Environments

Challenge	Description	Implication	Example/Detail
Centralized Control Vulnerabilities	Single point of failure in SDN controller can lead to system-wide compromise	Increases risk of full-network attacks	Attackers gaining control over flow rules can reroute or disrupt network traffic
Weak Communication Protocols	Insufficient default security in protocols like OpenFlow	Prone to spoofing and man-in-the-middle attacks	Lack of authentication enables command injection into SDN switches
API and Application Layer Risks	Northbound APIs and third-party apps expand the attack surface	Facilitates unauthorized access or code injection	Compromised apps may modify flow tables or leak sensitive network data
Legacy System Interoperability	Difficulty integrating SDN with non-programmable legacy infrastructure	Operational disruptions and inconsistent policy enforcement	Hybrid environments may suffer from partial visibility and policy drift

3. ENTREPRENEURIAL TRENDS AND STARTUPS IN AI-POWERED SDN SECURITY

3.1 Case Studies of Cybersecurity Startups

Cybersecurity startups have emerged as critical players in redefining how anomaly detection and threat mitigation are applied in SDN-powered environments. These companies often possess dynamic capabilities that allow them to iterate rapidly, integrate novel technologies, and pivot in response to evolving threats—traits that are less prevalent in established incumbents (Teece, 2018). A leading example is Darktrace, a startup leveraging unsupervised machine learning and neural network models to detect network anomalies across hybrid environments, including SDN deployments (Ononiwu, et al., 2023). Their AI-based "Enterprise Immune System" adapts to new traffic patterns and responds to threats in real time without requiring predefined signatures.

Another example is Vectra AI, which combines behavioral analytics and real-time monitoring to detect threats in east-west traffic within SDN environments. By focusing on context-aware analysis and leveraging machine learning pipelines, Vectra AI enables early detection of lateral movements, account takeovers, and command-and-control communications (Ononiwu, et al., 2025). Such innovation stems not just from technical agility, but from policy environments that support startup activity. Peripheral innovation agencies in countries like Israel and Finland have historically supported radical innovation through flexible regulation and targeted R&D funding (Breznitz & Ornston, 2013).

These startups exemplify how entrepreneurial ventures serve as incubators for AI-enhanced, SDN-compatible cybersecurity solutions—demonstrating scalability, adaptability, and commercial readiness for securing critical infrastructure systems.

3.2 Investment Trends and Venture Capital in AI-SDN Security

The surge in venture capital (VC) investment toward AI-based cybersecurity startups operating in Software-Defined Networking (SDN) environments reflects a broader shift in strategic funding priorities. Investors are increasingly drawn to companies that develop machine learning algorithms for network security, anomaly detection, and policy automation—particularly those with scalable architectures suited for critical infrastructure sectors (Ononiwu, et al., 2023). These startups present high growth potential due to the convergence of AI and programmable networks, which offers a robust market for innovative threat mitigation tools (Hegeman, & Sørheim, 2021).

Private and institutional investors prioritize ventures that combine intellectual property, market applicability, and regulatory readiness. For example, companies like SentinelOne and Cybereason have attracted hundreds of millions in funding due to their AI-enhanced endpoint detection systems and real-time threat analytics engines, both applicable to SDN-based enterprise architectures (James, et al., 2024). Venture capitalists also value startups that integrate explainable AI and edge-based inference models into their SDN solutions, enabling secure deployment in latency-sensitive environments like smart grids or healthcare.

Governmental VC initiatives further stimulate this trend by reducing early-stage investment risk and catalyzing technology transfer from academia to market (James, et al., 2023). In countries like Italy, such investments have significantly improved startup survivability and innovation output, especially in sectors deemed strategically vital (Cumming, et al., 2017). Overall, VC momentum is driving deep integration of AI in SDN security applications.

3.3 Innovation Hubs and Accelerators Focusing on Network Security

Innovation hubs and startup accelerators have become instrumental in advancing cybersecurity solutions tailored for Software-Defined Networking (SDN) environments. These ecosystems provide startups with technical mentorship, early-stage funding, and access to enterprise partnerships that accelerate the development of AI-powered anomaly detection tools (Ijiga, O. M., et al., 2025). Many of these hubs specialize in high-risk, high-reward domains such as programmable networks and critical infrastructure protection. For instance, programs like CyberXcelerator and Mach37 focus exclusively on security-centric startups, equipping them with the tools to integrate AI capabilities into network orchestration platforms (Prohorovs & Bistrova, 2021) as shown in figure 2.

Accelerators not only offer access to funding but also serve as experimental grounds where SDN-specific use cases—such as dynamic policy reconfiguration, flow-level monitoring, and autonomous mitigation—are tested in sandboxed environments (Imoh, et al., 2024). Their structured curricula often include sessions on explainable AI, regulatory compliance (e.g., GDPR, NIST), and zero-trust architecture, ensuring that startups are aligned with both market and policy expectations (Clarisse, et al., 2015).

Moreover, proximity to academic institutions and enterprise partners creates a collaborative pipeline for transferring cutting-edge research into deployable solutions. As a result, accelerators have evolved from mere funding vehicles into full-fledged innovation orchestrators (Ijiga, O. M., et al., 2023). Their role is pivotal in scaling AI-SDN startups that can address increasingly complex cybersecurity challenges in energy, healthcare, and industrial systems.

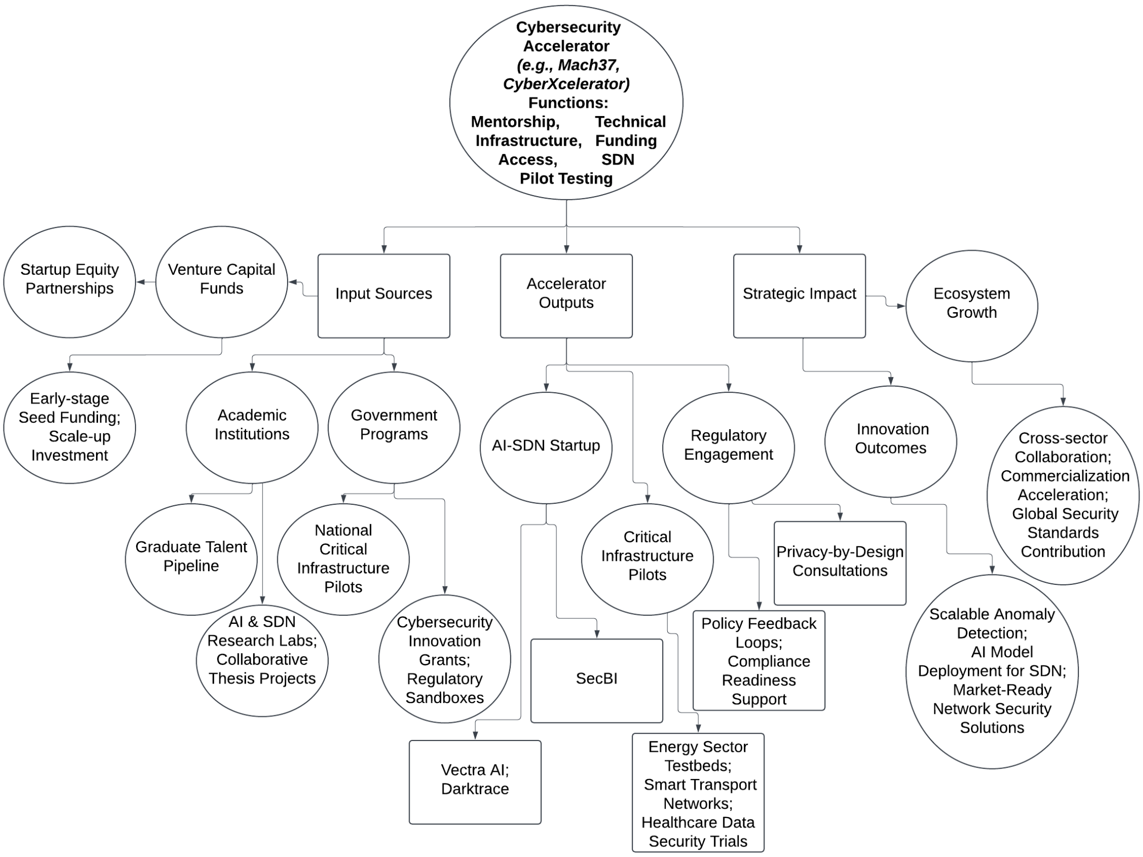
Cybersecurity Accelerator (e.g., Mach37, CyberXcelerator) Functions: Mentorship, Technical Infrastructure, Funding Access, SDN Pilot Testing
Input Sources
Accelerator Outputs
Strategic Impact
Startup Equity Partnerships
Venture Capital Funds
Ecosystem Growth
Early-stage Seed Funding; Scale-up Investment
Academic Institutions
Government Programs
AI-SDN Startup
Regulatory Engagement
Innovation Outcomes
Cross-sector Collaboration; Commercialization Acceleration; Global Security Standards Contribution
Graduate Talent Pipeline
National Critical Infrastructure Pilots
Critical Infrastructure Pilots
Privacy-by-Design Consultations
AI & SDN Research Labs; Collaborative Thesis Projects
Cybersecurity Innovation Grants; Regulatory Sandboxes
SecBI
Policy Feedback Loops; Compliance Readiness Support
Scalable Anomaly Detection; AI Model Deployment for SDN; Market-Ready Network Security Solutions
Vectra AI; Darktrace
Energy Sector Testbeds; Smart Transport Networks; Healthcare Data Security Trials

Figure 2: Diagram Illustration of a Structured Innovation Framework Demonstrating the Role of Cybersecurity Accelerators in Advancing AI-SDN Network Security.

Figure 2 demonstrates the central role of cybersecurity accelerators in fostering innovation for AI-based anomaly detection in Software-Defined Networking (SDN) environments. At the core is the Cybersecurity Accelerator, which provides startups with critical support through mentorship, technical infrastructure, funding access, and real-world SDN pilot testing. The accelerator draws inputs from three main sources: academic institutions, which contribute cutting-edge research, skilled talent, and collaborative projects; venture capital funds, which provide financial investment and strategic guidance; and government programs, which offer innovation grants, regulatory flexibility, and pilot programs in national infrastructure. These inputs enable the accelerator to produce tangible outputs including AI-SDN cybersecurity startups (e.g., Vectra AI, Darktrace), critical infrastructure pilots in sectors such as energy, transportation, and healthcare, and regulatory engagement to ensure compliance and feedback integration. Extending from the accelerator's outputs, the third branch highlights its strategic impact, including scalable and market-ready security innovations, broader ecosystem growth through cross-sector collaboration, and contributions to the development of global network security standards. This structured innovation framework supports a holistic model of cybersecurity advancement that blends entrepreneurship, policy, and research.

4. APPLICATIONS IN CRITICAL INFRASTRUCTURE PROTECTION

4.1 Use Cases in Energy Grids, Smart Transportation, Healthcare, etc.

AI-powered anomaly detection in SDN environments is revolutionizing how critical sectors—such as energy, transportation, and healthcare—monitor and respond to cyber threats. In smart grids, SDN enables dynamic control of energy distribution while integrating renewable sources and real-time pricing systems. AI-enhanced anomaly detection systems in this context provide predictive fault identification, unauthorized access prevention, and real-time event classification to mitigate cascading failures and blackouts (Gungor et al., 2013) as shown in figure 3.

In smart transportation systems, SDN supports vehicular ad hoc networks (VANETs), traffic signal coordination, and fleet management. AI models detect anomalous vehicle-to-infrastructure (V2I) communications, spoofed sensor signals, and malicious rerouting instructions that could compromise public safety or traffic flow (Ijiga, O. M., et al., 2022). AI-SDN integration facilitates adaptive routing and network load balancing, thereby ensuring reliable communication in highly mobile and latency-sensitive environments (Zanella et al., 2014).

Healthcare systems benefit from AI-driven SDN solutions through secure handling of sensitive patient data and real-time monitoring of interconnected medical devices. These systems detect unauthorized access to electronic health records (EHRs), unusual network flows in connected ICU devices, and potential ransomware activities (Ijiga, O. M., et al., 2021). The dynamic programmability of SDN coupled with contextual learning models enables sector-specific protection. Across all use cases, AI-SDN architectures serve as critical infrastructures' nervous system—enabling adaptability, resilience, and intelligence under high operational stakes.

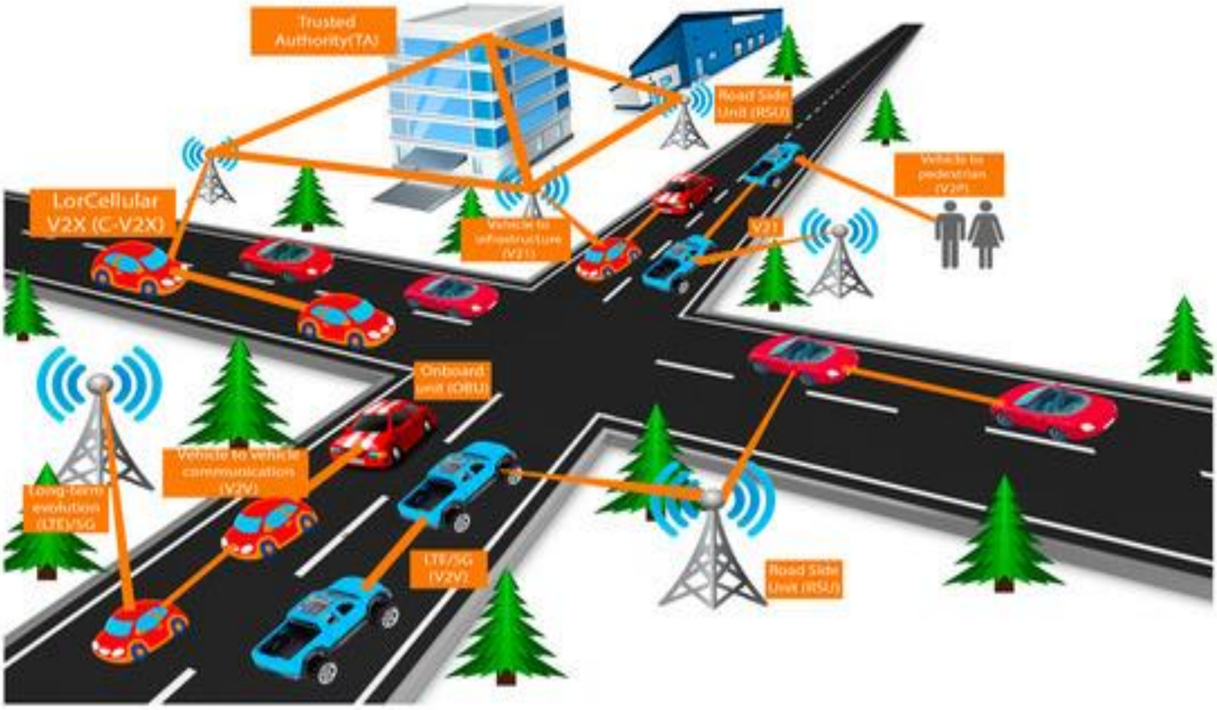
Trusted Authority(TA)
Road Side Unit (RSU)
LorCellular V2X (C-V2X)
Vehicle to pedestrian (V2P)
Vehicle to infrastructure (V2I)
V2I
Onboard unit (OBU)
Vehicle to vehicle communication (V2V)
Long-term evolution (LTE)/5G
LTE/5G (V2V)
Road Side Unit (RSU)

Figure 3: Picture of Intelligent V2X Communication Ecosystem for Smart Transportation Security and Coordination (Polat, O. et al., 2024).

Figure 3 provides a visual representation of smart transportation infrastructure enabled by vehicle-to-everything (V2X) communication, a key use case in the integration of AI-driven anomaly detection within Software-Defined Networking (SDN) environments. Vehicles in the illustration communicate with each other (V2V), with pedestrians (V2P), with infrastructure (V2I), and with centralized entities such as a Trusted Authority (TA) via Long-Term Evolution (LTE)/5G networks. Road Side Units (RSUs) and Onboard Units (OBUs) facilitate secure, low-latency communication, allowing dynamic exchange of traffic, safety, and routing data. This multi-layered communication supports intelligent decision-making in real time, such as collision avoidance, traffic congestion prediction, and pedestrian safety alerts. SDN plays a critical role in managing these data flows by separating the control logic from physical devices, enabling centralized orchestration, dynamic policy enforcement, and traffic optimization across connected vehicles and infrastructure. AI-based anomaly detection systems embedded within this architecture can identify malicious data injection, spoofed identities, or erratic traffic patterns that could signal cyber-physical attacks or system failures. This concept extends similarly to other critical sectors, such as energy grids and healthcare, where SDN-enabled AI frameworks ensure reliability, real-time responsiveness, and predictive security across distributed, mission-critical systems. The illustration exemplifies how intelligent transportation networks serve as a foundational use case for advancing AI-SDN applications in smart infrastructure management.

4.2 Real-Time Detection and Response Systems

Real-time detection and response systems are vital to safeguarding Software-Defined Networking (SDN) environments used in critical infrastructure operations. These systems utilize AI algorithms to monitor network traffic continuously, identify deviations from baseline behavior, and initiate autonomous mitigation actions—all within milliseconds (Ijiga, O. M., et al., 2021). Machine learning models such as decision trees, ensemble classifiers, and neural networks are trained to identify subtle changes in packet flow, latency spikes, or routing inconsistencies indicative of threats (Sommer & Paxson, 2010) as presented in table 2. Deep learning approaches, particularly convolutional neural networks (CNNs) and LSTMs, have shown high efficacy in extracting spatiotemporal features from large volumes of data, enabling fast and accurate classification of unknown attacks. These models are particularly beneficial in high-throughput environments where manual rule-writing and static intrusion detection systems are insufficient. In SDN, once a threat is detected, the centralized controller can dynamically update flow rules to reroute, isolate, or drop malicious traffic, preventing lateral spread (Ofoegbu, et al., 2024).

Furthermore, integrating explainable AI within these systems offers operational transparency, ensuring that responses are auditable and interpretable. This combination of real-time AI detection and programmable network response transforms SDN into an intelligent, self-defending infrastructure (Ijiga, O. M., et al., 2025). It significantly reduces response time and minimizes human intervention, thus improving security postures in mission-critical domains like defense, utilities, and finance.

Table 2: Summary of Real-Time Detection and Response Systems

Feature	Function	Benefit	Example/Detail
Continuous Monitoring	Real-time traffic inspection and behavioral analysis	Enables early anomaly detection and attack classification	AI models flag traffic anomalies within milliseconds
AI-Driven Decision Engines	Utilizes ML/DL for threat prediction and pattern recognition	Reduces false positives and automates mitigation	LSTM models detect lateral movement and initiate isolation of affected nodes
Programmable SDN Control	Dynamic reconfiguration of flows based on threat status	Immediate containment and reduced downtime	SDN controller updates flow tables to reroute or block malicious traffic
Explainable AI (XAI) Integration	Enhances interpretability of detection decisions	Builds trust and accountability in automated responses	SHAP values used to explain anomaly triggers in encrypted traffic streams

4.3 Integration with Legacy Systems and Industrial Control Systems (ICS)

Integrating AI-enhanced Software-Defined Networking (SDN) into legacy systems and Industrial Control Systems (ICS) presents both a critical opportunity and a complex challenge. Legacy infrastructure in sectors such as power generation, manufacturing, and water treatment often relies on proprietary protocols, outdated hardware, and minimal native security measures (Ijiga, A. C., et al., 2024). These systems were designed for availability, not resilience against advanced cyber threats. Consequently, retrofitting AI-SDN frameworks into such environments must address compatibility, latency, and operational continuity (Humayed et al., 2017).

SDN acts as an overlay that can abstract legacy network behaviors, introducing programmable control without physically altering existing devices. AI-based anomaly detection models can learn traffic patterns from legacy protocols like Modbus or DNP3, providing passive monitoring and predictive threat analysis (Ijiga, A. C., et al., 2024). These models help uncover stealthy attacks such as false data injection, command spoofing, or malicious reprogramming attempts.

Despite the advantages, ICS operators often face significant barriers, including fear of downtime, regulatory limitations, and interoperability issues (Idika, et al., 2023). Security management in ICS environments must therefore be phased, beginning with non-intrusive deployments and progressing toward hybrid architectures that combine SDN flexibility with the deterministic performance of ICS components (Knowles et al., 2015). Over time, AI-SDN integration enhances visibility, automates incident response, and enforces granular access controls—without compromising the operational mandates of legacy infrastructure.

5. CHALLENGES AND FUTURE DIRECTIONS

5.1 Scalability and Deployment Barriers for Startups

Despite their agility and innovation capacity, cybersecurity startups operating in AI-SDN domains face considerable challenges when attempting to scale their technologies across critical infrastructure environments. One major limitation is the resource-intensive nature of deploying and maintaining AI-driven anomaly detection systems, which often require customized integration with existing enterprise networks (Igba, et al., 2024). Startups typically lack the cloud infrastructure, engineering scale, and system redundancy needed for broad, real-time deployment across multiple sectors or geographies (Cusumano et al., 2019) as represented in figure 4.

In addition, startups encounter difficulty in achieving trust from risk-averse industries such as energy, healthcare, and transportation. These sectors demand high assurance, robust compliance, and long-term support—commitments that early-stage ventures may struggle to guarantee. Furthermore, the modularity of SDN introduces heterogeneity in implementation, meaning that solutions must be adaptable to diverse controllers, protocols, and flow configurations (Idika, et al., 2024).

Startups also face competitive bottlenecks in ecosystems dominated by platform leaders, who control data access and integration pipelines, effectively shaping market entry thresholds (Zahra & Nambisan, 2012). Building strategic partnerships with integrators, infrastructure providers, and regulators is essential to bypass deployment friction. Without such alliances, even the most promising AI-SDN security innovations risk obsolescence before achieving operational maturity (Azonuche, & Enyejo, 2024). Thus, addressing scalability issues demands not just technical robustness but also strategic ecosystem navigation and platform interoperability.

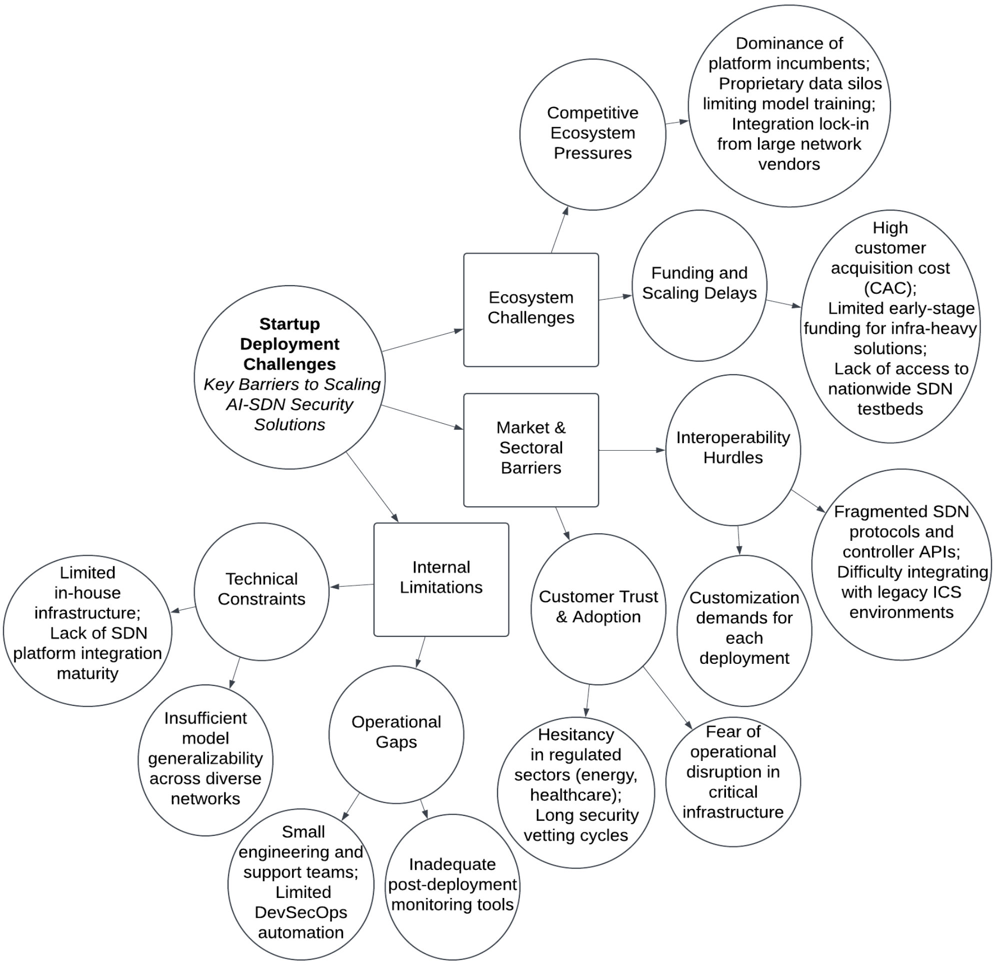
Startup Deployment Challenges
Key Barriers to Scaling AI-SDN Security Solutions
Ecosystem Challenges
Competitive Ecosystem Pressures
Dominance of platform incumbents; Proprietary data silos limiting model training; Integration lock-in from large network vendors
Funding and Scaling Delays
High customer acquisition cost (CAC); Limited early-stage funding for infra-heavy solutions; Lack of access to nationwide SDN testbeds
Market & Sectoral Barriers
Interoperability Hurdles
Fragmented SDN protocols and controller APIs; Difficulty integrating with legacy ICS environments
Customization demands for each deployment
Customer Trust & Adoption
Hesitancy in regulated sectors (energy, healthcare); Long security vetting cycles
Fear of operational disruption in critical infrastructure
Internal Limitations
Technical Constraints
Limited in-house infrastructure; Lack of SDN platform integration maturity
Insufficient model generalizability across diverse networks
Operational Gaps
Small engineering and support teams; Limited DevSecOps automation
Inadequate post-deployment monitoring tools

Figure 4: Diagram Illustration of Categorized Scalability and Deployment Barriers for AI-SDN Cybersecurity Startups.

Figure 4 outlines the multifaceted scalability and deployment barriers faced by AI-SDN cybersecurity startups, organized into three major categories: internal limitations, market and sectoral barriers, and broader ecosystem challenges. Internally, startups often lack the technical infrastructure, platform integration maturity, and human capital needed to develop, deploy, and support complex security solutions at scale. Operational gaps such as minimal DevSecOps automation and limited real-time monitoring tools exacerbate post-deployment inefficiencies. Externally, sector-specific adoption barriers prevail, especially in critical industries like healthcare and energy, where stakeholders exhibit high resistance due to strict regulatory compliance requirements, perceived risks of system downtime, and prolonged vetting processes. Furthermore, integration challenges arise from fragmented SDN controller protocols and legacy system dependencies. From an ecosystem perspective, startups compete with large incumbents who leverage proprietary ecosystems and data silos to entrench their market dominance. Limited funding opportunities and lack of access to national-scale SDN testbeds further constrain startups' ability to test, scale, and refine their offerings. This interconnected web of challenges reveals that scaling AI-based cybersecurity within SDN infrastructures demands not only technical innovation but also strategic navigation of regulatory, operational, and market constraints.

5.2 Regulatory and Ethical Considerations

The deployment of AI-based anomaly detection in Software-Defined Networking (SDN) for critical infrastructure introduces a range of regulatory and ethical complexities. AI systems—particularly those using opaque models—raise concerns over algorithmic accountability, data privacy, and decision-making transparency (Ayoola, et al., 2024). These concerns are exacerbated in sectors like energy and healthcare, where decisions made by AI can have immediate and far-reaching societal impacts. As Taddeo and Floridi (2018) argue, ethical AI design must go beyond technical performance and prioritize fairness, explainability, and alignment with societal values.

Regulatory frameworks have yet to fully adapt to AI-SDN convergence, especially regarding data residency, cross-border threat intelligence sharing, and automated response policies. Fragmented legal standards across jurisdictions further complicate compliance for startups seeking multinational deployments (Azonuche, & Enyejo, 2024). Additionally, real-time data processing for anomaly detection often requires deep packet inspection and behavioral profiling—techniques that may conflict with personal data protection laws such as the GDPR or HIPAA.

Moreover, Zuboff (2019) warns of the emergence of "surveillance capitalism," in which user data is commodified without adequate consent or oversight. This risk is particularly acute in AI-driven cybersecurity systems that operate with minimal human intervention (Atalor, et al., 2023). To mitigate such ethical risks, regulatory sandboxes, transparent AI guidelines, and cross-sector collaboration must be embedded into the design, training, and deployment lifecycle of SDN-integrated AI solutions.

5.3 Future Research Directions (e.g., Federated Learning, Adversarial Robustness)

Advancing the robustness and adaptability of AI-enhanced anomaly detection in Software-Defined Networking (SDN) environments requires intensified research in several key domains. One promising direction is federated learning, which enables the training of AI models across distributed datasets without requiring direct data sharing (Atalor, et al., 2023). This approach is particularly relevant for critical infrastructure, where privacy-preserving data strategies are essential for compliance and trust. Federated learning can enhance anomaly detection by leveraging cross-domain insights while protecting organizational data boundaries (Yang et al., 2019) as presented in table 3.

Another critical research frontier involves enhancing adversarial robustness in machine learning models. AI systems used in cybersecurity are themselves susceptible to adversarial attacks, wherein subtle manipulations of input data can mislead detection algorithms (Ajayi, et al., 2024). In SDN contexts, such vulnerabilities could be exploited to evade intrusion detection or trigger false positives that degrade system performance. Research must focus on developing resilient model architectures, such as robust training with adversarial examples, certified defenses, and ensemble methods capable of maintaining performance under attack (Biggio & Roli, 2018).

Further investigation is also needed in hybrid AI models that combine symbolic reasoning with neural architectures to boost explainability without compromising detection efficacy (Aikins, et al., 2024). Incorporating these advancements into AI-SDN systems will enable more secure, transparent, and adaptive frameworks suitable for the dynamic threat landscape confronting modern critical infrastructure.

Table 3: Summary of Future Research Directions in AI-SDN Security

Research Area	Focus	Benefit	Example/Detail
Federated Learning	Distributed model training without centralized data collection	Preserves privacy and supports cross-organizational collaboration	Utility sectors training intrusion models without data-sharing agreements
Adversarial Robustness	Defending models against manipulated inputs	Increases resilience of detection systems against evasion tactics	Use of adversarial examples during training to improve robustness of classifiers
Hybrid AI Architectures	Combining symbolic reasoning with neural models	Balances accuracy with interpretability	Integrating rule-based logic with deep networks for precise flow classification
Explainable Threat Detection	Enhancing transparency of AI decisions in anomaly detection	Improves auditability and compliance adherence	Use of LIME to validate AI decisions during forensic investigations

6. CONCLUSION

6.1 Summary of Key Findings

This review has demonstrated that the convergence of artificial intelligence (AI) and software-defined networking (SDN) within critical infrastructure protection is both a technical necessity and a fertile ground for entrepreneurial innovation. Key findings highlight that SDN, through its decoupled architecture and centralized control, introduces programmable flexibility that can be leveraged for real-time anomaly detection, but also amplifies the attack surface if not secured adequately. The integration of AI techniques—such as machine learning, deep learning, and explainable AI—provides powerful tools for detecting anomalous behaviors, predicting threats, and automating response actions. These techniques have proven especially effective in managing large-scale, high-velocity data flows common to energy grids, smart transportation, and healthcare systems.

The study further revealed that startups are playing an increasingly pivotal role in pushing the boundaries of AI-SDN security by deploying modular, scalable solutions often overlooked by larger, legacy vendors. However, despite their technical prowess, these ventures encounter significant deployment and scaling challenges—ranging from interoperability issues with legacy systems to infrastructural limitations and customer trust barriers. Real-time AI-based detection systems have shown promise in enhancing response times and reducing false positives, but concerns persist around explainability, regulatory compliance, and adversarial robustness.

Moreover, innovation hubs and accelerators serve as catalysts in maturing these technologies and business models. Taken together, the findings underscore a dynamic, rapidly evolving landscape where entrepreneurial ventures are driving security innovations in SDN environments, albeit within a complex regulatory and infrastructural ecosystem.

6.2 Strategic Importance of Entrepreneurship in Cybersecurity Innovation

Entrepreneurship is emerging as a strategic linchpin in advancing cybersecurity innovation, particularly within the domain of AI-powered anomaly detection in software-defined networking (SDN) systems. Unlike traditional technology providers, startups bring a unique combination of speed, specialization, and risk tolerance—enabling them to develop and iterate cutting-edge security solutions that address both existing and emerging threats in critical infrastructure. These ventures often capitalize on niche technological capabilities such as federated learning for decentralized model training, graph-based AI for network path analysis, or adversarial defense algorithms to detect stealthy intrusions. By offering lightweight, modular applications that integrate seamlessly into SDN environments, entrepreneurial firms can deliver highly adaptive and scalable solutions at a fraction of the cost and time associated with conventional security vendors.

Additionally, startups frequently operate within innovation ecosystems supported by accelerators, incubators, and venture capital networks that provide critical early-stage resources—including funding, mentorship, and access to pilot environments. These ecosystems facilitate experimentation with advanced AI models in real-world network contexts, allowing for iterative refinement before wide-scale deployment. Furthermore, entrepreneurship introduces competitive pressure into the cybersecurity market, compelling established firms to invest in R&D and adopt more flexible, customer-centric approaches.

Importantly, entrepreneurial initiatives often serve as the first movers in regulatory adaptation, proactively embedding data privacy features, auditability mechanisms, and ethical AI principles. This strategic adaptability positions them as key actors in shaping the next generation of cybersecurity standards, policies, and practices essential for protecting digitally interconnected infrastructure.

6.3 Call to Action for Industry–Government–Academia Collaboration

To fully realize the transformative potential of AI-enhanced anomaly detection in SDN environments, a coordinated and sustained collaboration among industry, government, and academia is imperative. The complexity of securing critical infrastructure demands not only technological innovation but also harmonized frameworks that address operational, regulatory, and societal concerns. Industry stakeholders—particularly startups and established cybersecurity providers—must align their development roadmaps with real-world threat scenarios and infrastructure needs. This requires direct partnerships with utilities, healthcare institutions, and transportation agencies to pilot, test, and refine AI-SDN solutions under operational constraints.

Governments, on the other hand, must take a proactive role in enabling this innovation through regulatory sandboxes, funding mechanisms, and policy frameworks that encourage experimentation without compromising public safety or data integrity. Establishing national and regional cybersecurity testbeds can serve as neutral grounds for evaluating emerging solutions across sectors. Additionally, public procurement programs can be tailored to favor innovative, high-assurance startups capable of delivering robust cybersecurity outcomes.

Academic institutions must bridge theoretical advancements with applied research, focusing on challenges such as model explainability, adversarial robustness, secure multi-party computation, and ethical AI design. Through joint research labs, co-authored publications, and interdisciplinary curricula, academia can prepare the next generation of cybersecurity professionals equipped to tackle the evolving threat landscape.

This tripartite collaboration must operate not in silos but as a dynamic innovation coalition—committed to securing critical digital ecosystems, scaling cutting-edge solutions, and setting global benchmarks for AI-enabled network security governance.

REFERENCES

[1] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

[2] Aikins, S. A., Avevor, J. & Enyejo, L. A. (2024). Optimizing Thermal Management in Hydrogen Fuel Cells for Smart HVAC Systems and Sustainable Building Energy Solutions. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 3, Issue 4, 2024 DOI: https://doi.org/10.38124/ijsrmt.v3i4.351

[3] Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum Cryptography and Blockchain-Based Social Media Platforms as a Dual Approach to Securing Financial Transactions in CBDCs and Combating Misinformation in U.S. Elections. International Journal of Innovative Science and Research Technology. Volume 9, Issue 10, Oct.– 2024 ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1697.

[4] Atalor, S. I., Ijiga, O. M., & Enyejo, J. O. (2023). Harnessing Quantum Molecular Simulation for Accelerated Cancer Drug Screening. *International Journal of Scientific Research and Modern Technology*, *2*(1), 1–18. https://doi.org/ 10.38124/ijsrmt.v2i1.502

[5] Atalor, S. I., Raphael, F. O. & Enyejo, J. O. (2023). Wearable Biosensor Integration for Remote Chemotherapy Monitoring in Decentralized Cancer Care Models. *International Journal of Scientific Research in Science and Technology* Volume 10, Issue 3 (www.ijsrst.com) doi : https://doi.org/10.32628/IJSRST23113269

[6] Ayoola, V. B., Ugoaghalam, U. J., Idoko P. I, Ijiga, O. M & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances,* 2024, 20(03), 094–117. https://gjeta.com/content/effectiveness-social-engineering-awareness-training-mitigating-spear-phishing-risks

[7] Azonuche, T. I., & Enyejo, J. O. (2024). Agile Transformation in Public Sector IT Projects Using Lean-Agile Change Management and Enterprise Architecture Alignment. *International Journal of Scientific Research and Modern Technology*, *3*(8), 21–39. https://doi.org/10.38124/ijsrmt.v3i8.432

[8] Azonuche, T. I., & Enyejo, J. O. (2024). Exploring AI-Powered Sprint Planning Optimization Using Machine Learning for Dynamic Backlog Prioritization and Risk Mitigation. *International Journal of Scientific Research and Modern Technology*, *3*(8), 40–57. https://doi.org/10.38124/ijsrmt.v3i8.448.

[9] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

[10] Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

[11] Breznitz, D., & Ornston, D. (2013). The revolutionary power of peripheral agencies: Explaining radical policy innovation in Finland and Israel. *Comparative Political Studies*, 46(10), 1219–1245. https://doi.org/10.1177/0010414012453442

[12] 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

[13] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

[14] Clarisse, B., Wright, M., & Van Hove, J. (2015). A look inside accelerators: Building business. *Recuperado de https://www. nesta. org. uk/sites/default/files/a_look_inside_accelerators. pdf*.

[15] Cumming, D. J., Grilli, L., & Murtinu, S. (2017). Governmental and independent venture capital investments in Europe: A firm-level performance analysis. *Journal of corporate finance*, *42*, 439-459.

[16] Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). The business of platforms: Strategy in the age of digital competition, innovation, and power. *Harvard Business Review Press*.

[17] Enyejo, J. O., Babalola, I. N. O., Owolabi, F. R. A. Adeyemi, A. F., Osam-Nunoo, G., & Ogwuche, A. O. (2024). Data-driven digital marketing and battery supply chain optimization in the battery powered aircraft industry through case studies of Rolls-Royce's ACCEL and Airbus's E-Fan X Projects. *International Journal of Scholarly Research and Reviews, 2024, 05(02), 001–020.* https://doi.org/10.56781/ijsrr.2024.5.2.0045

[18] Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: An intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review*, 44(2), 87–98. https://doi.org/10.1145/2602204.2602219

[19] Gans, J. S., & Stern, S. (2017). The product market and the market for "ideas": Commercialization strategies for technology entrepreneurs. *Research Policy*, 46(10), 1783–1799. https://doi.org/10.1016/j.respol.2017.08.008

[20] Geeksforgeeks, (2024). What is Software Defined Networking (SDN)? https://www.geeksforgeeks.org/computer-networks/software-defined-networking/

[21] Ghosh, S., & Saha, S. (2021). Explainable AI (XAI) for anomaly detection: A survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 11(1), e1394. https://doi.org/10.1002/widm.1394

[22] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). Smart grid technologies: Communication technologies and standards. *Journal of Industrial Informatics*, 9(1), 14–24. https://doi.org/10.1109/JII.2013.2238656

[23] Hegeman, P. D., & Sørheim, R. (2021). Why do they do it? Corporate venture capital investments in cleantech startups. *Journal of Cleaner Production*, *294*, 126315.

[24] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *Future Generation Computer Systems*, 74, 417–438. https://doi.org/10.1016/j.future.2016.10.029

[25] Idika, C. N., James, U. U., Ijiga, O. M., Okika, N. & Enyejo, L. A, (2024). Secure Routing Algorithms Integrating Zero Trust Edge Computing for Unmanned Aerial Vehicle Networks in Disaster Response Operations *International Journal of Scientific Research and Modern Technology, (IJSRMT)* Volume 3, Issue 6, https://doi.org/10.38124/ijsrmt.v3i6.635

[26] Idika, C. N., James, U.U, Ijiga, O. M., Enyejo, L. A. (2023). Digital Twin-Enabled Vulnerability Assessment with Zero Trust Policy Enforcement in Smart Manufacturing Cyber-Physical System *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* Volume 9, Issue 6 doi : https://doi.org/10.32628/IJSRCSEIT

[27] Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Akoh, O., & Ileanaju, S. (2024). Harmonizing the voices of AI: Exploring generative music models, voice cloning, and voice transfer for creative expression.

[28] Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Akoh, O., & Isenyo, G. (2024). Integrating superhumans and synthetic humans into the Internet of Things (IoT) and ubiquitous computing: Emerging AI applications and their relevance in the US context. **Global Journal of Engineering and Technology Advances**, 19(01), 006-036.

[29] Idoko, I. P., Ijiga, O. M., Agbo, D. O., Abutu, E. P., Ezebuka, C. I., & Umama, E. E. (2024). Comparative analysis of Internet of Things (IOT) implementation: A case study of Ghana and the USA-vision, architectural elements, and future directions. **World Journal of Advanced Engineering Technology and Sciences**, 11(1), 180-199.

[30] Igba, E., Danquah, E. O., Ukpoju, E. A., Obasa, J., Olola, T. M., & Enyejo, J. O. (2024). Use of Building Information Modeling (BIM) to Improve Construction Management in the USA. World Journal of Advanced Research and Reviews, 2024, 23(03), 1799–1813. https://wjarr.com/content/use-building-information-modeling-bim-improve-construction-management-usa

[31] Ijiga, A. C., Aboi, E. J., Idoko, P. I., Enyejo, L. A., & Odeyemi, M. O. (2024). Collaborative innovations in Artificial Intelligence (AI): Partnering with leading U.S. tech firms to combat human trafficking. *Global Journal of Engineering and Technology Advances, 2024,18(03), 106-123.* https://gjeta.com/sites/default/files/GJETA-2024-0046.pdf

[32] Ijiga, A. C., Enyejo, L. A., Odeyemi, M. O., Olatunde, T. I., Olajide, F. I & Daniel, D. O. (2024). Integrating community-based partnerships for enhanced health outcomes: A collaborative model with healthcare providers, clinics, and pharmacies across the USA. *Open Access Research Journal of Biology and Pharmacy,* 2024, 10(02), 081–104. https://oarjbp.com/content/integrating-community-based-partnerships-enhanced-health-outcomes-collaborative-model

[33] Ijiga, A. C., Igbede, M. A., Ukaegbu, C., Olatunde, T. I., Olajide, F. I. & Enyejo, L. A. (2024). Precision healthcare analytics: Integrating ML for automated image interpretation, disease detection, and prognosis prediction. *World Journal of Biology Pharmacy and Health Sciences,* 2024, 18(01), 336–354. https://wjbphs.com/sites/default/files/WJBPHS-2024-0214.pdf

[34] Ijiga, O. M., Balogun, S. A., Okika, N., Agbo, O. J. & Enyejo, L. A. (2025). An In-Depth Review of Blockchain-Integrated Logging Mechanisms for Ensuring Integrity and Auditability in Relational Database Transactions *International Journal of Social Science and Humanities Research* Vol. 13, Issue 3, DOI: https://doi.org/10.5281/zenodo.15834931

[35] Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journals.* Volume 13, Issue. https://doi.org/10.53022/oarjst.2024.11.1.0060I

[36] Ijiga, O. M., Ifenatuora, G. P., Olateju, M. (2021). Bridging STEM and Cross-Cultural Education: Designing Inclusive Pedagogies for Multilingual Classrooms in Sub Saharan Africa. JUL 2021 | *IRE Journals* | Volume 5 Issue 1 | ISSN: 2456-8880.

[37] Ijiga, O. M., Ifenatuora, G. P., Olateju, M. (2021). Digital Storytelling as a Tool for Enhancing STEM Engagement: A Multimedia Approach to Science Communication in K-12 Education. *International Journal of Multidisciplinary Research and Growth Evaluation.* Volume 2; Issue 5; September-October 2021; Page No. 495-505. https://doi.org/10.54660/.IJMRGE.2021.2.5.495-505

[38] Ijiga, O. M., Ifenatuora, G. P., Olateju, M. (2022). AI-Powered E-Learning Platforms for STEM Education: Evaluating Effectiveness in Low Bandwidth and Remote Learning Environments. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology I*SSN : 2456-3307 Volume 8, Issue 5 September-October-2022 Page Number : 455-475 doi : https://doi.org/10.32628/IJSRCSEIT

[39] Ijiga, O. M., Ifenatuora, G. P., Olateju, M. (2023). STEM-Driven Public Health Literacy : Using Data Visualization and Analytics to Improve Disease Awareness in Secondary Schools. *International Journal of Scientific Research in Science and Technology.* Volume 10, Issue 4 July-August-2023 Page Number : 773-793. https://doi.org/10.32628/IJSRST

[40] Ijiga, O. M., Okika, N., Balogun, S. A., Agbo, O. J. & Enyejo, L. A. (2025). Recent Advances in Privacy-Preserving Query Processing Techniques for Encrypted Relational Databases in Cloud Infrastructure, *International Journal of Computer Science and Information Technology Research* Vol. 13, Issue 3, DOI: https://doi.org/10.5281/zenodo.15834617

[41] Imoh, P. O. & Enyejo, J. O. (2025). Analyzing Social Communication Deficits in Autism Using Wearable Sensors and Real-Time Affective Computing Systems, *International Journal of Innovative Science and Research Technology* Volume 10, Issue 5 https://doi.org/10.38124/ijisrt/25may866

[42] Imoh, P. O., Adeniyi, M., Ayoola, V. B., & Enyejo, J. O. (2024). Advancing Early Autism Diagnosis Using Multimodal Neuroimaging and Ai-Driven Biomarkers for Neurodevelopmental Trajectory Prediction. *International Journal of Scientific Research and Modern Technology*, *3*(6), 40–56. https://doi.org/10.38124/ijsrmt.v3i6.413

[43] James, U. U., Idika, C. N., & Enyejo, L. A. (2023). Zero Trust Architecture Leveraging AI-Driven Behavior Analytics for Industrial Control Systems in Energy Distribution Networks, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* Volume 9, Issue 4 doi : https://doi.org/10.32628/CSEIT23564522

[44] James, U. U., Idika, C. N., Enyejo, L. A., Abiodun, K., & Enyejo, J. O. (2024). Adversarial Attack Detection Using Explainable AI and Generative Models in Real-Time Financial Fraud Monitoring Systems. *International Journal of Scientific Research and Modern Technology,* 3(12), 142–157. https://doi.org/10.38124/ijsrmt.v3i12.644

[45] Klöti, R., Kotronis, V., & Ager, B. (2013). OpenFlow: A security analysis. *Proceedings of the 21st IEEE International Conference on Network Protocols (ICNP)*, 1–6. https://doi.org/10.1109/ICNP.2013.6733589

[46] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

[47] Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1), 14–76. https://doi.org/10.1109/JPROC.2014.2371999

[48] Lara, A., Kolasani, A., & Ramamurthy, B. (2014). Network innovation using OpenFlow: A survey. *IEEE Communications Surveys & Tutorials*, 16(1), 493–512. https://doi.org/10.1109/SURV.2013.081313.00105

[49] Lee, S. M., Trimi, S., & Kim, C. (2013). The impact of cultural differences on technology entrepreneurship: A multi-country analysis. *Technological Forecasting and Social Change*, 80(6), 1124–1134. https://doi.org/10.1016/j.techfore.2012.10.017

[50] Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, 16(3), 1617–1634. https://doi.org/10.1109/SURV.2014.012214.00180

[51] Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. *Computer Science & IT Research Journal*, *4*(3).

[52] Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2023). Exploring Influencer Marketing Among Women Entrepreneurs using Encrypted CRM Analytics and Adaptive Progressive Web App Development. *International Journal of Scientific Research and Modern Technology*, *2*(6), 1–13. https://doi.org/10.38124/ijsrmt.v2i6.562

[53] Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Assessing Kanban Implementation for Secure Workflow Optimization in Cloud DevOps Using Zero Trust Architecture Enhancements, *Magna Scientia Advanced Research and Reviews*, 2025, DOI: https://doi.org/10.30574/msarr.2025.14.1.0072

[54] Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2023). Exploring SAFe Framework Adoption for Autism-Centered Remote Engineering with Secure CI/CD and Containerized Microservices Deployment *International Journal of Scientific Research in Science and Technology* Volume 10, Issue 6 doi : https://doi.org/10.32628/IJSRST

[55] Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2024). Evaluating Blockchain Content Monetization Platforms for Autism-Focused Streaming with Cybersecurity and Scalable Microservice Architectures *ICONIC RESEARCH AND ENGINEERING JOURNALS* Volume 8 Issue 1

[56] Ononiwu, M., Azonuche, T. I., Okoh, O. F.. & Enyejo, J. O. (2023). Machine Learning Approaches for Fraud Detection and Risk Assessment in Mobile Banking Applications and Fintech Solutions *International Journal of Scientific Research in Science, Engineering and Technology* Volume 10, Issue 4 doi : https://doi.org/10.32628/IJSRSET

[57] Pemmasani, P. K. (2023). National Cybersecurity Frameworks for Critical Infrastructure: Lessons from Governmental Cyber Resilience Initiatives. *International Journal of Acta Informatica*, *2*(1), 209-218.

[58] Polat, O., Oyucu, S., Türkoğlu, M., Polat, H., Aksoz, A. & Yardımcı, F. (2024). Hybrid AI-Powered Real-Time Distributed Denial of Service Detection and Traffic Monitoring for Software-Defined-Based Vehicular Ad Hoc Networks: A New Paradigm for Securing Intelligent Transportation Networks https://www.mdpi.com/2076-3417/14/22/10501

[59] Prohorovs, A., & Bistrova, J. (2021). Innovation ecosystems and the role of accelerators: Case study of cybersecurity start-ups. *Technological Forecasting and Social Change*, 169, 120818. https://doi.org/10.1016/j.techfore.2021.120818

[60] Radanliev, P., De Roure, D., Nurse, J. R. C., Montalvo, R. M., Cannady, S., & Santos, O. (2020). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, 102, 14–22. https://doi.org/10.1016/j.compind.2018.08.002

[61] Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016). A survey of security in software-defined networks. *IEEE Communications Surveys & Tutorials*, 18(1), 623–654. https://doi.org/10.1109/COMST.2015.2453114

[62] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

[63] Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752. https://doi.org/10.1126/science.aat5991

[64] Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, 51(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007

[65] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19. https://doi.org/10.1145/3298981

[66] Zahra, S. A., & Nambisan, S. (2012). Entrepreneurship and strategic thinking in business ecosystems. *Business Horizons*, 55(3), 219–229. https://doi.org/10.1016/j.bushor.2011.12.004

[67] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *Journal of Internet Services and Applications*, 1(1), 1–18. https://doi.org/10.1186/s13174-014-0010-3

[68] Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. *Sensors*, *23*(2), 788.

[69] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *PublicAffairs*.