

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.casjournal.org/index.php/CAJMTCS/

Volume: 08 Issue: 01 | January 2027 ISSN: 2660-5309

Article

From Cloud Complexity to Intelligent Cyber Resilience Through AI-Powered Defense and Strengthened Digital Governance

Zarin Tasnim Raisa[1]*

1. Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh.
* Correspondence: zarin.tasnim.raisa1@gmail.com

Abstract: The rapid adoption of cloud computing and artificial intelligence (AI) is transforming cybersecurity governance while introducing complex challenges in accountability, risk management, and digital operational resilience. This review examines the intersection of cloud governance and AI-driven cyber defense, focusing on emerging security vulnerabilities, shared responsibility, regulatory compliance, and strategies for strengthening digital infrastructure. It explores accountability gaps among cloud service providers, customers, developers, and third-party vendors, alongside AI-specific threats, including data poisoning, adversarial manipulation, prompt injection, unauthorized access, and model exploitation. The review also highlights the growing role of AI in enhancing cybersecurity operations through intelligent threat detection, behavioral analysis, anomaly identification, contextual alert prioritization, and accelerated incident response. Furthermore, it evaluates the implications of the European Union's NIS 2 Directive and Digital Operational Resilience Act (DORA) for organizational accountability, ICT risk management, incident reporting, and business continuity. Key protective strategies include lifecycle-based risk assessment, secure-by-design architecture, least-privilege access control, continuous security monitoring, vulnerability testing, model validation, and comprehensive incident response and recovery planning. The findings emphasize that AI-enabled cybersecurity cannot rely solely on automated decision-making; rather, effective protection requires transparent governance, clearly defined responsibilities, continuous human oversight, and coordinated organizational controls. Integrating regulatory frameworks with intelligent defense mechanisms and proactive resilience strategies is essential for mitigating evolving cyber threats and ensuring the confidentiality, integrity, and availability of interconnected digital infrastructures.

Keywords: Cloud Governance; AI Driven Defense; Cybersecurity Risk; Accountability; Digital Resilience.

Citation: Raisa, Z. T. From Cloud Complexity to Intelligent Cyber Resilience Through AI-Powered Defense and Strengthened Digital Governance. Central Asian Journal of Mathematical Theory and Computer Sciences 2027, 8(1), 61-72.

Received: 07th Aug 2026
Revised: 08th Sep 2026
Accepted: 55th Oct 2026
Published: 10th Nov 2026

Copyright: © 2027 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

In the era of on-demand cloud computing and automation, cloud governance and AI-assisted cybersecurity are increasingly critical. The shared responsibility model requires clear security accountability between cloud providers and customers. However, ownership gaps can emerge, while AI-driven security introduces challenges, including false positives, adversarial attacks, and insufficient human oversight [1]. Cloud computing has changed the way that companies provision and manage their computing resources to both scale and speed. Cloud services are different to traditional data centres, because they offer computing and storage as services on demand, resources can be created and removed through automated processes. This has reduced the suitability of traditional governance

methods that rely on manual processes and infrastructure limitations for the needs of modern operations [2]. Consequently, organizations have adapted their policies and procedures to address the specific configuration, access, and operational requirements of cloud services. Cloud governance has evolved into a comprehensive framework for managing cloud environments and associated risks. It encompasses security, regulatory compliance, operational reliability, and cost management through defined policies, processes, and controls. While security governance focuses on encryption, identity management, and network access, broader governance also addresses resource provisioning, data residency, and continuous compliance monitoring [3]. The shared responsibility model clearly defines the security and compliance obligations of cloud service providers and customers according to the services adopted. Meanwhile, the integration of artificial intelligence (AI) into cybersecurity offers significant opportunities while introducing new governance challenges. AI-driven systems enhance threat detection, alert prioritization, anomaly identification, and incident response. However, their effectiveness depends on reliable data, appropriate governance, and seamless integration with existing security infrastructures. False positives, false negatives, adversarial attacks, and excessive reliance on automated decisions may undermine overall security and compliance [4]. These concerns are not only applicable to individual tools, but also apply to third party models, data sources and application programming interfaces. Lifecycle governance is therefore required to further risks from the organizational and supply chain perspectives as well as system performance. Clear accountability across organisations, suppliers and AI lifecycle – essential for effective governance. Additional binding requirements that cover cybersecurity and operational resilience are the NIS 2 Directive of the European Union and the Digital Operational Resilience Act (DORA); the voluntary NIST AI Risk Management Framework offers guidance on managing risks associated with AI [5]. These instruments cover similar, but separate responsibilities. Responsible people need the power, resources and know-how to question and/or halt automated processes. Misconfiguration, too much access, reliance on supply chain and attacks on AI systems are also security concerns. These risks need a multi-layered approach to security controls, ongoing monitoring, frequent testing, and a plan in place for dealing with an incident and for recovery [6]. AI support to defence should be used in addition to existing security practices and not as a replacement for human judgment or existing controls.

2. Materials and Methods

2.1 Governance, Accountability, and Human Oversight in AI Driven Cloud Infrastructures

Good governance for cloud and AI enabled systems requires clarity of accountability, transparency and the ability to maintain human oversight while adhering to organisational policies. In the financial sector the Digital Operational Resilience Act (DORA) puts the management body ultimately responsible for the information and communication technology (ICT) risk management framework of the entity [7]. Overall, AI governance sets a precedent by shifting the role of risk management from a technical and ethical concern to one of the organization's responsibilities, involving senior leaders in the oversight of the AI lifecycle and beyond, taking into account technical, ethical, and societal implications. To establish meaningful AI oversight, they must assign individuals with the power and resources to intervene in AI-driven processes, along with the necessary information and data [8]. This can include over-riding, pausing or stopping a system where the output or operation of the system are deemed to be an unacceptable risk. There are also feedback loops that need to be in place to fine-tune models and keep a transparent log of decisions made using AI. Within organizations, accountability can be allocated across the AI lifecycle. The developers will document the accuracy, fairness and limitations of the model, and the platform operators will set up and test the systems [9].

2.2 Emerging Cybersecurity Risks and Vulnerabilities in Cloud and AI Driven Digital Infrastructures

Cybersecurity threats include threats to information system confidentiality, integrity, and availability. These risks can include anything from the malicious, the human, the software, the supply chain, the infrastructure, the fire, the flood, the trespasser, and everything in between [10]. The NIS 2 Directive is consistent with the broader all hazards concept in that it calls on organisations to respond to incidents that could affect a function or services they offer, whether intentional or unintentional. Traditional intrusion detection systems that rely on rules and/or signatures can detect known patterns of malicious activity. Their reliance on pre-defined rules and signatures, however, can hinder them from identifying new or changing, or more advanced attacks (Figure 1). That's why it's critical to monitor it continuously, especially when there are often changes to configurations, permissions and workloads in cloud environments [11]. If these are undetected or uncorrected, systems can be exposed to unauthorized access and exploitation due to misconfigurations and deviations from approved security baselines. Cloud security risks are also influenced by the shared responsibility model. The underlying infrastructure is typically protected by the cloud service provider, but the data, applications, configurations and access controls are the responsibility of the customer (Table 1) [12]. But this is going to vary on the basis of the kind of cloud service that's being used. Lack of clarity may result in serious security holes, especially if customers believe that the security of the application programming interface (API) and least privilege access has been set up by their providers. As cloud environments continue to change, automated security monitoring and checks can help detect unwanted policy changes, too many permissions, unauthorized changes and configuration issues. But regular security evaluations, responsibilities clearly assigned and timely corrective action is needed to support automated detection [13]. To minimize cybersecurity risks and ensure the confidentiality, integrity and availability of cloud based systems, a coordinated effort involving technical, organizational and continuous monitoring measures is needed.

Table 1. Governance, Accountability, and Cybersecurity Risks in Cloud and AI Driven Infrastructures

Governance or risk domain	Key issues	Key measures	References
Cloud governance	Unclear security responsibilities among cloud providers, customers, developers, and suppliers	Define ownership of security controls, data protection, and infrastructure management	[12, 34, 37]
AI accountability	Unclear responsibility for automated security decisions and model failures	Assign lifecycle accountability, document model limitations, and establish human intervention mechanisms	[9, 35, 37]
Regulatory compliance	Increasing requirements for cybersecurity risk management, incident reporting, and operational resilience	Align governance procedures with applicable regulatory requirements and organizational risk assessments	[38, 39]

Governance or risk domain	Key issues	Key measures	References
Cloud misconfiguration	Excessive permissions, insecure interfaces, and unauthorized configuration changes	Apply least privilege, continuous monitoring, and automated configuration checks	[6, 13, 21]

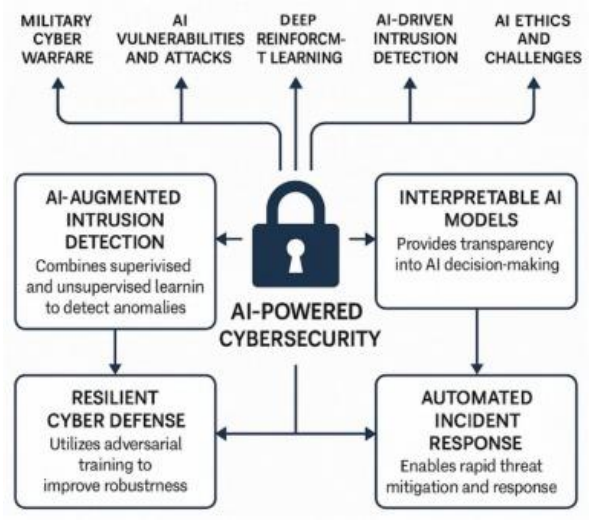


Figure 1. AI-powered cybersecurity components, core capabilities, and application domains [46].

2.3 AI Assisted Cyber Defense, Intelligent Threat Detection, and Automated Security Operations

AI in Cyber Defense utilizes machine learning and automation to detect suspicious activity, prioritize security alerts, and aid in incident response. Behavior based approaches set a pattern for users, devices, or other entities and then determine if there are deviations from that pattern that could signal something malicious, such as logging in from a different location or accessing the data in a different way [14]. Unsupervised anomaly detection can be used to detect events that are not known to be attacks or events that are not previously labeled as an attack, and hybrid approaches can merge known attack indicators and techniques that detect new attacks. From this, AI can enhance the efficiency of security operations centres (SOCs) by allowing security teams to sort through alerts based on context and severity, instead of regarding all alerts as equal (Table 2) [15]. For instance, if the critical production server shows suspicious activity, it might be more important to deal with than a similarly suspicious activity on a low risk testing server. Behaviours, coupled with threat intelligence, can also elevate the priority of an unfamiliar network connection if there is further evidence that the connection may be malicious. Other uses range from attack path visualization, predictive analytics, and automated collection of forensic evidence to aid investigations and speed security analysis [16]. These features work best when they are part of a multi-layered cybersecurity approach, not an alternative to traditional security solutions. While traditional detection systems are effective for recognizing known threats, AI and machine learning can assist in detecting new, more complex, or less apparent attack patterns. These strategies can be used in combination to enhance detection timeliness, accuracy, and vulnerability in a dynamic threat landscape [17]. AI-based defence systems are not without their drawbacks. Adversaries may manipulate input data to compromise model logic, exploit vulnerabilities, or adapt their tactics to evade detection. As attack patterns evolve and operating environments change, model performance may deteriorate. Therefore, continuous monitoring, regular updates, rigorous validation, and ongoing feedback from cybersecurity experts are essential to maintaining effectiveness and resilience [18]. Explainable outputs and human oversight

enable analysts to assess automated recommendations, question dubious decisions, and hold accountable when audited and investigated concerning security incidents. However, it is important that organizations still have the responsibility to set up agent permissions, check and ensure human oversight, incident response plans, and accountability. Combining intelligent detection, traditional security measures, ongoing assessment, and intuitive decision making by humans is essential to effective AI-driven cybersecurity [19].

Table 2. AI Driven Cyber Defense, Risk Reduction, and Operational Resilience Strategies

Strategic domain	Key practices	Expected contribution	References
Intelligent threat detection	Behavioral analysis, anomaly detection, and hybrid detection approaches	Identification of unusual activities and emerging attack patterns	[14, 15, 17]
Automated security operations	Context based alert prioritization, attack path visualization, and automated forensic evidence collection	Improved security analysis and faster incident response	[15, 16]
Risk assessment and prioritization	Evaluate threats according to likelihood, impact, urgency, and organizational risk tolerance	More effective allocation of cybersecurity resources	[20, 24]
Access control and security segmentation	Least privilege, access control lists, network segmentation, and monitoring of nonhuman identities	Reduced unauthorized access and containment of potential attacks	[21, 22]
Security testing and validation	Vulnerability assessments, penetration testing, red teaming, and threat modeling	Identification of system weaknesses and improved defensive controls	[23, 26]

2.4 Cybersecurity Risk Reduction, Preventive Measures, and Operational Security Controls

Risk reduction is a crucial component of a comprehensive strategy for addressing uncertainty in AI-powered systems and digital infrastructure. There are several ways to deal with risks once they have been identified – risk avoidance, risk reduction, risk transfer and risk acceptance. Risk avoidance is the elimination of applications that pose unacceptable risks, and risk reduction is using technical or procedural controls to reduce potential risks [20]. Risk transfer can be done by insurance or contract, while risk acceptance is done by formally acknowledging the risks within defined organizational boundaries. When prioritizing, you should take into account potential impact, likelihood, urgency and organizational risk tolerance to make sure that resources are focused on the highest order threats. Operational security controls are required to reduce the risk of access to critical resources by third parties. The principle of least privilege should be used to ensure that users, applications and automated systems are assigned only those privileges necessary for their functions [21]. Access control lists can help limit access and network segmentation can help separate AI systems and other critical infrastructure, reducing the potential impact of any attacks. When considering effective permissions, check for permissions that have been granted on the basis of groups or roles, or by permission boundaries, as well as permissions that have been directly assigned to the user. Service

accounts, non-human identities, are essential to be inventoried, owned, expired and monitored, otherwise, access to these identities could continue, unnecessarily [22]. Dynamic access controls can also modify privileges based on real time risk assessments, and ongoing monitoring will determine if there are any unusual movements or unauthorized changes. Testing and evaluation are also crucial steps in the identification of weaknesses across the entire AI system lifecycle. Security controls should be tested for their function and effectiveness through vulnerability assessments, penetration testing and compliance testing (Figure 2). Red teaming and threat modelling can help to simulate a potential attack, look for weaknesses in the system, and determine the effectiveness of current defenses [23]. The results of these activities should be used to enhance technical security, organizational policies and governance issues. Ongoing oversight needs to be conducted to keep track of new security risks, breakdowns in operations, and ethical issues. Effectiveness of risk management can be measured by the percentage of risks identified that are then mitigated, the number and severity of incidents, the time it takes to implement security controls and the percentage of those that complied with security procedure [24]. Another critical aspect of operational resilience is incident response planning. Effective response plans should have procedures in place to respond to security incidents promptly, contain them and minimise their impact. Containment can be achieved by isolating affected systems to avoid the further compromise, followed by remediation and recovery through the verified backup or clean infrastructure snapshots [25]. Testing of restored systems should be conducted in an appropriate manner prior to returning to normal operations to validate that vulnerabilities have been resolved and integrity of the system maintained. Frequent training and exercises, such as tabletop drills and red team exercises, can enhance coordination and contribute to the assessment of readiness for various incident scenarios. By combining risk prioritization, access control, ongoing testing, incident response, and recovery planning, organizations can develop a holistic strategy for managing cybersecurity risks and ensuring resilience in AI-powered digital environments [26].

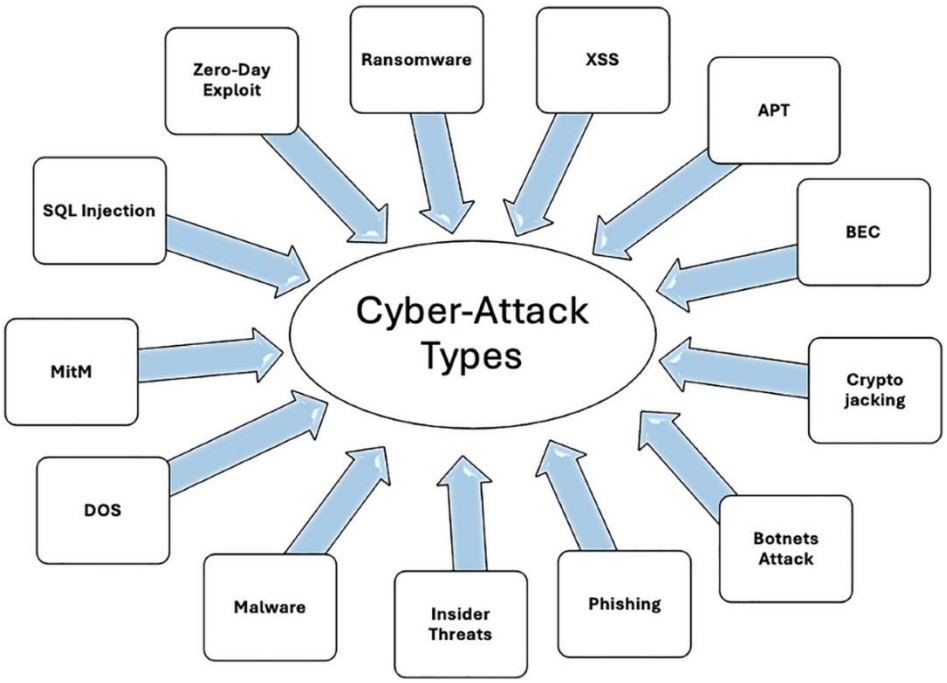


Figure 2. Taxonomy and classification of primary cyber-attack types [47].

2.5 Digital Operational Resilience, Business Continuity, and Cybersecurity Recovery Strategies

Digital resilience is the ability of an organisation to continue or resume its critical services if its information and communication technology (ICT) systems are disrupted. The Digital Operational Resilience Act (DORA) harmonizes and enhances the ICT risk

management obligations contained in different EU sectoral rules for the financial sector [27]. The main goal is to help financial institutions resist, react to, and recover from disruption to their ICT systems and contribute to the stability of the financial system. DORA also strengthens resolution planning under the Bank Recovery and Resolution Directive by mandating maintaining the operational continuity of institutions during resolution processes. ICT resilience can thus be used to inform the testing of whether critical functions can continue to operate in insolvency conditions [28]. DORA does not require certification to ISO 27001 nor the use of the NIST Cybersecurity Framework (NIST CSF) but the principles and controls within the NIST CSF may be used to complement DORA. ISO 27001 also has some overlaps with NIST CSF areas involving ICT risk management, such as NIST CSF Detect, Respond, and Recover which have appropriate methods to incident management and service restoration [29]. The European Systemic Risk Board also has a pan European framework for the coordination of the handling of systemic cyber incidents proposed for adoption at the European level, which is based on DORA and complements existing financial and cybersecurity coordination frameworks such as the NIS 2 Directive and the Critical Entities Resilience Directive. Comprehensive disaster recovery plans, crisis communication plans and effective backup and recovery processes are essential to effective resilience planning [30]. But recovery plans can fall short if testing is infrequent or impossible, people are under-trained, or insufficient resources are dedicated to backing up data, replicating it, and putting up infrastructure quickly. Therefore, regular and comprehensive exercises, including unannounced exercises, are essential to assess preparedness of organisations. Exercises and real-life incidents should be used to identify lessons, which should be taken into account when developing new recovery procedures, and capacity planning and cost-benefit analysis can be used to allocate resources to ensure operational continuity [31].

3. Results and Discussion

Artificial Intelligence (AI) has transformed the landscape of cloud governance and cybersecurity, revolutionizing the way digital infrastructures are managed, secured, and monitored. Traditional governance models were mostly based on human decision making, pre-defined security policies and pre-established operational procedures [32]. As we move from traditional manual networks to automated systems, interdependent cloud networks and AI-powered security solutions, however, new accountability, risk management and operational resilience demands have emerged. While AI can enhance threat detection, speed up incident response, and optimize the handling of intricate digital landscapes, it also presents risks that are hard to mitigate using traditional cybersecurity measures [33]. The biggest hurdle is creating governance frameworks that can manage AI's automated decisions, who is responsible for them, and managing them effectively across the AI lifecycle. Cloud governance is the organisational and technical structure by which the management of digital resources, information systems and security responsibilities are managed. In distributed environments, responsibilities are often split among Cloud Service Providers, customers, software developers and external suppliers [34]. This can lead to accountability issues, especially with interdependent systems failing down the road. While cloud providers may be responsible for the general infrastructure, customers are responsible for other areas of data protection, access control, configuration, and application security. AI's inclusion introduces an additional layer of complexity, as it could impact decisions that were previously taken by security experts. Responsibility should not only be assigned for infrastructure and data management, but also for the creation, deployment, monitoring and decision making of the AI models [35]. There should therefore be defined ownership, decision-making, escalation and human intervention mechanisms in governance arrangements. Accountability is especially critical when automated systems are applied in environments where security is a critical issue. AI models can detect unusual activities, classify potential threats, prioritise alerts and

recommend defensive actions. But they can misclassify an incomplete training set, be misled by biased training classes, fail on unexpected inputs, or be unfitted for use by changes in the operating conditions [36]. If an automated recommendation is mistaken, it can be challenging to define who's responsible for the security decision, if anyone, unless proper governance processes are in place. When multiple organisations are involved in developing and operating an AI powered service, the challenge is exacerbated. Contractual responsibilities, technical documentation, audit mechanisms and ongoing performance evaluation are, therefore, necessary to ensure accountability across organisational boundaries [37]. The growing number of laws and regulations shows that cyber security governance is increasingly becoming an organisational matter and not just a technical one. Regulatory requirements, such as the NIS 2 Directive from the European Union and the Digital Operational Resilience Act, set out expectations on risk management, incident reporting, supplier management and operational resilience [38]. The requirements are especially applicable to organisations running complex digital infrastructures as issues can arise from a third party service provider, interdependent systems or security process failures within the organization. DORA reinforces the focus on digital operational resilience in the financial industry and NIS 2 expands the scope of cybersecurity requirements to include essential and important entities. They demonstrate the importance of documented governance processes, robust risk assessment, incident management facilities and suitable management of external dependencies [39]. However, this does not ensure that the business is properly protected from Cyber Security. Regulatory demands normally outline the least requirements while new threats to AI can evolve much quicker than the legislation can. Organisations need to therefore translate legal obligations into operational controls that are applicable to their specific technological environments. International standards or industry guidance may also assist this process by providing a structured approach to information security management, risk assessment, system validation and ongoing improvements [40]. Cybersecurity and AI risks can be identified and mitigated through system development and deployment with the help of frameworks like NIST guidance. The effectiveness of these frameworks, however, is dependent on their implementation, buy-in and re-evaluation. Cloud environments are also becoming more complex, relying on interconnected apps, APIs, automated workflows, and service providers, introducing a new layer of cybersecurity threats [41]. A vulnerability in one element can provide entry points to another system or allow access to multiple systems. Examples of important exposure points are misconfigured cloud resources, insecure interfaces, compromised credentials, inadequate access restrictions, and insufficient monitoring. Adversarial inputs, data poisoning, model exploitation, and prompt injection are all ways that behavior can be compromised, introducing new risks to AI systems. These risks can impact the accuracy of model results and can give malicious actors an opportunity to manipulate automated systems. When such safeguards are not implemented, prompt injection may cause an AI system to misinterpret instructions from malicious inputs and result in information being disclosed or actions being taken that were not intended [42]. But there's also an issue with potential misuse of AI. While AI can assist in defensive measures, other technologies could also be used to enable malicious operations such as creating deceptive content, social engineering, and automating attack processes. The dual use aspect makes cybersecurity governance difficult, as the same technology could be used in a beneficial security role but also for malicious reasons. Organisations need to assess both the technical capabilities of AI systems and their potential misuse as well as access to the systems and threats from outside the organization [43]. The deployment strategies should include appropriate restrictions, usage monitoring, secure development practices, and incident response procedures. It should be the goal to put AI tools to use in a safe and ethical manner with well-defined boundaries. With frameworks like DORA, the implementation of resilience requirements highlights the need for cyber security and wider organisational risk management. Digital disruptions can impact on the availability of services, financial stability, customers' confidence and on-

going operations [44]. Hence, senior management, technical teams, compliance functions and external service providers need to be considered in the process of resilience planning. The role of suppliers is especially critical as they can have a detrimental impact on the security and availability of services that an organisation does not directly own [45]. The following processes can ease these dependencies: regular assessments, contractual safeguards, incident notification procedures, contingency plans. Resilience testing should also be carried out to assess if systems and/or organisations will be able to adapt effectively to realistic scenarios of disruption. Overall, cloud governance, AI-driven defense, cybersecurity risk management, and operational resilience can be seen as a governance challenge that are linked together.

4. Conclusion

Effective cybersecurity in automated digital infrastructures requires the integration of cloud governance, AI driven defense, accountability, and operational resilience. Although AI strengthens threat detection, security monitoring, and incident response, its adoption introduces risks involving data integrity, system manipulation, unauthorised access, and unclear responsibility. Regulatory frameworks and established security standards provide essential guidance, but continuous oversight and practical implementation remain necessary. Human supervision, secure system design, controlled automation, and supplier accountability should therefore be prioritised. Ultimately, sustainable digital security depends on aligning technological innovation with transparent governance, proactive risk management, and tested resilience strategies to protect critical services against evolving cyber threats.

REFERENCES

[1] S. Ibeneme, J. Okeibunor, D. Muneene, I. Husain, P. Bento, C. Gaju, B. Housseynou, M. Chibi, H. Karamagi, and L. Makubalo, "Data revolution, health status transformation and the role of artificial intelligence for health and pandemic preparedness in the African context," *BMC Proc.*, vol. 15, p. 22, 2021, doi: 10.1186/s12919-021-00228-1.

[2] C. A. Abdullah and M. J. I. Ridoy, "Artificial intelligence-driven cyber threat detection for protecting critical digital infrastructure," *Innov.: Int. Multidiscipl. J. Appl. Technol.*, vol. 1, no. 2, pp. 76–83, 2023, doi: 10.51699/zb8kwv06.

[3] O. S. Owolabi, P. C. Uche, N. T. Adeniken, C. Ihejirika, R. B. Islam, and B. J. T. Chhetri, "Ethical implication of artificial intelligence (AI) adoption in financial decision making," *Comput. Inf. Sci.*, vol. 17, no. 1, p. 49, 2024, doi: 10.5539/cis.v17n1p49.

[4] A. Schreiber and I. Schreiber, "AI for cyber-security risk: Harnessing AI for automatic generation of company-specific cybersecurity risk profiles," *Inf. Comput. Secur.*, vol. 33, pp. 520–546, 2025, doi: 10.1108/ICS-08-2024-0177.

[5] V. Capraro, A. Lentsch, D. Acemoglu, S. Akgun, A. Akhmedova, E. Bilancini, J.-F. Bonnefon, P. Brañas-Garza, L. Butera, K. M. Douglas, *et al.*, "The impact of generative artificial intelligence on socioeconomic inequalities and policy making," *Proc. Natl. Acad. Sci. USA Nexus*, vol. 3, p. pgae191, 2024, doi: 10.2139/ssrn.4666103.

[6] A. T. Shama and A. Biswas, "Cloud Misconfiguration as a Governance Failure in AI-Enabled Healthcare and Finance with Privacy Risk Implications," *International Journal on Economics, Finance and Sustainable Development*, vol. 5, no. 1, pp. 208–214, 2023. doi: 10.31149/ijefsd.v5i1.5799.

[7] O. J. Gstrein, N. Haleem, and A. Zwitter, "General-purpose AI regulation and the European Union AI Act," *Internet Policy Rev.*, vol. 13, pp. 1–26, 2024, doi: 10.14763/2024.3.1790.

[8] D. Flonk, M. Jachtenfuchs, and A. Obendiek, "Controlling internet content in the EU: Towards digital sovereignty," *J. Eur. Public Policy*, vol. 31, pp. 2316–2342, 2024, doi: 10.1080/13501763.2024.2309179.

[9] J. Pohle and T. Thiel, "Digital sovereignty," *Internet Policy Rev.*, vol. 9, pp. 1–19, 2020, doi: 10.14763/2020.4.1532.

[10] Y. Chen and P. Esmaeilzadeh, "Generative AI in medical practice: In-depth exploration of privacy and security challenges," *J. Med. Internet Res.*, vol. 26, p. e53008, 2024, doi: 10.2196/53008.

[11] J. Mökander, J. Morley, M. Taddeo, and L. Floridi, "Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations," *Sci. Eng. Ethics*, vol. 27, p. 44, 2021, doi: 10.1007/s11948-021-0031-4.

[12] C. A. Abdullah and M. J. I. Ridoy, "ARTIFICIAL INTELLIGENCE DRIVEN INFRASTRUCTURE SECURITY ENHANCING CYBERSECURITY AND PROTECTING NATIONAL SECURITY SYSTEMS", IPTEKS, vol. 1, no. 3, pp. 191–200, Jul. 2024. 2.doi: 10.61796/ipteks.v1i3.498.

[13] L. Weidinger, J. Uesato, M. Rauh, C. Griffin, P.-S. Huang, J. Mellor, A. Glaese, M. Cheng, B. Balle, A. Kasirzadeh, *et al.*, "Taxonomy of risks posed by language models," in *Proc. 2022 ACM Conf. Fairness, Accountability, and Transp. (FAccT '22)*, New York, NY, USA, 2022, pp. 214–229, doi: 10.1145/3531146.3533088.

[14] M. H. Chin, N. Afsar-Manesh, A. S. Bierman, C. Chang, C. J. Colón-Rodríguez, P. Dullabh, D. G. Duran, M. Fair, T. Hernandez-Boussard, M. Hightower, *et al.*, "Guiding principles to address the impact of algorithm bias on racial and ethnic disparities in health and health care," *JAMA Netw. Open*, vol. 6, p. e2345050, 2023, doi: 10.1001/jamanetworkopen.2023.45050.

[15] J. Ayling and A. Chapman, "Putting AI ethics to work: Are the tools fit for purpose?" *AI Soc.*, vol. 8, pp. 405–429, 2022, doi: 10.1007/s43681-021-00084-x.

[16] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023, doi: 10.1109/ACCESS.2023.3300381.

[17] M. M. Hossain and A. T. Shama, "GRC Accountability Gap in AI and Cloud Security: Limitations of Automated Compliance and Risk Control Mechanisms," *International Journal on Orange Technologies*, vol. 7, no. 1, pp. 56–63, 2025. doi: 10.31149/ijot.v7i1.5798.

[18] K. Wach, C. D. Duong, J. Ejdys, R. Kazlauskaitė, P. Korzynski, G. Mazurek, J. Paliszkiewicz, and E. Ziemba, "The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT," *Entrep. Bus. Econ. Rev.*, vol. 11, pp. 7–29, 2023, doi: 10.15678/EBER.2023.110201.

[19] Y. Zhou, T. Ni, W. B. Lee, and Q. Zhao, "A survey on backdoor threats in large language models (LLMs): Attacks, defenses, and evaluations," *arXiv preprint*, arXiv:2502.05224, 2025, doi: 10.53941/tai.2025.100003.

[20] P. O. Shoetan, O. O. Amoo, E. S. Okafor, and O. L. Olorunfemi, "Synthesizing AI's impact on cybersecurity in telecommunications: A conceptual framework," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 594–605, 2024, doi: 10.51594/csitrj.v5i3.908.

[21] M. J. I. Ridoy and A. Akhir, "Smart transportation solutions using AI to optimize traffic flow and reduce urban congestion for improved urban mobility," *Int. J. Orange Technol.*, vol. 7, no. 2, pp. 116–123, 2025, doi: 10.31149/ijot.v7i2.5707.

[22] Y. Walter, "Embracing the future of artificial intelligence in the classroom: The relevance of AI literacy, prompt engineering, and critical thinking in modern education," *Int. J. Educ. Technol. High. Educ.*, vol. 21, p. 15, 2024, doi: 10.1186/s41239-024-00448-3.

[23] R. Raman, R. M. Kowalski, K. Achuthan, A. Iyer, and P. Nedungadi, "Navigating artificial general intelligence development: Societal, technological, ethical, and brain-inspired pathways," *Sci. Rep.*, vol. 15, p. 8443, 2025, doi: 10.1038/s41598-025-92190-7.

[24] H. Liu, W. Wang, H. Sun, C. X. Tian, C. Kong, X. L. Dong, and H. Li, "Unraveling the mechanics of learning-based demonstration selection for in-context learning," in *Proc. 63rd Annu. Meet. Assoc. Comput. Linguist. (ACL)*, vol. 1, Vienna, Austria, 2025, pp. 2623–2641, doi: 10.18653/v1/2025.acl-long.132.

[25] A. T. Shama, "Evolution of Software-Defined Networking in Enterprise and Service Provider Networks: Opportunities, Challenges, and Future Directions," *Central Asian Journal of Mathematical Theory and Computer Sciences*, vol. 3, no. 7, pp. 75–83, 2022.

[26] N. Chukwurah, A. B. Ige, V. I. Adebayo, and O. G. Eyieyien, "Frameworks for effective data governance: Best practices, challenges, and implementation strategies across industries," *Comput. Sci. IT Res. J.*, vol. 5, no. 7, pp. 1666–1679, 2024, doi: 10.51594/csitrj.v5i7.1351.

[27] S. M. Varnosfaderani and M. Forouzanfar, "The role of AI in hospitals and clinics: Transforming healthcare in the 21st century," *Bioengineering*, vol. 11, p. 337, 2024, doi: 10.3390/bioengineering11040337.

[28] R. J. Torraco, "Writing integrative literature reviews: Guidelines and examples," *Hum. Resour. Dev. Rev.*, vol. 4, pp. 356–367, 2005, doi: 10.1177/1534484305278283.

[29] T. Birkstedt, M. Minkkinen, A. Tandon, and M. Mäntymäki, "AI governance: Themes, knowledge gaps and future agendas," *Internet Res.*, vol. 33, pp. 133–167, 2023, doi: 10.1108/INTR-01-2022-0042.

[30] J. Thomas and A. Harden, "Methods for the thematic synthesis of qualitative research in systematic reviews," *BMC Med. Res. Methodol.*, vol. 8, p. 45, 2008, doi: 10.1186/1471-2288-8-45.

[31] M. J. I. Ridoy and C. A. Abdullah, "AI-driven threat intelligence and cybersecurity performance in US organizations: Examining the roles of adoption, system complexity, and workforce expertise," *Bus. Soc. Sci.*, vol. 1, no. 1, pp. 1–18, 2021, doi: 10.25163/business.1110777.

[32] A. Dafoe, *AI Governance: A Research Agenda*, Oxford, UK: Governance of AI Program, Future of Humanity Inst., Univ. of Oxford, 2018.

[33] H. Canton, "Organisation for Economic Co-operation and Development—OECD," in *The Europa Directory of International Organizations 2021*, Abingdon, UK: Routledge, 2021, pp. 677–687, doi: 10.4324/9781003179900-102.

[34] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nat. Mach. Intell.*, vol. 1, pp. 389–399, 2019, doi: 10.1038/s42256-019-0088-2.

[35] S. McLennan, A. Fiske, D. W. Tigard, R. Müller, S. Haddadin, and A. Buyx, "Embedded ethics: A proposal for integrating ethics into the development of medical AI," *BMC Med. Ethics*, vol. 23, p. 6, 2022, doi: 10.1186/s12910-022-00746-3.

[36] A. T. Shama, "AI Governance Challenges in Banking: Model Explainability, Regulatory Compliance, and the Limits of Traditional Risk Management," *Business and Social Sciences*, vol. 3, no. 1, pp. 1–10, 2025. doi: 10.25163/business.3110901.

[37] M. Mantymaki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Defining organizational AI governance," *AI Ethics*, vol. 2, pp. 603–609, 2022, doi: 10.1007/s43681-022-00143-x.

[38] E. Zaidan and I. Ibrahim, "AI governance in a complex and rapidly changing regulatory landscape: A global perspective," *Humanit. Soc. Sci. Commun.*, vol. 11, p. 511, 2024, doi: 10.1057/s41599-024-03560-x.

[39] P. Hacker, A. Engel, and M. Mauer, "Regulating ChatGPT and other large language AI models: Challenges and prospects," in *Proc. 2023 ACM FAccT Conf.*, New York, NY, USA, 2023, pp. 1112–1123, doi: 10.1145/3593013.3594067.

[40] R. Putchakayala and R. Yallavula, "The Intelligent Governance Core: A Multi-Layer AI Framework for Predictive Compliance and Autonomous Digital Analytics," *Int. J. AI BigData Comput. Manag. Stud.*, vol. 6, pp. 171–179, 2025, doi: 10.63282/3050-9416.IJAIBDCMS-V6I1P117.

[41] M. J. I. Ridoy and A. Islam, "Integrating machine learning into financial systems to improve risk management and economic stability," *J. Knowl. Learn. Sci. Technol.*, vol. 4, no. 4, pp. 119–126, 2025, doi: 10.60087/jklst.vol4.n4.013.

[42] P. Solanki, J. Grundy, and W. Hussain, "Operationalising ethics in artificial intelligence for healthcare: A framework for AI developers," *AI Ethics*, vol. 3, pp. 223–240, 2023, doi: 10.1007/s43681-022-00195-z.

[43] J. Wang, T. Ni, W. B. Lee, and Q. Zhao, "A contemporary survey of large language model assisted program analysis," *arXiv preprint*, arXiv:2502.18474, 2025, doi: 10.53941/tai.2025.100006.

[44] R. Charow, T. Jeyakumar, S. Younus, E. Dolatabadi, M. Salhia, D. Al-Mouaswas, M. Anderson, S. Balakumar, M. Clare, A. Dhalla, *et al.*, "Artificial intelligence education programs for health care professionals: Scoping review," *JMIR Med. Educ.*, vol. 7, p. e29787, 2021, doi: 10.2196/preprints.31043.

[45] T. S. Afsara and C. Proggo, "Privacy Governance Challenges in AI-Enabled Banking Surveillance Systems: From Compliance to Accountability," *Journal of Knowledge Learning and Science Technology*, vol. 5, no. 2, pp. 131–141, 2026. doi: 10.60087/jklst.vol5.n2.009.

[46] B. Hutchinson, A. Smart, A. Hanna, R. Denton, C. Greer, O. Kjartansson, P. Barnes, M. Mitchell, and E. Denton, "Towards accountability for machine learning datasets: Practices from software engineering and

infrastructure," in *Proc. 2021 ACM FAccT Conf.*, New York, NY, USA, 2021, pp. 560–575, doi: 10.1145/3442188.3445918.

[47] B. C. Cheong, "Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making," *Front. Hum. Dyn.*, vol. 6, p. 1421273, 2024, doi: 10.3389/fhumd.2024.1421273.