Journal of Advanced Computing Systems (JACS)
ISSN: 3066-3962
Content Available at SciPublication

AI-Driven Anomaly Detection in U.S. University Networks: A Qualitative Study of Development, Implementation, and Governance

Okhae Joel Ojugo[1], Nseobot Afaha[2], Oghogho Timothy Obasuyi[3], Segun Onilude[4]
[1]*Virginia Polytechnic Institute and State University*
[2]*East Tennessee State University*
[3]*East Tennessee State University*
[4]*Waukesha County Technical College*
[1]*ORCID iD: 0009-0008-8092-5746*

DOI: 10.69987/JACS.2026.60801

Keywords

Artificial intelligence, anomaly detection, cybersecurity, higher education, university networks, IT governance, ethical AI

Abstract

Despite the growing adoption of artificial intelligence (AI) to strengthen cybersecurity, qualitative research examining the development, implementation, and governance of AI-driven anomaly detection systems within U.S. higher education remains limited. Universities present a distinct cybersecurity environment due to their decentralized IT infrastructures, diverse stakeholder communities, and the need to balance security with academic openness.This study investigates the development and implementation of AI-driven anomaly detection systems for identifying abnormal network behavior in U.S. university environments. A qualitative multiple-case study design was employed, drawing on semi-structured interviews with 11 cybersecurity professionals from six U.S. universities. The interview data were analyzed using thematic analysis to address the study's research questions. The findings reveal that the adoption and operation of AI-driven anomaly detection systems are shaped by several interconnected factors, including vendor influence, governance frameworks, and ethical considerations. Participants also identified significant implementation challenges, such as false-positive alerts, the complexity of university network environments, and institutional cultures that emphasize academic freedom and privacy. Overall, the findings highlight the critical role of effective governance in ensuring the successful deployment and responsible use of AI-driven cybersecurity technologies in higher education.

Introduction

Universities have undergone a profound digital transformation over the past decade, with teaching, research, and administrative activities becoming increasingly dependent on advanced information and communication technologies. Learning management systems, cloud computing, digital libraries, research repositories, and online collaboration platforms now form the foundation of modern higher education. While these technologies have expanded access to knowledge and improved institutional efficiency, they have also created a broader and more complex cybersecurity landscape by increasing the number of potential entry points for cyber threats (Kalume and Owiti, 2025). Consequently, safeguarding institutional networks and sensitive information has become a strategic priority for higher education institution At the same time, universities have become attractive targets for cybercriminals because they manage vast amounts of valuable information, including student records, financial data, proprietary research, and intellectual

property. Cyber incidents such as ransomware attacks, phishing campaigns, data breaches, and insider threats have become more frequent and increasingly sophisticated across the higher education sector (Othman, 2023). Traditional rule-based security mechanisms, which depend on predefined attack signatures and static detection rules, are often unable to identify evolving threats that manifest through unusual patterns of network behavior rather than known attack signatures (Huma and Muzaffar, 2024). In response, many institutions are adopting artificial intelligence (AI)-based cybersecurity technologies to strengthen their threat detection capabilities.

Artificial intelligence has emerged as a significant advancement in cybersecurity by enabling automated threat detection, adaptive learning, and continuous monitoring of network activity. AI-driven security systems employ machine learning algorithms to analyze large volumes of network traffic, identify deviations from normal behavioral patterns, and detect potential security incidents with greater speed and accuracy than conventional approaches (Ashraf et al., 2024). This growing reliance on AI reflects a broader shift toward intelligent, data-driven cybersecurity strategies capable of responding to increasingly dynamic and unpredictable threat environments. Within U.S. universities, the adoption of AI is particularly important because institutional networks are large, decentralized, and serve diverse user communities while operating under growing regulatory expectations for data security and privacy (Khorshed, Ali and Wasimi, 2012).

The U.S. higher education sector presents a particularly compelling setting for examining AI-driven cybersecurity. Universities in the United States operate some of the world's largest academic networks and maintain extensive repositories of federally funded research, making them attractive targets for cyber espionage, financial crime, and intellectual property theft (Nespoli et al., 2025). At the same time, institutions must comply with regulatory requirements such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and an expanding body of state-level data protection legislation. These legal obligations reinforce the need for cybersecurity solutions that are not only technically effective but also transparent, accountable, and ethically governed (Salih and Abdulrazzaq, 2023).

This study is positioned at the intersection of artificial intelligence, anomaly detection, and network security within the context of higher education. In cybersecurity, AI refers to the application of machine learning and advanced data analytics to automate threat detection, identify malicious activities, and improve incident response capabilities (Sarker, 2021). A key application of AI in this domain is anomaly detection, which focuses on identifying patterns of network behavior that deviate from established norms and may indicate a security compromise. Within universities, network security encompasses the policies, technologies, and operational practices designed to protect institutional digital assets while preserving the accessibility, openness, and collaboration that are fundamental to academic environments (Ullah et al., 2019).

AI-driven anomaly detection systems enhance existing network security frameworks by identifying threats in real time, particularly in environments characterized by highly diverse user behavior and heterogeneous computing infrastructures. University networks support a broad range of users including students, faculty, researchers, administrative staff, and external collaborators, whose activities generate highly variable patterns of network traffic. Machine learning techniques can distinguish between legitimate deviations in user behavior and potentially malicious activity more effectively than traditional signature-based detection methods (Katragadda, Kehinde and Kezron, 2020). However, the deployment of these technologies also introduces important governance challenges related to transparency, accountability, privacy, and the ethical use of AI.

The organizational structure of universities further complicates the implementation of AI-enabled cybersecurity solutions. Unlike corporate organizations, universities are founded on principles of academic freedom, openness, and shared governance. Their networks are intentionally designed to facilitate unrestricted access to

information, interdisciplinary collaboration, and innovation in teaching and research (Madhuri, 2023). While these characteristics are essential to the academic mission, they also increase institutional exposure to cyber threats and limit the effectiveness of restrictive security controls commonly employed in commercial organizations.

In addition, most higher education institutions operate through decentralized governance structures in which authority is distributed across colleges, departments, and administrative units. This decentralization often leads to fragmented IT environments, inconsistent security policies, and varying levels of technical expertise throughout the institution (Benaroch and Chernobai, 2017). Consequently, implementing AI-driven anomaly detection systems extends beyond technical deployment and requires careful coordination among multiple stakeholders, the establishment of effective governance mechanisms, and the development of security strategies that balance institutional protection with academic autonomy.

AI-Driven Anomaly Detection in Cybersecurity

Artificial intelligence (AI) has become a cornerstone of modern cybersecurity due to its ability to automate threat detection, process vast volumes of data, and adapt to evolving attack patterns (Lunardi et al., 2017). Unlike traditional rule-based security systems, AI-driven solutions rely on machine learning algorithms that continuously learn from historical data to identify patterns associated with malicious activity (Buchwald, Urbach and Ahlemann, 2014). This adaptive capability enables organizations to detect and respond to cyber threats more rapidly, particularly in complex and data-intensive network environments. Empirical studies have shown that AI-enhanced cybersecurity systems outperform conventional signature-based approaches in identifying previously unseen and zero-day attacks (Akhtar and Rawol, 2024). However, AI is not without limitations. Researchers have highlighted challenges including false-positive alerts, model drift, and biases introduced through training data, all of which can reduce the reliability of AI-based detection systems (Patchipala, 2023). These limitations underscore the continued need for human oversight and robust governance, particularly in sensitive environments such as higher education institutions.

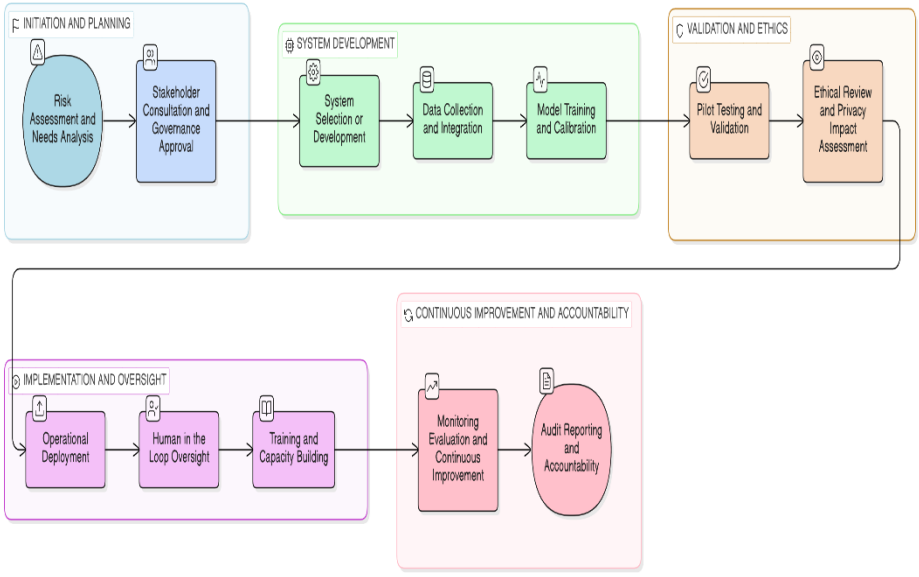
One of the most significant applications of AI in cybersecurity is anomaly detection, which focuses on identifying patterns of behavior that deviate from established norms (DeMedeiros, Hendawi and Alvarez, 2023). Within network security, anomalies may include unusual traffic patterns, unauthorized access attempts, abnormal login behavior, or unexpected data transfers (Xiong et al., 2014). AI-driven anomaly detection systems commonly employ unsupervised or semi-supervised machine learning techniques, enabling them to detect previously unknown threats without relying on predefined attack signatures or labeled datasets. This capability makes anomaly detection particularly valuable for identifying emerging cyber threats that may evade traditional detection methods.

Despite the technical advances reported in the literature, the operational deployment of AI-driven anomaly detection systems continues to present important challenges. Researchers consistently identify concerns related to model interpretability, scalability, and integration with existing cybersecurity operations (Samariya and Thakkar, 2023). High false-positive rates remain a persistent issue, often overwhelming security analysts, contributing to alert fatigue, and diminishing confidence in automated detection systems. Establishing stable behavioral baselines is also difficult because network activity continuously evolves, especially within heterogeneous environments such as universities, where users including students, faculty, researchers, and administrative staff generate highly diverse and dynamic patterns of network behavior (Teng, 2010). These technical and operational challenges reinforce the importance of considering organizational context, governance, and human expertise alongside advances in AI-based cybersecurity technologies.

IT Governance and Ethical AI in Higher Education

IT governance refers to the structures, policies, and decision-making processes that guide the management and strategic use of information technology within organizations (Bianchi and Sousa,

2016). In higher education, IT governance is shaped by shared governance models, decentralized organizational structures, and competing institutional priorities. Unlike centralized corporate environments, universities distribute decision-making authority across academic and administrative units, creating additional complexity in coordinating institution-wide technology initiatives. Nugroho (2014) and Scalabrin-Bianchi et al. (2021) argue that effective cybersecurity governance in higher education depends on close collaboration among institutional leaders, information technology professionals, faculty members, and regulatory stakeholders.



The increasing use of AI-enabled cybersecurity and surveillance technologies also raises important ethical questions concerning privacy, surveillance, individual autonomy, and data governance. These concerns are particularly significant in higher education, where institutional decisions may directly influence academic freedom, student trust, and organizational legitimacy. Umba et al. (2022) argue that AI-driven surveillance can normalize intrusive monitoring practices and alter institutional power relationships, potentially undermining the principles of transparency, intellectual freedom, and openness that universities seek to uphold. Accordingly, frameworks for ethical AI emphasize transparency, fairness, accountability, proportionality, and meaningful human oversight. Despite growing interest in these principles, empirical evidence on how they are operationalized within university cybersecurity programs remains limited, particularly in the context of AI-driven anomaly detection systems (Cummings et al., 2021).

Existing research further suggests that cybersecurity professionals generally adopt a cautious approach to AI-enabled security technologies, favoring human-in-the-loop models that preserve professional judgment, accountability, and oversight (George, 2024; Shahana et al., 2024). However, little is known about how trust in AI systems develops within higher education institutions, where governance structures, institutional cultures, and organizational priorities differ substantially from those of corporate organizations.

Against this backdrop, the present study qualitatively explores the development, implementation, and governance of AI-driven anomaly detection systems for identifying unusual network behavior in U.S. university environments. Specifically, the study seeks to:

Examine how AI-driven anomaly detection systems are developed within cybersecurity operations at U.S. universities.

Explore the challenges associated with implementing AI-driven anomaly detection systems

in university network environments across the United States.

Assess cybersecurity professionals' perceptions of how institutional values influence cybersecurity practices and the adoption of AI-driven anomaly detection technologies within university network environments.

Investigate the governance structures, institutional policies, and accountability mechanisms that guide the implementation and use of AI-driven anomaly detection systems in U.S. universities.

Conceptual Process Model for AI-Driven Anomaly Detection in U.S. University EnvironmentsFigure 1: A conceptual process model illustrating the sequential stages involved in the development, implementation, and governance of AI-driven anomaly detection systems (Adapted from Zeng et al., 2024) Figure 1 presents a conceptual process model illustrating how technical, organizational, and governance processes interact in the development, implementation, and governance of AI-driven anomaly detection systems within U.S. university environments. Adopting a socio-technical perspective, the model emphasizes that effective cybersecurity in higher education depends not only on technological capability but also on robust institutional governance, ethical oversight, and informed human decision-making. It serves as a conceptual framework for the discussion presented in the following sections.

The process begins with risk assessment and needs analysis, during which institutions evaluate their cybersecurity threat landscape, regulatory obligations, and network vulnerabilities. This stage establishes institutional justification for adopting AI-driven anomaly detection while ensuring alignment with legal, regulatory, and organizational policies. The next stage, stakeholder consultation and governance approval, reflects the shared governance structure common in higher education. Information technology leaders, legal counsel, data protection officers, and faculty representatives collectively participate in evaluating proposed cybersecurity initiatives, ensuring that technical decisions are informed by institutional priorities and stakeholder perspectives.

Following governance approval, institutions proceed to system selection or development, where commercial vendor solutions and internally developed platforms are assessed based on institutional requirements, interoperability, implementation costs, scalability, and regulatory compliance. This is followed by data collection and integration, in which network traffic data, security logs, and other relevant operational information are consolidated while adhering to principles of data minimization, anonymization, and privacy protection.

The model training and calibration phase adapts machine learning algorithms to the unique characteristics of university networks. Because higher education environments generate diverse patterns of legitimate activity—including research computing, academic collaboration, and decentralized network operations—the AI system must be calibrated to distinguish normal institutional behavior from potential security threats. Effective calibration reduces false-positive alerts while improving the contextual accuracy of anomaly detection.

Before institution-wide implementation, the system undergoes pilot testing and validation to evaluate technical performance, operational effectiveness, and unintended consequences. This phase is complemented by an ethical review and privacy impact assessment, which examines whether the proposed system aligns with institutional values such as academic freedom, transparency, individual privacy, and responsible data stewardship. These governance activities distinguish cybersecurity implementation in higher education from corporate settings, where operational efficiency often receives greater emphasis than institutional autonomy and academic values.

Following successful validation, the system enters operational deployment, where it is integrated into the university's security operations center (SOC) and incident response processes. A defining feature of the model is its emphasis on human-in-the-loop decision-making. Rather than allowing AI systems to operate autonomously, cybersecurity professionals retain responsibility for interpreting AI-generated alerts, validating system recommendations, and

making final response decisions. Maintaining human oversight reduces the risks associated with automation bias, improves accountability, and increases trust in AI-supported security operations.

The final stages—training and capacity building, continuous monitoring and performance evaluation, and audit, reporting, and accountability—position AI-driven anomaly detection as an evolving institutional capability rather than a static technological solution. Continuous professional development equips cybersecurity personnel to interpret AI outputs effectively, understand emerging threats, and apply ethical principles in operational decision-making. Ongoing monitoring enables institutions to refine system performance as network conditions and threat landscapes evolve, while formal auditing and reporting mechanisms strengthen transparency, regulatory compliance, and organizational accountability.

Overall, the conceptual process model demonstrates that implementing AI-driven anomaly detection in higher education extends beyond technological deployment. Successful implementation requires integrating AI within institutional governance structures, embedding ethical safeguards throughout the system's lifecycle, and maintaining meaningful human oversight. By balancing technological innovation with governance, privacy, and academic values, universities can strengthen their cybersecurity posture without compromising the openness, collaboration, and academic freedom that define higher education.

Higher education institutions present a distinctive cybersecurity environment because of their organizational structures, institutional missions, and academic culture. University networks are typically large, heterogeneous, and decentralized, supporting teaching, research, administration, and external collaboration across diverse user communities. Unlike corporate organizations, universities prioritize openness, knowledge sharing, and academic freedom, which can limit the use of restrictive security controls and centralized monitoring practices (Slade and Prinsloo, 2013).

At the same time, universities have become increasingly attractive targets for cybercriminals because they store valuable personal information, financial records, and high-value research data while often maintaining highly accessible network environments (Back and LaPrade, 2020). However, limited financial resources, decentralized governance, fragmented IT infrastructures, and uneven technical capabilities across institutional units frequently complicate the implementation of comprehensive cybersecurity strategies. These organizational characteristics make the adoption of advanced AI-driven security technologies particularly challenging, requiring institutions to balance evolving security requirements with their longstanding commitments to openness, privacy, and academic autonomy.

Research Questions

The following research questions guided this study:

How are AI-driven anomaly detection systems developed within cybersecurity operations at U.S. universities?

What challenges do cybersecurity professionals encounter when implementing AI-driven anomaly detection systems in U.S. university network environments?

How do cybersecurity professionals perceive the influence of institutional values on cybersecurity practices and the adoption of AI-driven anomaly detection systems in U.S. universities?

What governance structures, policies, and accountability mechanisms guide the implementation and use of AI-driven anomaly detection systems in U.S. universities?

Methodology

This study employed a qualitative multiple-case study design to examine the development, implementation, and governance of AI-driven anomaly detection systems in U.S. university network environments. A qualitative approach was selected because it enables an in-depth exploration of institutional processes, governance practices, stakeholder experiences, and ethical considerations that cannot be adequately captured through

quantitative methods (Creswell & Poth, 2018). The multiple-case study design facilitated comparisons across institutions, providing a richer understanding of how AI-driven anomaly detection systems are developed and implemented in different organizational contexts while enhancing the transferability of the findings (Yin, 2018).

The study population comprised cybersecurity and information technology professionals working in U.S. higher education institutions who were directly involved in the development, implementation, governance, or oversight of AI-driven anomaly detection systems. Participants were selected through purposive sampling to ensure they possessed relevant expertise and practical experience (Patton, 2015). Eleven participants from six U.S. universities were recruited, representing a range of institutional contexts, including public and private universities as well as research-intensive and teaching-focused institutions. The sample size was considered sufficient to achieve thematic saturation while enabling meaningful cross-case comparisons (Creswell & Poth, 2018).

Primary data were collected through semi-structured interviews lasting between 45 and 75 minutes. Interviews were conducted via secure video-conferencing platforms or, where feasible, in person. An interview guide was developed from the study's research questions and explored topics including the selection or development of AI-driven anomaly detection systems, implementation challenges, the influence of institutional values such as academic freedom and privacy, and governance structures supporting AI-enabled cybersecurity. All interviews were conducted with participants' informed consent, audio-recorded, and transcribed verbatim for analysis.

To complement the interview data, relevant institutional documents—including publicly available cybersecurity policies, AI governance frameworks, and incident response procedures—were analyzed to provide organizational context and support data triangulation (Bowen, 2009). Integrating documentary evidence with interview data strengthened the credibility and trustworthiness of the study.

Ethical principles were observed throughout the research process. Participants received detailed information about the purpose of the study, data collection procedures, confidentiality measures, and their right to withdraw at any stage without consequence. To protect anonymity, pseudonyms were assigned to both participants and institutions, and identifying information was removed from all transcripts and research records. Given the sensitivity of cybersecurity information, participants were advised not to disclose confidential operational details or specific system vulnerabilities. All research data were stored in encrypted digital files accessible only to the researcher.

The data were analyzed using Braun and Clarke's (2006) six-phase thematic analysis framework. The analysis involved familiarization with the data through repeated reading of interview transcripts and documents, systematic coding of the dataset, identification of preliminary themes, review and refinement of emerging themes, definition and naming of final themes, and production of the analytical narrative. NVivo qualitative data analysis software was used to facilitate data organization and coding. A cross-case analysis was subsequently undertaken to identify recurring patterns as well as contextual differences across participating institutionsFindings

Table 1: Summary of Participant Responses (U.S. Universities)

Participant	Role & Institution Type	System Development / Selection	Implementation Challenges	Institutional Values Influence	Governance Structures
P1	CISO, Public R1 University	Evaluated commercial AI platforms aligned with NIST and	Tuning system to avoid	Academic freedom shapes system	Multi-layered governance involving IT committees,

		existing SIEM systems.	misclassifying research activity.	configuration and transparency.	legal counsel, and privacy offices.
P2	Security Architect, Private University	System emerged from a federally funded pilot project.	High false positives from research labs.	Privacy considerations override technical efficiency.	AI ethics guidelines approved by provost's office.
P3	Network Security Manager, State University	Partnered with vendor specializing in higher education AI tools.	Data integration across decentralized departments.	Shared governance culture slows but strengthens adoption.	Risk management and compliance offices oversee AI use.
P4	IT Director, Private Research University	Customized commercial platform with internal rules and models.	Faculty resistance and surveillance concerns.	Cybersecurity framed as shared responsibility, not policing.	Governance informed by federal guidance and research ethics policies.
P5	Security Analyst, Public Teaching University	Adopted system via state IT consortium recommendation.	Limited staffing and budget constraints.	Equity and inclusion shape policy communication.	Policies reviewed annually by cybersecurity advisory board with faculty members.
P6	SOC Manager, Public Research University	Consulted faculty experts to advise on transparency and bias.	FERPA compliance and privacy governance layers.	Avoidance of black-box systems due to ethical research standards.	Institutional risk assessment and review processes required for deployment.
P7	Privacy Officer, Private University	System selected after privacy impact assessment.	Tension between security and openness values.	Trust and justification required for monitoring tools.	Internal audits and compliance reporting mechanisms.
P8	Cybersecurity Engineer, Public University	Tested multiple platforms using historical network data.	Legacy infrastructure limitations.	Faculty autonomy shapes departmental implementation.	Cross-functional governance groups ensure value alignment.
P9	IT Security Lead, Community	Gradual transition from rule-based to	Staff training to interpret AI	Student rights and data protection	Governance prioritizes transparency,

	College System	AI-based detection.	outputs responsibly.	obligations shape configuration.	documentation, and oversight.
P10	Director of IT Security, Private Liberal Arts University	Relied on peer institution case studies and EDUCAUSE reports.	Organizational change management challenges.	Liberal arts mission promotes minimal intrusion.	AI governance embedded in broader IT and data governance frameworks.
P11	Deputy CISO, Large Public University	Formal procurement emphasizing explainability and compliance.	Aligning AI security practices with institutional risk tolerance.	Transparency norms require public documentation of AI policies.	Governance shaped by regulatory frameworks and accreditation requirements.

Theme 1: Development Pathways of AI-Driven Anomaly Detection Systems in U.S. Universities

Subtheme 1: Vendor-Led Adoption and Pilot-Based Innovation

Interview data indicate that AI-driven anomaly detection systems in U.S. universities are acquired primarily through structured vendor evaluation rather than developed internally. Participants, particularly Chief Information Security Officers (CISOs) from large public research universities, described formal procurement processes that assessed commercial platforms for compliance with cybersecurity standards, scalability, interoperability, and compatibility with existing Security Information and Event Management (SIEM) infrastructures. One participant explained:

"We evaluated several commercial platforms aligned with NIST and our SIEM infrastructure. Vendor compliance and scalability were critical factors in our selection." (P1)

Participants also described pilot implementations as an important stage in the adoption process. Rather than deploying AI technologies institution-wide immediately, universities commonly evaluated system performance through controlled pilot projects before broader implementation. These pilots enabled institutions to assess detection accuracy, operational impact, and compatibility with the highly dynamic nature of university network environments, particularly those supporting research-intensive activities. As one security architect noted:

"The system emerged from a federally funded pilot project. After demonstrating reduced incident response times, it was formally adopted." (P2)

Document analysis supported these findings. Publicly available institutional cybersecurity policies and EDUCAUSE guidance advocate phased implementation and pilot testing to reduce operational risk and improve organizational readiness (Doc 4; Doc 5). Together, these findings suggest that AI adoption in higher education is characterized by incremental implementation, emphasizing evidence-based decision-making rather than rapid technological deployment.

Table 2: Summary of Publicly Available U.S. Universities AI Adoption Documents

Doc ID	Document Title	Source / University	Key Content Summary
Doc 1	**Northern Illinois University – Information Security Policy** https://www.niu.edu/policies/policy-documents/information-security-policy.shtml	Northern Illinois University policy library	Defines data classification (Restricted, Private, Public), roles for security incident response, responsibilities for system administrators and information stewards, and incident reporting procedures. This gives insight into institutional cybersecurity governance and procedural frameworks.
Doc 2	NJIT Information Security Policy https://www.njit.edu/policies/information-security-policy	New Jersey Institute of Technology policy library	University-wide information security framework that integrates NIST standards (800-53 & 800-171), governance structure for information asset protection, and decision-making authority for security controls. Useful for understanding how a public research university governs network security and compliance.
Doc 3	**University of Southern Indiana – Information Security Policy** https://www.usi.edu/it/security/information-security-policy	University of Southern Indiana IT security	Network encryption, physical security standards, and vendor management elements. Shows real-world practices for securing network infrastructure, which can be triangulated with interviews on implementation challenges and governance.
Doc 4	**EDUCAUSE – Governance, Compliance, and Policy Guide** https://www.educause.edu/cybersecurity-and-privacy-guide/governance-compliance-and-policy	EDUCAUSE Cybersecurity & Privacy Guide	A curated repository of governance, compliance, risk management, and policy templates and examples used by U.S. higher education institutions; a good reference point for comparing institutional approaches to cybersecurity governance.
Doc 5	**EDUCAUSE – Campus AI/Policy Collection** https://library.educause.edu/topics/policy-and-law/campus-policy	EDUCAUSE Library (campus policies collection)	Index of higher education campus policies including Acceptable Use, AI, data classification, FERPA, etc. Useful to locate specific AI-related governance and responsible use policies from real universities.
Doc 6	FERPA and Cybersecurity Regulatory Considerations https://www.educause.edu/research/community/2024/navigating-the-xr-educational-landscape-privacy-safety-and-ethical-guidelines/regulatory-and-ethical-considerations	EDUCAUSE regulatory overview	Explains how FERPA and related legal frameworks (GLBA, NIST 800-171 guidance) influence data protection and cybersecurity practices at U.S. colleges and universities. Relevant for ethical and governance analysis.
	NIST Cybersecurity Framework (CSF) (General) https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework	NIST overview via Wikipedia	Widely adopted framework for cybersecurity governance (Identify, Protect, Detect, Respond, Recover). Many university policies reference or align with NIST CSF, making this highly applicable for document comparison.

Subtheme 2: Integration of Academic Expertise and Ethical Oversight

A distinguishing feature of AI implementation in universities was the active involvement of academic expertise in system development and evaluation. Participants reported collaborating with faculty members, particularly computer science researchers, to assess the transparency, interpretability, and potential bias of machine learning models before deployment. One security operations manager stated:

"Faculty researchers advised on transparency and bias risks, ensuring that our anomaly detection models were aligned with ethical and institutional norms." (P6)

This collaborative approach reflects the governance culture of higher education, where technical decisions frequently incorporate academic expertise and institutional oversight. Documentary evidence reinforced this finding, with university AI governance frameworks requiring ethical review and privacy impact assessments before operational deployment (Doc 4; Doc 6). Unlike many corporate environments, where cybersecurity decisions are typically centralized within information technology departments, universities integrate academic participation into decision-making processes, reflecting their commitment to transparency, accountability, and shared governance.

Subtheme 3: Privacy and Regulatory Compliance as Development Constraints

Privacy protection and regulatory compliance emerged as major factors influencing both system selection and implementation. Participants consistently described privacy impact assessments as a prerequisite for adopting AI-driven anomaly detection technologies, ensuring that security objectives were balanced with institutional responsibilities to protect personal information. As one privacy officer explained:

"The system was selected after a privacy impact assessment. Our design choices reflect a commitment to protecting student and faculty data while maintaining operational effectiveness." (P7)

These perspectives were consistent with institutional policies and publicly available guidance emphasizing compliance with the Family Educational Rights and Privacy Act (FERPA), state privacy legislation, and other applicable regulatory requirements (Doc 1; Doc 2). Rather than functioning solely as legal obligations, privacy and compliance considerations actively shaped system architecture, operational policies, and governance decisions. This finding reinforces the socio-technical nature of AI implementation, where technological capability is continually balanced against legal, ethical, and institutional responsibilities.

Subtheme 4: Collaborative Procurement and Shared Governance

Participants also described collaborative procurement as an important mechanism for acquiring AI-driven cybersecurity technologies, particularly among smaller and teaching-focused institutions with limited technical and financial resources. Several participants reported adopting solutions through state higher education IT consortia, allowing institutions to share expertise, reduce procurement costs, and standardize cybersecurity capabilities across multiple campuses. One participant explained:

"We adopted the system through a state IT consortium, which allowed us to leverage collective expertise and reduce procurement risk." (P5)

Beyond improving resource efficiency, consortium-based procurement strengthened governance by promoting shared standards, coordinated decision-making, and collective accountability. These collaborative arrangements illustrate how institutional partnerships can expand access to advanced cybersecurity technologies while supporting governance structures that emphasize transparency, consistency, and responsible technology adoption.

Theme Summary

Collectively, the findings demonstrate that the development of AI-driven anomaly detection systems in U.S. universities extends beyond technology acquisition. Development pathways are shaped by regulatory compliance, institutional governance, ethical oversight, privacy considerations, organizational capacity, and collaborative partnerships. Rather than relying exclusively on technical criteria, universities adopt AI-driven cybersecurity solutions through governance-oriented processes that seek to balance operational effectiveness with institutional values and public accountability.

Theme 2: Implementation Challenges of AI-Driven Anomaly Detection Systems in U.S. University Networks

Subtheme 1: Technical Complexity and False Positives in Academic Network Environments

Participants consistently identified false-positive alerts as one of the most significant technical challenges associated with implementing AI-driven anomaly detection systems. University networks generate highly diverse and dynamic traffic patterns resulting from research computing, academic collaboration, student activities, and administrative operations. Consequently, legitimate network behavior was frequently classified as suspicious, increasing the burden on security teams. One network security manager explained:

"Research labs running high-volume data transfers were frequently flagged as threats, which increased analyst workload and delayed response times." (P3)

Documentary evidence supported this observation, with institutional cybersecurity policies emphasizing continuous model tuning, adaptive monitoring, and regular refinement of detection rules to improve system accuracy (Doc 2; Doc 4). These findings suggest that many commercially available AI-driven security platforms are designed primarily for enterprise environments and require substantial customization to accommodate the unique operational characteristics of university networks.

Subtheme 2: Organizational Fragmentation and Decentralized IT Structures

The decentralized governance structure of higher education institutions emerged as another major implementation challenge. Participants described difficulties integrating AI-driven anomaly detection systems across departments that maintained independent IT infrastructures, security policies, and operational procedures. As one cybersecurity engineer noted:

"Departments use different tools and network architectures, which made system integration slow and uneven." (P8)

This finding was reinforced by institutional governance documents highlighting the complexity of coordinating cybersecurity policies and technology deployment across autonomous academic units (Doc 5). The evidence indicates that organizational fragmentation extends implementation timelines and complicates institution-wide standardization, underscoring the importance of governance frameworks that facilitate collaboration while respecting departmental autonomy.

Subtheme 3: Workforce Readiness and Interpretability of AI Outputs

Participants also emphasized that successful implementation depends on the ability of cybersecurity personnel to understand, interpret, and trust AI-generated outputs. Several participants reported that limited explainability reduced confidence in automated alerts and created uncertainty during incident response. One IT security lead explained:

"We had challenges training staff to interpret AI outputs responsibly. Without explainability, trust in the system was limited." (P9)

These observations are consistent with institutional guidance advocating human-in-the-loop decision-making and explainable artificial intelligence (XAI) to support responsible cybersecurity operations (Doc 2; Doc 3). The findings demonstrate that implementation success depends not only on algorithmic performance but also on workforce capability, organizational learning, and confidence in AI-assisted decision-making.

Subtheme 4: Institutional Resistance and Cultural Tensions

Institutional culture also influenced the implementation of AI-driven anomaly detection systems. Participants reported that faculty members and researchers occasionally expressed concerns regarding surveillance, academic freedom, and the collection of network activity data. One IT director from a private research university commented:

"Faculty resistance was an issue, especially concerns about academic freedom and surveillance." (P4)

These concerns were reflected in institutional privacy policies and FERPA guidance emphasizing proportional monitoring, data minimization, and respect for individual privacy (Doc 1; Doc 6). Rather than representing simple resistance to technological change, participant responses suggest that implementation requires careful negotiation between institutional security objectives and the core values of higher education. Building trust among stakeholders therefore becomes an essential component of successful AI adoption.

Theme Summary

Overall, the findings demonstrate that implementing AI-driven anomaly detection systems in U.S. universities is influenced by a combination of technical, organizational, and cultural factors. False-positive alerts, decentralized IT environments, workforce preparedness, and institutional concerns regarding privacy and academic freedom all shape implementation outcomes. These findings reinforce the view that successful AI adoption in higher education requires more than technical capability; it also depends on effective governance, stakeholder engagement, continuous workforce development, and alignment with institutional values.

Theme 3: Institutional Values and Their Influence on Cybersecurity Practices in U.S. Universities

Subtheme 1: Academic Freedom as a Constraint on Security Surveillance

Participants consistently identified academic freedom as a defining institutional value that influences the design, configuration, and operation of AI-driven anomaly detection systems. Rather than maximizing surveillance capabilities, security leaders described deliberately limiting monitoring practices to protect scholarly independence and intellectual inquiry. As one Chief Information Security Officer (CISO) explained:

"Academic freedom strongly influences how surveillance tools are configured. We prioritize transparency and minimal intrusion." (P1)

Document analysis reinforced this perspective, with institutional governance frameworks emphasizing the protection of academic freedom and intellectual autonomy as fundamental principles of higher education (Doc 4). These findings suggest that cybersecurity decision-making in universities extends beyond technical risk management and is shaped by institutional values that establish clear boundaries for security practices.

Subtheme 2: Privacy and Data Protection as Dominant Operational Values

Privacy protection emerged as one of the most influential factors shaping cybersecurity practices. Participants described privacy impact assessments, legal reviews, and compliance evaluations as routine components of the decision-making process before AI-enabled security technologies were deployed. One privacy officer noted:

"Privacy considerations often override technical efficiency in our decision-making." (P2)

This perspective was consistent with publicly available FERPA guidance and institutional privacy policies, which require universities to safeguard personal information while minimizing unnecessary data collection and monitoring (Doc 1; Doc 5). The findings indicate that privacy functions not only as a regulatory requirement but also as an institutional value that shapes both technical design decisions and operational policies.

Subtheme 3: Transparency and Trust as Governance Imperatives

Transparency was identified as another core institutional value influencing the governance of AI-driven cybersecurity technologies. Participants explained that universities frequently accompany AI deployment with formal policies, governance documentation, and communication initiatives intended to explain how AI systems operate and how institutional data are protected. A deputy CISO stated:

"Institutional transparency norms require us to publicly document AI use policies." (P11)

These findings are consistent with EDUCAUSE guidance promoting transparency, stakeholder engagement, and responsible AI governance within higher education (Doc 4). Participants suggested that transparent governance strengthens institutional trust, increasing stakeholder confidence in AI-supported cybersecurity while reinforcing organizational accountability.

Subtheme 4: Shared Governance and Collective Responsibility

Participants also emphasized the influence of shared governance on cybersecurity decision-making. Rather than relying exclusively on centralized IT leadership, universities frequently involve faculty committees, governance councils, legal advisors, and cross-functional working groups in the development and oversight of cybersecurity policies. One IT director explained:

"We frame cybersecurity as a shared responsibility rather than a policing function." (P4)

Institutional governance documents similarly characterize cybersecurity as a collaborative responsibility that extends beyond technical departments to include the broader university community (Doc 4). This participatory approach reflects the governance traditions of higher education and demonstrates that successful implementation of AI-driven cybersecurity technologies depends on institutional collaboration, stakeholder engagement, and collective accountability.

Theme Summary

Collectively, the findings demonstrate that cybersecurity practices in U.S. universities are shaped as much by institutional values as by technological considerations. Academic freedom, privacy, transparency, and shared governance influence how AI-driven anomaly detection systems are designed, implemented, and governed. Rather than constraining cybersecurity effectiveness, these values establish the ethical and organizational framework within which AI technologies are deployed, ensuring that institutional security objectives remain aligned with the broader mission and principles of higher education.

Theme 4: Governance Structures, Policies, and Accountability Mechanisms Guiding AI-Driven Anomaly Detection in U.S. Universities

Subtheme 1: Multi-Layered Governance Architectures

Participants consistently described the governance of AI-driven anomaly detection systems as a distributed institutional process involving multiple stakeholders. Rather than residing solely within cybersecurity teams, governance responsibilities were shared among information technology leaders, legal counsel, privacy offices, risk management units, and academic governance bodies. One Chief Information Security Officer (CISO) explained:

"We operate under a multi-layered governance model involving IT governance committees, legal counsel, and data privacy offices." (P1)

Institutional governance documents reflected similar structures, emphasizing cross-functional oversight, consultation, and shared accountability in cybersecurity decision-making (Doc 2; Doc 4). These findings indicate that AI governance in higher education relies on collaborative institutional structures that distribute authority across multiple organizational units, ensuring that technical, legal, ethical, and academic considerations are incorporated into governance decisions.

Subtheme 2: Policy Frameworks and Regulatory Alignment

Participants emphasized that governance decisions are guided by formal institutional policies and external regulatory requirements. AI-driven anomaly detection systems were implemented within governance frameworks aligned with federal legislation, state regulations, institutional policies, and established cybersecurity standards such as the National Institute of Standards and Technology (NIST) framework. One security architect explained:

"AI security tools are governed by institutional AI ethics guidelines approved by the provost's office." (P2)

Document analysis supported these accounts, demonstrating that universities require formal risk assessments, policy approval processes, governance documentation, and compliance reviews before implementing AI-enabled cybersecurity technologies (Doc 2; Doc 4; Doc 6). Collectively, these findings suggest that governance is embedded within a structured policy environment that promotes regulatory compliance while supporting responsible AI adoption.

Subtheme 3: Accountability Through Oversight, Audit, and Documentation

Participants identified accountability as a defining characteristic of AI governance. Oversight mechanisms included periodic internal audits, policy reviews, documentation requirements, access controls, and formal incident reporting procedures. A privacy officer explained:

"Accountability is enforced through internal audits and compliance reporting mechanisms." (P7)

Institutional policies similarly required comprehensive documentation of system configurations, user access logs, governance decisions, and incident response activities (Doc 1; Doc 2). These findings demonstrate that accountability extends beyond technological safeguards and is institutionalized through governance processes that emphasize transparency, documentation, and continuous oversight.

Subtheme 4: External Regulatory and Accreditation Pressures

Participants also highlighted the influence of external regulatory agencies and accreditation requirements on institutional governance practices. Compliance obligations arising from federal legislation, state cybersecurity regulations, funding agencies, and accreditation standards were described as important drivers of governance decisions. As one deputy CISO noted:

"External regulatory frameworks and accreditation requirements shape our governance decisions." (P11)

Publicly available policy documents confirmed that universities operate within overlapping compliance frameworks requiring ongoing monitoring, documentation, and periodic assessment of cybersecurity practices (Doc 5; Doc 6). These findings indicate that AI governance in higher education is shaped not only by internal institutional priorities but also by external accountability mechanisms that reinforce responsible technology management and regulatory compliance.

Theme Summary

Overall, the findings demonstrate that governance of AI-driven anomaly detection systems in U.S. universities is characterized by distributed decision-making, policy-driven implementation, institutional accountability, and external regulatory oversight. Rather than functioning solely as an administrative process, governance provides the organizational framework through which universities balance cybersecurity objectives with legal obligations, ethical principles, and institutional values. This multi-layered approach enables universities to adopt AI-driven cybersecurity technologies while maintaining transparency, accountability, and public trust.

Discussion

Evidence from the participating universities indicates that AI driven anomaly detection systems are developed through a combination of commercial vendor partnerships, pilot based innovation, and collaborative governance involving information technology leaders, legal counsel, privacy officers, and faculty stakeholders. This pattern is consistent with previous studies reporting an increasing reliance on commercial AI cybersecurity solutions as institutions respond to escalating cyber threats while operating under financial and technical constraints (Dopamu, Adesiyan and Oke, 2024). Beyond confirming previous research, the findings reveal that universities distinguish themselves from many other sectors by embedding ethical review, privacy assessments, and academic oversight throughout the development process. Rather than

treating AI adoption as a purely technical procurement decision, participating universities integrated governance, ethical review, and institutional oversight into system design and deployment, reflecting long standing commitments to transparency, accountability, and academic freedom (Ibitoye, 2023). These observations are consistent with socio technical systems theory, which argues that technological systems are shaped through the interaction of technical capabilities, organizational structures, institutional values, and regulatory environments (Baxter and Sommerville, 2011). Within higher education, AI driven cybersecurity systems therefore emerge not only as technical solutions but also as products of institutional governance, organizational culture, and ethical responsibility.

While development pathways reflect institutional governance and ethical priorities, successful implementation introduces an additional set of technical and organizational challenges. Implementation was constrained by several interrelated factors, including false positive alerts, decentralized network infrastructures, workforce preparedness, and institutional resistance to AI enabled surveillance. These observations are consistent with earlier research highlighting the limitations of opaque AI models, particularly their tendency to generate excessive alerts and reduce operational trust among cybersecurity professionals (Bhatt, 2024; NIST, 2022). The present findings extend this body of knowledge by demonstrating that these challenges are amplified within higher education because of the diversity of network users, the variability of research related network activity, and decentralized governance structures. Unlike enterprise environments with relatively standardized network behavior, university networks support highly heterogeneous activities that make it more difficult to distinguish legitimate anomalies from malicious behavior. Consequently, successful implementation requires continuous model refinement, context specific calibration, and sustained human oversight. These findings reinforce growing support for explainable artificial intelligence (XAI) and human in the loop approaches that enhance transparency, strengthen analyst confidence, and improve decision making in cybersecurity operations.

These implementation challenges cannot be fully understood without considering the institutional environment in which universities operate. Beyond technical considerations, institutional values emerged as a defining influence on cybersecurity practice. Participants consistently identified academic freedom, privacy, transparency, and shared governance as principles that shape how AI-driven anomaly detection systems are designed, configured, and governed. These findings support earlier studies describing the tension between surveillance oriented security strategies and the values that underpin higher education institutions (Prinsloo and Slade, 2015). More importantly, the findings demonstrate how these values are translated into everyday governance practices through privacy impact assessments, stakeholder consultation, ethical review processes, and transparent policy development. From the perspective of institutional theory, cybersecurity practices in universities are influenced not only by technical risk but also by the need to maintain organizational legitimacy and stakeholder trust (Scott, 2017). Security decisions are therefore evaluated against institutional norms and expectations, resulting in governance approaches that balance effective risk management with the preservation of academic autonomy and individual rights.

The influence of institutional values is further reflected in the governance mechanisms established to oversee AI deployment. Governance of AI-driven anomaly detection systems was characterized by multi layered accountability involving cybersecurity committees, legal and compliance offices, ethics boards, executive leadership, and other institutional stakeholders. This observation supports previous research emphasizing the importance of governance frameworks for responsible AI deployment (De Almeida, Dos Santos and Farias, 2021). The findings also demonstrate how governance in higher education differs from many organizational settings by operating within a pluralistic institutional environment where legal compliance, ethical stewardship, academic governance, and organizational accountability intersect (Chelvachandran et al., 2020). Accountability was achieved primarily through institutional processes, including policy development, documentation, auditing, compliance monitoring, and reporting,

rather than through technical controls alone. This suggests that effective AI governance depends on embedding accountability within organizational structures, decision making processes, and institutional culture, ensuring that technological innovation remains aligned with ethical principles and public responsibility.

Taken together, the findings suggest that the successful adoption of AI driven anomaly detection systems in U.S. universities depends on considerably more than technological capability. Effective implementation requires governance structures that integrate technical expertise, institutional values, regulatory compliance, and meaningful human oversight throughout the system's lifecycle. Viewed from a socio technical perspective, AI enabled cybersecurity in higher education is fundamentally an organizational and governance challenge as much as it is a technological one. Universities that align AI deployment with institutional values, transparent governance, and collaborative decision making are likely to be better positioned to strengthen cybersecurity resilience while preserving the openness, trust, and academic freedom that define higher education.

Conclusion

The successful development and implementation of AI driven anomaly detection systems in U.S. universities depend on considerably more than technological capability. This article has shown that institutional values, governance structures, ethical oversight, and human judgment are central to how these systems are designed, deployed, and managed. Although AI has considerable potential to strengthen cybersecurity through improved threat detection and incident response, its effectiveness within higher education is shaped by the distinctive organizational characteristics of universities, including shared governance, academic freedom, privacy expectations, and regulatory compliance.

The findings underscore the importance of governance frameworks that balance cybersecurity objectives with institutional values. Human oversight, transparent decision making, and organizational accountability emerged as essential foundations for building trust in AI driven anomaly detection systems and supporting their sustainable adoption. As universities continue to expand their digital infrastructure and confront increasingly sophisticated cyber threats, AI should be implemented within governance frameworks that are transparent, ethically grounded, and responsive to the unique mission of higher education. Such an approach can strengthen institutional cyber resilience while preserving the openness, collaboration, and academic freedom that remain central to the university environment.

References

[1] Akhtar, Z. Bin and Rawol, A.T. (2024) 'Enhancing cybersecurity through AI-powered security mechanisms', IT journal research and development, 9(1), pp. 50–67.

[2] De Almeida, P.G.R., Dos Santos, C.D. and Farias, J.S. (2021) 'Artificial intelligence regulation: a framework for governance', Ethics and Information Technology, 23(3), pp. 505–525.

[3] Ashraf, M.W.A. et al. (2024) 'A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things', Scientific Reports, 14(1), p. 27058. Available at: https://www.nature.com/articles/s41598-024-78976-1.pdf.

[4] Back, S. and LaPrade, J. (2020) 'Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions', International Journal of Cybersecurity Intelligence & Cybercrime, 3(2), pp. 25–47.

[5] Baxter, G. and Sommerville, I. (2011) 'Socio-technical systems: From design methods to systems engineering', Interacting with computers, 23(1), pp. 4–17.

[6] Benaroch, M. and Chernobai, A. (2017) 'Operational IT failures, IT value destruction, and board-level IT governance changes', MIS quarterly, 41(3), pp. 729-A6.

[7] Bhatt, U. (2024) 'Trustworthy Machine Learning: From Algorithmic Transparency to Decision Support'.

[8] Bianchi, I.S. and Sousa, R.D. (2016) 'IT Governance mechanisms in higher education', Procedia Computer Science, 100, pp. 941–946.

[9] Buchwald, A., Urbach, N. and Ahlemann, F. (2014) 'Business value through controlled IT: Toward an integrated model of IT governance success and its impact', Journal of Information Technology, 29(2), pp. 128–147.

[10] Chelvachandran, N. et al. (2020) 'Considerations for the governance of AI and government legislative frameworks', in Cyber defence in the age of AI, smart societies and augmented humanity. Springer, pp. 57–69.

[11] DeMedeiros, K., Hendawi, A. and Alvarez, M. (2023) 'A survey of AI-based anomaly detection in IoT and sensor networks', Sensors, 23(3), p. 1352.

[12] Dopamu, O., Adesiyan, J. and Oke, F. (2024) 'Artificial intelligence and US financial institutions: review of AI-assisted regulatory compliance for cybersecurity', World J Adv Res Reviews, 21(3), pp. 964–979.

[13] George, A.S. (2024) 'Emerging trends in AI-driven cybersecurity: an in-depth analysis', Partners Universal Innovative Research Publication, 2(4), pp. 15–28.

[14] Huma, Z. and Muzaffar, J. (2024) 'Hybrid AI Models for Enhanced Network Security: Combining Rule-Based and Learning-Based Approaches', Global Perspectives on Multidisciplinary Research, 5(3), pp. 52–63. Available at: http://snmzpublications.com/index.php/gpmr/article/download/21/22.

[15] Ibitoye, J. (2023) 'Zero-Trust cloud security architectures with AI-orchestrated policy enforcement for US critical sectors', International Journal of Science and Engineering Applications, 12(12), pp. 88–100.

[16] Kalume, S.N. and Owiti, S.O. (2025) 'cybersecurity challenges strategies and emerging trends in higher education institutions–a survey', EPRA International Journal of Research & Development (IJRD), pp. 98–103. Available at: https://cdn.epratrustpublishing.com/article/202501-02-019824.pdf.

[17] Katragadda, S., Kehinde, O. and Kezron, I.E. (2020) 'Anomaly detection: Detecting unusual behavior using machine learning algorithms to identify potential security threats or system failures', International Research Journal of Modernization in Engineering Technology and Science, 2(5), pp. 1342–1350.

[18] Khorshed, M.T., Ali, A.B.M.S. and Wasimi, S.A. (2012) 'Classifying different denial-of-service attacks in cloud computing using rule-based learning', Security and Communication Networks, 5(11), pp. 1235–1247.

[19] Lunardi, G.L. et al. (2017) 'Antecedents of IT governance effectiveness: An empirical examination in Brazilian firms', Journal of information systems, 31(1), pp. 41–57.

[20] Madhuri, K. (2023) 'Security Threats and Detection Mechanisms in Machine Learning', Handbook of Artificial Intelligence, 255.

[21] Masengo Wa Umba, S., Abu-Mahfouz, A.M. and Ramotsoela, D. (2022) 'Artificial intelligence-driven intrusion detection in software-defined wireless sensor networks: Towards secure IoT-enabled healthcare systems', International Journal of Environmental Research and Public Health, 19(9), p. 5367.

[22] Nespoli, P. et al. (2025) 'Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision', IEEE Communications Surveys & Tutorials [Preprint]. Available at: https://ieeexplore.ieee.org/abstract/document/11053975/.

[23] Nugroho, H. (2014) 'conceptual model of it governance for higher education based on Cobit 5 framework.', Journal of Theoretical & Applied Information Technology, 60(2).

[24] Othman, Z. (2023) 'Sustainability of higher education institutions: Case study on cyber attacks', Global Business Management Review (GBMR), 15(1), pp. 24–38. Available at: https://repo.uum.edu.my/id/eprint/30022/1/GBMR 15 01 2023 24-38.pdf.

[25] Patchipala, S. (2023) 'Tackling data and model drift in AI: Strategies for maintaining accuracy during ML model inference', International Journal of Science and Research Archive, 10(2), pp. 1198–1209.

[26] Prinsloo, P. and Slade, S. (2015) 'Student privacy self-management: Implications for learning analytics', in Proceedings of the fifth international conference on learning analytics and knowledge, pp. 83–92.

[27] Salih, A.A. and Abdulrazzaq, M.B. (2023) 'Cyber security: performance analysis and challenges

for cyber attacks detection', Indonesian Journal of Electrical Engineering and Computer Science, 31(3), pp. 1763–1775. Available at: https://www.academia.edu/download/105081342/17588.pdf.

[28] Samariya, D. and Thakkar, A. (2023) 'A comprehensive survey of anomaly detection algorithms', Annals of Data Science, 10(3), pp. 829–850.

[29] Sarker, I.H. (2021) 'Machine learning: Algorithms, real-world applications and research directions', SN computer science, 2(3), p. 160.

[30] Scalabrin Bianchi, I., Dinis Sousa, R. and Pereira, R. (2021) 'Information technology governance for higher education institutions: A multi-country study', in Informatics. MDPI, p. 26.

[31] Scott, W.R. (2017) 'Institutional theory: Onward and upward', The Sage handbook of organizational institutionalism, 900, pp. 853–871.

[32] Shahana, A. et al. (2024) 'AI-driven cybersecurity: Balancing advancements and safeguards', Journal of Computer Science and Technology Studies, 6(2), pp. 76–85.

[33] Slade, S. and Prinsloo, P. (2013) 'Learning analytics: Ethical issues and dilemmas', American Behavioral Scientist, 57(10), pp. 1510–1529.

[34] Teng, M. (2010) 'Anomaly detection on time series', in 2010 IEEE International Conference on Progress in Informatics and Computing. IEEE, pp. 603–608.

[35] Ullah, F. et al. (2019) 'Cyber security threats detection in internet of things using deep learning approach', IEEE access, 7, pp. 124379–124389.

[36] Xiong, W. et al. (2014) 'Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications', Information Sciences, 258, pp. 403–415.

[37] Zeng, H. et al. (2024) 'Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity', Journal of Innovation & Knowledge, 9(4), p. 100601.