Chapter 19

Advanced Materials, Artificial Intelligence, and Sustainable Technologies for Energy and Environmental Engineering
ISBN: 978-9915-704-10-4
DOI: 10.62486/978-9915-704-10-4.ch19
Pages: 310-329

Cybersecurity in AI-enabled Infrastructures

Fuad Abaszadeh[1] ✉, Taleh Asgarov[1], Rashad Ismibayli[2], L.R. Priya[3] ✉, Malikov Ziyodullo Abdurayim[4] ✉, Abduraxmonov Muhammad Sulaymon[4] ✉

[1]National Aviation Academy. Baku, Azerbaijan.

[2]Azerbaijan University of Architecture and Construction. Baku, Azerbaijan.

[3]Electronics and Communication Engineering., Francis Xavier Engineering College. Tirunelveli, India.

[4]Department of Software Engineering, Faculty of Artificial Intelligence and Digital Technologies, Samarkand State University. Uzbekistan.

ABSTRACT

Artificial Intelligence (AI) is now an aspect of advancing future infrastructures because it promises to be more efficient, flexible, and automatized. Tech infrastructures are generally more prone to cyber attacks because AI-enabled infrastructures, including smart grid, smart cities, and smart transportation, are interconnected. Entrenched in the underpinnings of such infrastructures is an amalgamation of IoT, big data and cloud computing, which unleash increased potential attacks and potentials. The critical services can be affected by cybersecurity by endangering their reliability with adversarial attacks, data poisoning, and a denial-of-service. It also uses the AI defense that allows identifying the anomaly, predictive analytics, and automated systems to respond to the incident. The aspects of the AI construct which have been discussed as its radar aspects include the complexities in its facet of transparency and argumentative to manipulative data, yet it poses new problems. Among such examples of case studies that still became a target of sophisticated attacks include energy network, health care and urban infrastructure. To solve out these concerns, researchers are considering the possibility of integrating blockchain and quantum computing technologies into the future with digital twins. These new technologies are associated with the added security and stability. However, AI will not become stagnant because it is not only a possible threat but also an effective means of fighting cybersecurity. Innovation and defence initiatives of a firm are the future of safe infrastructures. Finally, in designing adaptive, resilient and sustainable infrastructure systems, AI informed, adaptive and transparent security frameworks will be adopted.

Keywords: Artificial Intelligence; Cybersecurity; Smart Infrastructures; IoT; Big Data; Cloud Computing; Blockchain; Digital Twins; Quantum Computing.

INTRODUCTION

This has turned AI into one of the most powerful success trends in the major infrastructures. It has infiltrated smart city networks, energy and transportation, and health care networks, and has been more efficient and resilient and responsive. Thanks to the seeming convergence of more and more infrastructures and AI, they, too, are apparently prone to cyberattacks. The Top Percent of the Foundation of the attack surface percentages were 90 percent with 100 percent point of high rate of data transfer and real time decision making. The shift in the threat of the enemy indicates the level of urgency of the need to develop efficient cybersecurity measures. Compared to animeghom, then on the side of the draining actuality, the cyber threats, also, command a wake-up call in the memory of the real material space wherein the societies of such formations were earlier formed. This, in turn, has opportunities and problems of its own because it presents AI into the realm of cybersecurity. On the one hand, AI could identify elaborate fires, intervene within the minimum duration feasible and could be utilized to counter new assaults. On one hand, AI models can be black boxed and hacked, abused and maliciously and maladaptively hacked. The doubling capacity of AI i.e. the thing exists and must bear some degree of responsibility to the harmonization between the safeguard and the innovation. Thus, even this characteristic of the data safety in the AI-led systems has become an object of the controversial list, as to the guarantee of the sustainability and the non-dangerousness of the technological processes. Medical scene has not been the last one to join the wave of implementing the trend to adapt to the utilization of the artificial intelligence to position jobs on the auto shutters and provide more reliable outcomes to the patients. The introduction of the AI into clinical practice proved successful as the hospitals received an opportunity to familiarize themselves with the vision and the plan within the context of air intelligence development.[1] This has not only been achieved by harmonizing the enabling technology technological latency, but also professional health care service providers training the skill-base to be in the forefront of the AI endeavors.[1] It has become an ethical perspective on revolutionizing engineering and materials sciences as well as digital infrastructures because the idea of artificial intelligence (AI) has turned out to be an ethical perspective. It enabled its application not only in smart cities but in health and energy production and production through its predictability and efficiency. The additional available concentrated walls around the surrounding sphere of infrastructures are, nevertheless, contributing incrementally gradually parallel to the contribution of the increase of the smartness intensity of the infrastructure life.[2,3] It is quite understandable that the threats and the opportunities posed by AI make it create such emotion as the need to install even more security equipment. The predictive modeling and the visualization of the high-performance are compared on the examples of the nanomaterials, i.e. the graphene oxide and the carbon nanotubes.[4,5,6,7] Since structural resiliency or material research is a research study, digital resiliency adopts (AI) infrastructures. Introduction makes AI a more distinguishing technology, and more that is needed in the realization of the infrastructure and security generation of the future. Support in AI integration simplifies the working process and here in this respect the rule rule in terms of concentrated time-frames governance and quality control can be executed according to will, the outcome of which is a reorganization of a entire healthcare delivery construct. The strength of AI also extends as far as the lifecycle management of the infrastructure, yet it was civilization engineering underpinnings which broke it. The fixes presented by the adoption of AI technologies intensify the intensive infrastructures, as they strengthen their heavy degree of schedule, cost inertia, and price monitoring during the cycles holidaying the construction.[8] The other AI service unmistakably linked to the construction two sector is the structural health monitoring (SHM) that offers an opportunity to rely on retroversion to any defect and the forecasting of the upkeep that enables expanding of the durability to both its structural property and its stability. So too can the latter perhaps aid in adequately supporting the objective of building efficient cities, yet delivers smart cities thanks to integrated AI and infrastructural building. There is also cloud and edge AI that offers even more scale and responsiveness that will theoretically take advantage in health tracking and patient outcome in the future.[9] The issues of implementation on AI with the old systems, however, are there. The subsequent issues are outlined by Singh in the sense of how the existing structures will transform into the implementations of the real time communication into the AI. He not only disinfects the necessity to achieve the improvements of the outdated systems but also to mitigate the risks and working enactment of operating AI and merits of application AI in the coming decade.[10] It implies also that the business risks in the cloud-based facility will zero on the venture-basis that will be actively personalized on the broader scale, and that the division of the herein goals at the safety status in general i.e. the possibilities of resources expansion with the help of the AI assistance can, in the objective sense, be multiple.[10] The susceptibilities of the Critical National Infrastructures (CNIS) system of the energy, the waters system, and the transport system among others are some of the issues. The electronics which form its infrastructures and which these authors are already starting specifying as core to the current day society and which can and even may be the subject of emerging growth in cybersecurity-related anxieties are not only reinforced by generative AI tech but are also capable of being protected by so-called Critical Infrastructure Protection (CIP).[11] The threats can be alleviated as the development of Large Language Models (LLM) progresses, and their results can be assessed regarding the standards, which have been released as part of the analysis by Yigit et al. These complexes upon each other are so interdependent that there will be no need to sever the connections of a strong AI security in order to prevent the possible attacks under the assumption that they are working with the arrangement in place that networks do, in fact, exist. Another cybersecurity players also offer another form of electronic insurgency. But when it comes to high-performing the performances of the pieces as it is imagined by its creators, the realization of AI, or at least of the processes that are, somehow, still in its infancy, e.g., Generative Adversarial Networks (GANs), is not only encouraging an aura of demonization of the authenticities; it also is not merely trafficking n the propaganda of spreading information into the scene, which contains, it must be noted, some of the most important Web 2.0 machinery.[12] The reputational retribution is perhaps too bad under these circumstances of massive opportunity of multimedia material, the strangulation of genuineness in upshot communications and because of the same reason the importance of a confidential being of a procedure of a forensic of the media and substantiation cannot be cursed. The primary benefit of applying AI as an aspect of road cybersecurity is that it may be activated to prepare bulk of past information and locate faint and recognizable patterns aside within them that can be related to the conduct of the pathogen, especially phishing-capability or malicious behaviors. This will be possible since the intruders will always be motivated to evolve and the AI that represents itself must also possess the ability to respond and PD the attacks at their initial levels.[13] Beyond this, there is explainable AI finding with SHAP and LIME enabling a more objective evaluation of how AI frameworks of cybersecurity capacity allocate and react to danger that would otherwise define a strictness to credit cybersecurity capacity across or even concern itself with. The fallacy of generalizability and prejudice is the first error in the case and the second disadvantage of introducing calls to apply the models of the machine learning (ML) and Deep Learning (DL) in healthcare. The fact they are handled in some of these disadvantages is unethical in nature. The healthcare facilities will need to set up programmers policy-complex to which sticking with technological infrastructure conformity, cost, and such biases into unifying the devices into the, as yet, heterogenous pattern in health care environment conditioned medical examination and treatment practices will add even further layers of distorting to the procedure of diagnosing and treating instruments in patients.[14] The latter is at least a disadvantageous fact, where the ingestion of AI has to balance data feeds in real-time and show breakdowns as a risk to patient safety in the situation of ineffectiveness. Second, the cyber-harmonize pug also threatens the anti-cyber capabilities of our national infrastructures (CNIs), however, data on the digital properties, especially the radiation of modern technology to the employability of AI technologies, harmonizes the labor, is that cyber infrastructures are enduring sinister enemies in the digital realm. Even the fact that there is a threat that actually exists that those AI systems made holes in the infrastructure, and therefore even exceptionally important services, power, water service and communications infrastructure, is also threatened. In the context of safe usage of the machine and learning systems in the critical infrastructure, there must be sufficient preventative mechanisms in the inclusive nature of the periphery of machine learning processes.[15] In addition to that, the conditions under which the effectiveness of AI based strategies may be debated as a subset of the paradigm of the critical infrastructural protection (CIP) frameworks are interjoined with the presence of even more stringent terms of assessment that would involve the physical challenge and the cybersecurity challenge.[11] These systems need susceptibilities and regular exercising to identify and rectify these points in order to become stronger to rectify any sort of assaults. VAD design has filled another vacuum in the health sector by introduction of new technology in the facilitation of better patient outcomes in other ways. One of these insists that decadence between more convenient and modernized VADs is already a trend and is compulsory in the majority of the cases of the occurrences of the heart diseases in the diseased. Suchsyntactic makeup of their equipment and the contemporary surgery can radically shift the propensity of prospects of survival of their heart failure patients as shown by both the studies and Edhen the explanation as to why the new studies appear noteworthy as to such significance in the sphere studies of the cardiac assist technology.[16] The machine machining and precision would also be regarded as part of the technological revolution in the manufacturing improvement. They have been recorded in literature as such machining systems were highly exact and the overall production line more efficient. The ability to continue to exist in the highly altering global environment is already a can-do and a bread-and-rose of production smarter and the smarter drones.

Fundamentals of AI-enabled Infrastructures

Communication systems and transport systems and even energy distribution systems are types of nature that constitute part of the AI-enabled infrastructures. The Internet of Things (IoT), big-data based analytics, cloud computing, and edge computing are also the basis of such infrastructures. The positive implications AI can bring can be seen lowering downtimes due to real time data analysis, preventing complex maintenance systems since the outcome will be automatically decided, and operating many subsystems simultaneously. One of those is smart grids that structure the energy demand and supply it on a dynamic basis within the principles of AI. Similarly, transport can also be optimized using AI-related solutions as they can minimize traffic and decrease congestion (table 1).

Table 1. Fundamentals of AI-enabled Infrastructures

Aspect	Description	AI Role
Core Technologies	Includes IoT, Big Data, Cloud Computing, and Edge Computing as foundational elements	Provides data-driven analysis and automation for infrastructure management
Key Applications	Smart grids, intelligent transport, healthcare systems, and smart cities	Optimizes performance, safety, and adaptive control in critical services
Data Requirements	Massive, high-quality, real-time data streams for AI training and decision-making	Processes large-scale datasets to enable accurate forecasting and mo

The characteristics of such systems are characterized by unceasing data and information exchange and communication between two or more connected devices whose relationships rely on each other. It thus leads to unnecessary formulation of data, which is likely to be investigated in the most skilled and in the safest way. Such dependence on AI does not merely introduce opportunities to resilience but also fresh grounds of weakness, as well. The need to have AI algorithm transparency and trust arise. The good must have justifiable reasons to be overcome by the evils of AI powered infrastructures. These are then based on either a sound security and good governance mixture and good technology development mix. AI has moved even further and has revolutionized in other spheres as well and been more of the manifestations of the abject effects to the contemporary infrastructures and structures. To be accustomed to the existence and content of high levels of AI usage, one must get used to the component of the multi-layered usage of AI on the sphere of health care, floor design, and agricultural energy stability. Furthermore, the value of the crossroad of AI and sustainability lies not merely in the opportunity but also in threats, in the first place, in terms of the governance of the climatic change. Regarding the necessity to create AI-based systems that are more energy efficient, i.e., the inclination to introduce such systems into the sphere of cryptocurrency, is already also already having negative implications at the environmental level as a side effect of implementing energy-consuming systems.[17] Code technology s (IoT, Big Data, Cloud, and Edge computing) are used by AI-enabled infrastructures. These systems encode real time information into action information in order to make a decision concerning the energy, health and transportation. According to the existing analysis of field-specific counterparts known as graphene oxide and CNTs, predictive models can be employed to smarten material activity, and could act as a reference to AI aided material optimization.[18,19] An aeronautical artificial intelligence will only augment efficiency but it will also add complexity and avalanche interoperability to scalability. Smart grids and transportation Infrastructure These constitute the kind of infrastructures that do not just appear to be over-reliant on AI forecasting models, but are also undergo significant consumers of AI forecasting models.[20] Fundamentals consider both the opportunities and the risk of the introduction of AI to the essential things initially. In the defined scenario, an artificial intelligence data center knitting, greener energy, and carbon neutrality will present an opportunity of climate-neutral operation re-introducing the digital infrastructures scene with a new veil of sustainability moving forward. Besides, AI has already entered the agricultural sector as well and discontinued the tradition of employing IFST by making recourse to Internet of things (IoT) technologies. The latter may be characterized as a logical extension of AI implementation by the sphere of smart agriculture, it is precision agriculture that may be asserted to have such Facebook benefits as actual tracking of crops and actual decision making based on raw data.[21] This radicalization is not always what makes the resources deployment simpler, yet the sustainability and feasibility of the agriculture industry, as one of the prevalent uses of AI to stream and refine the efficiencies of my-to-may and seasonal farming management, serve on it. The paradox of the use of AI in the lower-middle-income countries (LMICs) possesses its own concerns. To get deeper insights into the situation, challenges, and mediating factors of AI acceptance in the healthcare (when deployed to diabetes interventions), a study presuppose that the experimental assessment of the immediate environment and existing structures would be carried out on a mass scale.[22] Such variables shall be identified and not only be utilized to replicate AI applications according to modern care delivery models in these areas but also account to priorities in the care of health. On balance, it is possible to say that it is a sophisticated argument in which different sectors in which AI-based infrastructures are discussed, and it assumes the availability of other efficiencies, sustainability, and structural beneficial effects. There will never be a feeling that AI is out of place since AI is still being scaled and is still being stretched to its limits to encompass the areas of the professions as well as taken to any other setting thus there is need to emphasize on the interface between the classical engineering and AI safety structures e.g. Google DeepMind Frontier Safety Framework. Those models might be used to deliver safety operationally credentials of wider thresholds by the critical parameters to the AI systems that would ultimately settle trustworthiness and reliance by the AI usages.[23]

Fundamentals of AI-enabled Infrastructures

In addition to a pragmatic factor, AI-planned infrastructures need to be initiated time-gradedly upon a multitude of mindful domains. Electronic intelligence and digital archduers together with 5G communication make them more flexible and efficient. AI can be used to make water management, waste systems, and environmental observation models in the smart cities. Hospitals have also practiced the use of AI to diagnose and manage certain disease and optimization of some resources. Robots The industry of 4.0 robots has the form of an AI industry. These are quality infrastructures built on the source of the distributed computing environments and performance and complexity is optimized (table 2). Blockchain, 5G communication is defined as the long-range and prevent blocks AI in the digital twin. The breakthroughs are introducing new advances in tracking and prediction systems and performance systems. The healthcare industry is one of the sectors through which the AI-driven data analysis can be implemented; specifically, the patient management facility Penetruk.[24] According to Industry 4.0, one has to streamline the process of manufacturing with the use of IoT and AI.[25] Nonetheless, to be within the avenue of discussion, the publications that analyze nanomaterials and other technologies report also that predictive modeling is also implemented in large scale, e.g., a predictable reality in the infrastructure of the future, yet predictor in that case, is the precise and multi-vagant entity.[26,27,28,29,30] 2 Unsurprisingly, AI is not a free phenomenon, but exists as systems that have acquired digital transformation.

Table 2. Fundamentals of AI-enabled Infrastructures

Aspect	Description	AI Role
Technological Foundation	Built on IoT, Big Data, Edge Computing, Cloud, and 5G networks.	Provides intelligence, automation, and predictive capabilities.
Applications	Smart cities, healthcare, energy, transportation, and Industry 4.0.	Optimizes urban services, energy flow, traffic, and healthcare management.
Data Role	Continuous, large-scale, real-time data is critical for AI decision-making.	Transforms raw data into actionable insights for forecasting and control.
Industrial Integration	Robotics, automation, and predictive maintenance in industrial systems.	Supports real-time monitoring, adaptive robotics, and quality control.
Challenges	Interoperability issues, legacy system integration, and scalability problems.	Facilitates flexible solutions while reducing system vulnerabilities.
Security Imperatives	Cybersecurity must be embedded to ensure trust, privacy, and system resilience.	Enables anomaly detection, secure decision-making, and risk mitigation.
Opportunities	Efficiency, sustainability, innovation, and adaptive infrastructures.	Drives digital transformation and next-generation resilient infrastructures.

The design should include the imposition of the protection and regime to all the layers. The data in AI quality presupposes that even the wrong input or even the corrupted one can destroy the whole machine. Cybersecurity as phenomenon cannot be viewed as an add-on, or as something complementary to the whole. At this point, the societies will be able to high risk as well as guarantee efficiency and security of emerging and operational infrastructures. The reality of interdependence between the stages of technological, economic and security levels is represented in the long-term vision. Incorporated into the systems infrastructure as a form of artificial intelligence (AI) is installed have properties like the users of major paradigm shifts and optimization of the quality of work, and is innovative on most domains. Nevertheless, in this situation, the fortuitous appearance of AI is going to require the corresponding illumination as well not only in the context of the security of the frameworks but also of informing the theory of information exploration and adherence of the system to the already existing systems. Physically meaningful AI safety is in the objects where physical infrastructure, be it civil engineering or mechanical engineering, needs to be taken into account. Specifically, by declaring such idea to propose the very concept of defining the safety brackets and buffers, Farahmand and Neu draw conclusions about the importance of the probabilistic strategies that at one point will be integrated into the portfolio of AI safety systems.[15] Otherwise, yet another architectural choice made in the information modelling undertaken on the precinct of the nature of AI application figures among other factors in making sure the utilization of AI-based infrastructure are helpful and scalable. Myeka explains how the AI-based database systems will outwit the virtual database systems not only to correct the aspect of quality performance but also to effectively improve the process of developing data into the systems.[31] The above techniques (partitioning and specialized indexing methods) is crucial in dealing with the massive data that the AI systems demand. With such practices all considered, the infrastructures will be designed to the extent that they are not only capable of addressing the contemporary demand of AI needs, but thematic of some more advanced technologies that can be developed in the long run, given time availability.[31] It would apply equally to the healthcare sphere in particular, wherein people would have an opportunity to benefit even more due to the coverage of AI in the specified combination of explainable artificial intelligence (XAI) and cloud processing when the latter runs on an edge computing platform. Those assumptions serve to withstand the learning that with the addition of XAI, we will be able to ensure that the medical personages will be capable of inferring the output that will be created by AI and be more certain that they can. Both the companies that also happen to be audaciously viewed, and that are hypothesis-shifted in that matter of the topic of the risk mitigation models, can effortlessly introduce the AI technologies without usability of altering the nature of the business, at large, including the business-critical component in particular.[32] A statistic advantage of AI-based infrastructures is also in cloud computing, which Wang explains by the management techniques of the resource. Using AI assists resource selection according to utilization of all potential park of consumed energy and least amount of the carbon they provide its function as it is brought up against the concept of sustainability.[33] Concisely, the AI-regulated infrastructures implement these principles to reflexivity its aspect of the safety, smarter modeling and thorough incorporation of the systems that can comprise it along with the effective use of the resources within the clouds. All these are essential because AI technologies should not only be successfully operationalized but also tied to the sustainability, efficiency, and the objective of safety.

Cybersecurity Threats in AI-enabled Infrastructures

The cybersecurity threat becomes a rather complex and interstice issue in AI-oriented constructions. Classic advanced attacks such as malware, phishing, and denial of service attacks can also be advanced and now be mounted with complex attacks against AI systems. Adversarial examples- they are motivated manipulations through artificial intelligence models where data is altered to influence change by causing slight deviations or alterations that predict miscarriage of justice. It can create a threat to the training process of the model because the model will learn vulnerable regions that it can apply later in life. They are attractive targets including critical infrastructural portions of power systems, transportation, healthcare and others (table 3). The nanomaterials-based literature study also marks such kind of problem stability among such kinds of situations as the predictive model validity.[33,34,35,36] These cyber security dangers, thus, coexist in multi-layers with both the digital and physical consequences.

Attack of such systems can be highly disabling and even damaging. Such ripple effects are intensified by the fact that various infrastructures are interlinked in manner that a collapse in one system can be transmitted into another system. Complex criminals exploit the trivial authentication or just insecure software or just insecure IOT toys. More to the point, state-sponsored cyber operation habitually employed infrastructures as its method of strategic interference.

Table 3. Cybersecurity Threats in AI-enabled Infrastructures

Threat Type	Description	Impact on Infrastructures
Adversarial Attacks	Manipulation of AI models by introducing small, imperceptible data changes.	Causes misclassification, wrong predictions, and unsafe decisions.
Data Poisoning	Corrupting training data to embed hidden vulnerabilities into AI systems.	Undermines AI reliability and enables backdoor access to critical systems.
Denial-of-Service (DoS/DDoS)	Overwhelming infrastructure services with excessive traffic to cause disruption.	Interrupts essential services such as energy, transport, and communication.
Malware and Ransomware	Malicious software designed to steal, encrypt, or damage infrastructure data.	Leads to financial losses, data breaches, and operational downtime.
Phishing and Social Engineering	Deceptive techniques used to trick users into revealing sensitive information.	Compromises user identities, system credentials, and trustworthiness.
IoT Device Exploitation	Exploiting weakly secured IoT devices as entry points into infrastructure systems.	Creates cascading failures across interconnected infrastructure networks.
Insider Threats	Malicious actions from authorized personnel or compromised insider accounts.	Breaches internal security, leading to sabotage or data exfiltration.

These requirements need to monitor them on a regular basis, to prepare on the working side, and reshape the cooperation across the divisions. The evolution of cyber threats has been proliferator with the result of offering infrastructures-specific resilience (facilitated by AI). The manifestation of multidimensional cybersecurity risks in the form of intermittent, dynamic and rapidly increasing integration of artificial intelligence (AI) and into all spheres of activity, namely areas of operation critical infrastructure and those under threat, is growing. AI can fuel more efficient processes, and may also be a source of ill intent that deserves its own consideration to cybersecurity policy. In addition, the industries such as healthcare are in some way susceptible to the degree that the information there is sensitive. This is because Zakhmi[37] constructed Zero Trust Architectures (ZTA) as the obligative security apparatus during these hazards of high-stake immediate localities. The phrase will always verify never trust comes very well in the area where patient work and integrity put the risk very high. Application in ZTA may be applicable in curbing AI targetcyber threats, since there is found gaps in the connectedness between the theoretical instructions and the practice-based applications. In the paradigm of the supply chain management, the incorporation of AI will point to potential areas of optimization yet will also bring phishing of the cybersecurity. Cybersecurity hazards, which Samuels brings out, reveal that there exists the necessity to mitigate them since the organizations move to the Industry 4.0 and beyond.[38] The abatement of the above-discussed barriers, along with AI analytics integration in the supply chains, can be applied to the formation of regulatory landscapes and the establishment of a sustainability and cybersecurity culture. All this and more is a sign of desperate need of prompt overall solutions that will not only inconvenience the development of AI but will curb the unparalleled flood of cybersecurity threats being unleashed in separate f nails. It is significant to establish a synergistic policy, which is regulatory and technical modifications, and culture one adjustments in order to avail the creation of sturdy infrastructures, which can resist the changing climate of cyberthreats.

AI for Cybersecurity Defense

AI has become a powerful tool in raising security levels of infrastructures than infrastructural and information sharing. The issue of locating anomalies with the help of machine learning models can arise because the proportions of data are significant, and locating datasets can occur in real-time. Deep learning can discriminate more expert example patterns of an attack that might be missed with a more traditional approach. Predictive analytics are also useful in those situations where an organization anticipates threats before they happen to the organization so that it prepares beforehand by anticipating threats. The threat intelligence log captured by the AI is not merely automated but it also presents the fewest elements of reaction to human error and response time. Simultaneously, the development of new graphene sensing and predictive nanomaterials to offer insights on the development of sturdier infrastructures might be presented.[39,40,41,42] Defense tactics based on favorable dangers can be mitigated by the reinforcement learning. These models must however be conditioned to train under good samples to make them effective (table 4).

Table 4. AI for Cybersecurity Defense

Defense Strategy	AI Approach	Benefits
Anomaly Detection	Machine learning models analyze traffic patterns to detect irregular behaviors.	Early detection of cyberattacks before damage occurs.
Predictive Analytics	AI forecasts potential threats by analyzing historical and real-time data.	Proactive risk management and improved resilience of infrastructures.
Automated Incident Response	Automated systems respond instantly to security breaches with minimal input.	Faster response times and minimized human error in handling threats.
Reinforcement Learning Defense	Reinforcement learning adapts defenses dynamically against evolving attacks.	Continuously evolving defense strategies tailored to new attack vectors.
Threat Intelligence Systems	AI-driven platforms aggregate and analyze global threat data for defense.	Improved preparedness with real-time global threat awareness.
Identity and Access Management	Biometric systems and AI algorithms manage secure authentication processes.	Enhanced protection of sensitive systems and reduction of unauthorized access.
Fraud and Intrusion Detection	Deep learning models identify anomalies in user behavior and transactions.	Greater accuracy in detecting fraud, hacking, and insider threats.

The AI may also help to authenticate identities, stopping of an intrusion and fraud. The artificial intelligence devices of smart infrastructures have the capacity to capture this information when suspicious energy flow, traffic records, or communication connections occur. These applications show that AI can be applied to serve as a computing defense against attacks related to cyber terrorism. AI, however, should not be carelessly applied in the defense with regards to transparency accountability, and maintenance of ethics. Over the past several years, an AI and its associated sub dependencies, such as Machine Learning (ML) and Deep learning (DL), have changed the fence of cybersecurity. These technologies contribute to the traditional cybersecurity that enables building more efficient, more responsive systems, and adapting the environment that varies with cyber threats. With AI, as the new facet of cybersecurity, the general trend in how organizations identify, react and eradicate different types of cyber menaces has greatly transformed and therefore becomes critical in the issue of modern cybersecurity practices. Besides that, AI methods can be employed in many more aspects of cybersecurity, including intrusion detection, spam detection, botnet, and malware. According to Mohamed, these AI techniques can significantly enhance the performance of the threat detectors not only in relation to the traditional systems, but also eliminate the vulnerability of the legality of older defense systems, in which the cyber-attacks were fully advanced.[43] But with restrictions, complexities etc that such models contribute to, one cannot deny them. They also foster the level of accuracy at the detriment of interpretability in the majority of cases, and make AI systems more difficult to apply and utilize in such fields as cybersecurity.[44] In a manner akin to a machine to this shift in adversity degree, fresh approaches, including reinforcement learning (RL) have been developed. Rahmati explains the ways RL can be deployed in improving real-time threat abuse by a lowering agent of false positives deployed to trusted infrastructure adhering to adversarial robust architecture as compared to the traditional one.[45] This enhanced automation of smart cybersecurity can be combined with the highlight of applications capable of safeguarding new-born threats without human intervention almost. Additionally, AI has the capacity to increase cybersecurity rather radically, but straddling that, the device is also some way compromising in the sense that the device can be used by the ill-intentioned user to commit cybercrime. El-Eremy[46] which provides a single glimpse of how the generative AI would operate in zero-day attacks and, consequently, any 2-sided applications of AI in relation to cybersecurity, are as multifaceted a way of implementing AI as possible. AI-assist cybersecurity is, however, a refreshing addition to the practice of responding to attack, thereby boosting it to the practice of detection and resolution in the wake of multifaceted cyber-crimes. Another aspect, although with the positive image, is to be wary of the moral aspect and potential imperfection of the application of the AI technologies to the realm.

Vulnerabilities of AI in Infrastructures

Amidst some of these advantages, there is also insecurity which the enemies of these infrastructures would also exploit although there are some aspects of positivity which are provided. All of the flaws absent AI models may be introduced when they are trained using the data tied to the stage of data poisoning. It plays a conrotatory role in decision making where decision-making handing skewness is concerned where misjudgment is propagated. Many AI jobs are black boxes, and by that very fact can be difficult to audit and justify their outputs. That can be explained by the fact that there is no transparency which casts doubt on the accountability in making sensitive decisions with regard to security. The attackers will also be able to have the security systems hacked via an algorithmic bias. These offer us their solutions as 0 trust architecture and it must be accomplished swiftly. Research in materials is also not much less close to resolving this problem related to predictive models reliability and validation.[47,48] Collusion with AI also presents a serious danger in that excessive dependence with AI can result in human laxity. Even the currently testable AI-based systems frequently cannot reveal any capabilities to resist zero-day attacks and new vectors. It is still to apply the law and ethical applications of AI to infrastructures. Explainable AI, extensive testing and a higher level of regulations can shape such weaknesses. AI weaknesses in infrastructures are trans-dimensional and inter-disciplinary in the sense that they cut across many lines (such as for example healthcare, critical national infrastructures, and the small and medium-sized enterprises (SMEs). The security, functional and ethical issue increases the danger that the technology AI can erode it and that they will need a bit of planning in strategic management. Also, SME, especially among low-income areas, poses a high risk to a digital divide. Significant earthquake of these business entities is very poor in finances, resources, and technological capabilities to make use of AI technologies. Such difference could permit justifying the differences in other domains such as tourism where AI could be employed as a competitive advantage provider. This form will necessitate slightly exceptional government assistance and infrastructure and even the possibility to parity distribution AI tools and to drive those vacuity areas to the extreme ends.[49] The reason is that the population dependence on AI is excessive, and this also imposes greater threats to the comparative freedom of discretion of the decisions of the humans. At the apex AI is highly sensitive to bulk data volumes, (this makes AI models reliant on data quality) entire systems can be bad (table 5), by pipelines of available data.

The development of infrastructure to facilitate the digital capacity plays a crucial role in making sure that small business does not fall behinds in the AI technology economy. The fact of being an internal organizational weakness and involvement in employment practices also largely contributes to the AI vulnerability.

Table 5. Vulnerabilities of AI in Infrastructures

Vulnerability	Description	Impact on Infrastructures
Data Poisoning	Injection of malicious or corrupted data into AI training sets.	Leads to unreliable AI systems vulnerable to exploitation.
Adversarial Examples	Small, imperceptible modifications to input data cause wrong predictions.	Causes misclassification and unsafe infrastructure decisions.
Black-box Models	Opaque models with limited explain ability hinder auditing and trust.	Decreases transparency and reduces trust in AI-enabled systems.
Algorithmic Bias	Biased training data leading to unfair or incorrect decisions.	Undermines fairness, accuracy, and inclusivity in infrastructure management.
Data Integrity Issues	Errors or corruption in data pipelines compromise system reliability.	Weakens system resilience and increases likelihood of cascading failures.
Overreliance on AI	Dependence on AI reduces human oversight and situational awareness.	Increases risk of undetected errors or manipulation in critical systems.
Zero-day Vulnerabilities	Exploitable flaws in software or systems unknown to developers.	Exposes infrastructures to high-impact attacks with no immediate patch.
Insufficient Regulations	Lack of standardized frameworks for accountability, ethics, and governance.	Hinders widespread adoption of secure AI practices in critical infrastructures.

Moreover, internal threats, i. e. misinformation, and AI-based ethical dilemmas also exist, which require an attentive assessment of the organizational communication practices. It may appear that the tic approach, i.e. the synthesis of mindsets of communication experts can illuminate the structural errors, which are the unavoidable consequences of the introduction of AI technologies.[3] This two-facet security issue, the expressly outward threats, and the covert internal-to-organization challenges render this question, why should the organizations declare the ethical problematic situation of AI implementation, knowing that it will be able to preserve the integrity of functioning. Finally, discussing a weak AI vulnerability in infrastructures is a matter that should be discussed in a multidisciplinary fashion. Such a plan should take into account technical means of possessing cybersecurity, strategic thinking regarding the equal use of AI technologies, and morality put into the center to consider internal and external issues that may arise because of implementing AI.

Emerging Technologies and Future Directions

The future of the new technologies of integrating the AI-enabled cybersecurity infrastructures into the future is bright. Data transactions are provided with strong and univalent security pointlessness of the blockchain. The digital twins are applicable to real-time simulation and monitoring of infrastructures, and in the resilience of cyber threats. Quantum computing has projected it to be mind-altering not only in the encryption level but also in the-decryption level. Such technologies comprise multi-layers defense and infusion or combination of AI. To form a secure power distribution, information blockchain and the use of AI will also take place in a smart grid. The output of individual treatment (table 6) data could be provided using digital twins which could be used to simulate patient data plotted under the healthcare system. The extra aspect of the use of the 5G communication is another factor complicating the interconnection of the infrastructures and requires extra protection. The level of this scope is that there is a need to do more studies on the solution to how the technology can be innovated without compromising ethical and legal requirement. The current gap lies in the fact that cybersecurity is a problem that the world is currently confronting that demands an inter-disciplinary approach to rising to the challenges. The emerging technologies will be implemented in infrastructures that will be more open, flexible and strong. Lastly, AI-driven infrastructures must be created to counter the evolving threats. They are also required to build intelligent and vulnerable infrastructures with AI. The technologies to be covered later on are altering various fields of the industries that impact the arena of healthcare, manufacturing, and energy and production regulation of the agriculture sector. On this appeal to increased efficiency, to correctness and duration of the product are determined the strides of innovation in the future. Smart grids improve their energy management system in artificial intelligence and edge computing aspects as well. Similarly, the realization of nanomaterials today has come to include the element of innovation towards versified long term sustainability and versatility.[50,51,52,53,54,55]

Application of deep learning algorithms in processing and analysis of massive bodies of operational data has been very useful and has garnered success in providing the accurate loads forecasting and settlement on issuing the energy assets. Such predictive analytics service will be essential in sidestepping and optimizing the performance of the energy distribution networks that will be heart of the road as the dynamics in the demand swings based on the raising number of renewable energy.[20] With big data and machine learning, the process of agriculture in the farming sector of agriculture is transforming. The recent tendencies in the PM ag technology lie in adhering to the overproduction of the presented resources and ongoing adjustment to the altering environments. These technologies were found to be able not only to contribute to the effectiveness of farming source operations but also work harder to secure the food security as farmers can now react suffice to the customer demand and environmental conditions.[56,57,58,59] In sum, the tendency toward the creation of the surge-forming technologies in the mentioned domains can be formulated as the field of the converging intelligent systems and the improved analysis of the data and creative designing that will eventually become the input of the advances of the efficiency,[60,61,62,63] sustainability, and the health outcomes.

Table 6. Emerging Technologies and Future Directions

Technology/ Approach	Description	Impact on Infrastructures
Blockchain	Decentralized and tamper-resistant technology ensuring data integrity and secure transactions.	Enhances trust, prevents tampering, and supports secure data sharing.
Digital Twins	Virtual replicas of infrastructures for real-time monitoring, simulation, and resilience.	Improves proactive maintenance and disaster management in smart systems.
Quantum Computing	Advanced computing that can break classical encryption but also create stronger security.	Provides new cryptographic methods to secure AI-enabled infrastructures.
5G and Beyond	High-speed, low-latency communication enabling massive IoT and real-time AI applications.	Expands connectivity but requires robust safeguards against cyber risks.
Edge AI	Deploying AI models directly on edge devices for faster processing and reduced risks.	Reduces dependency on centralized servers and improves privacy/security.
Explainable AI (XAI)	AI systems designed for transparency, interpretability, and accountability.	Strengthens user trust and adoption of AI in critical infrastructure security.
Cross-disciplinary Collaboration	Joint efforts between governments, academia, and industry for sustainable cybersecurity.	Ensures holistic resilience and shared responsibility in cybersecurity.

This is a favorable omen in that because research is not likely to be silent in providing such guidance the trends are bound to discover the fate of automized industries.(64,65,66,67)

CONCLUSIONS

Artificial intelligence has infiltrated both services of disruptive technologies, and a security risk in contemporary infrastructures. Its use in smart grids, transportation and urban control has also resulted in massive efficiency and automation. Nevertheless, the developments equally are revealing other cyber-attacks to cause devastations to infrastructures. The vulnerability of the interconnected systems can be signaled by cybersecurity attacks like hostile demonstrations reportedly through adversarial attacks, data poisoning, and denial-of-service. Defensive aspects of AI also include the cases where the latter is implemented to identify anomaly, real-time monitoring, and predictive analytics. Despite these advantages, AIs in themselves are liable to being manipulated and not being transparent. To address these pitfalls multidisciplinary solutions which require the use of technology, regulation as well as ethical standards are needed. New developments are made in the field of quantum computing and the blockchain that stand chances of more certain cyber security structures. Artificial Intelligence (AI)-driven digital twins, have offered the capability to observe and warn in time against developing threats. However, cyber-attacks are multidimensional in their essence, and they require ongoing advancement of adaptation and innovation. The industry and academia should work together with the government to put strong infrastructures. It will need to reach a middle ground where they can both have AI/intelligible. It is crucial that both have the potential to weaponize AI, rooted in the stability of the future and based on the scaling policies, which are essential to sustainability in the long run. The high potential is to work towards creation of smart infrastructures more resistant to cyber-attacks. With it, AIs cybersecurity will help it become the critical corpse solution to active, adaptable, and future-proofed structures.

BIBLIOGRAPHIC REFERENCES

1. Leenen J, Hiemstra P, Hoeve M, Jansen A, Dijk J, Vendel B, et al. Exploring the complex nature of implementation of artificial intelligence in clinical practice: an interview study with healthcare professionals, researchers and policy and governance experts. Plos Digit Health. 2025;4(5):e0000847. https://doi.org/10.1371/journal.pdig.0000847

2. Amerini I, Barni M, Battiato S, Bestagini P, Boato G, Bruni V, et al. Deepfake media forensics: status and future challenges. J Imaging. 2025;11(3):73. https://doi.org/10.3390/jimaging11030073

3. Zhao W, Rachwalski A, Berndt M, Jin Y. An examination of management of ai-triggered organisational threats from communication practitioners' perspective. J Contingencies Crisis Manag. 2025;33(1). https://doi.org/10.1111/1468-5973.70031

4. Abaszade RG, Kapush OA, Nabiyev AM. Properties of carbon nanotubes doped with gadolinium. J Optoelectron Biomed Mater. 2020;12(3):61–5. https://www.chalcogen.ro/61_AbaszadeRG.pdf

5. Abaszade RG, Kapush OA, Mamedova SA, Nabiyev AM, Melikova SZ, Budzulyak SI. Gadolinium doping influence on the properties of carbon nanotubes. Phys Chem Solid State. 2020;21(3):404–8. https://doi.org/10.15330/pcss.21.3.404-408

6. Figarova SR, Aliyev EM, Abaszade RG, Alekberov RI, Figarov VR. Negative differential

resistance of graphene oxide-sulphur compound. J Nano Res. 2021;67:25–31. https://doi.org/10.4028/www.scientific.net/JNanoR.67.25

7. Abaszade RG, Mammadova SA, Kapush OA, Agayev FG, Nabiev AM, Mammadova MM, et al. Synthesis and characterization of graphene oxide flakes for transparent thin films. Phys Chem Solid State. 2021;23(3):595-601. https://doi.org/10.15330/pcss.22.3.595-601

8. Xu G, Guo T. Advances in ai-powered civil engineering throughout the entire lifecycle. Adv Struct Eng. 2025. https://doi.org/10.1177/13694332241307721

9. Wang H, Chelvan B, Golec M, Gill S, Uhlig S. Healthedgeai: gai and xai based healthcare system for sustainable edge ai and cloud computing environments. Concurr Comput Pract Exp. 2025;37(9-11). https://doi.org/10.1002/cpe.70057

10. Singh A, Lalotra N, Shah SS, Rather MD, López-Maldonado EA, Pathania K, et al. A comprehensive review on the synthesis and properties of MXenes for supercapacitor applications. ACS Appl Energy Mater. 2025;8(8):4884–914. https://doi.org/10.1021/acsaem.4c03194

11. Wang H. Ainet0: ai forecasting based carbon neutral cloud resource management for net zero targets. Trans Emerg Telecommun Technol. 2025;36(6). https://doi.org/10.1002/ett.70166

12. Yigit Y, Ferrag M, Ghanem M, Sarker I, Μαγλαράς Λ, Chrysoulas C, et al. Generative ai and llms for critical infrastructure protection: evaluation benchmarks, agentic ai, challenges, and opportunities. Sensors. 2025;25(6):1666. https://doi.org/10.3390/s25061666

13. Fetaji B, Samanta D. Artificial intelligence in cybersecurity: a comprehensive analysis of machine learning applications on phishing urls and malware api calls for devising cyber defense strategies. 2025. https://doi.org/10.21203/rs.3.rs-6154552/v1

14. Vazquez B. Machine and deep learning for the diagnosis, prognosis, and treatment of cervical cancer: a scoping review. Diagnostics. 2025;15(12):1543. https://doi.org/10.3390/diagnostics15121543

15. Farahmand F, Neu R. Ai safety for physical infrastructures: a collaborative and interdisciplinary approach. Fatigue Fract Eng Mater Struct. 2025;48(4):1919-28. https://doi.org/10.1111/ffe.14575

16. Sood A, Rao A. A study on the global patterns in the design and development of ventricular assist devices: a visualization approach. Front Cardiovasc Med. 2025;12. https://doi.org/10.3389/fcvm.2025.1371443

17. Lal A, You F. Climate sustainability through ai-crypto synergies and energy transition in the digital landscape to cut 0.7 gtco2e by 2030. Environ Sci Technol. 2025;59(12):6061-73. https://doi.org/10.1021/acs.est.4c11477

18. Abaszade RG. Synthesis and analysis of flakes graphene oxide. J Optoelectron Biomed Mater. 2022;14(3):107–14. https://doi.org/10.15251/JOBM.2022.143.107

19. Mammadov AG, Abaszade RG, Kotsyubynsky VO, Gur EY, Bayramov IY, Khanmamadova EA, et al. Photoconductivity of carbon nanotubes. Tech Phys Probl Eng. 2022;14(3):155–60.

20. Xue J. Real time load forecasting and optimal dispatching of smart grid based on edge computing and deep learning. 2025:64. https://doi.org/10.1117/12.3073787

21. Miller T. The iot and ai in agriculture: the time is now—a systematic review of smart sensing technologies. Sensors. 2025;25(12):3583. https://doi.org/10.3390/s25123583

22. Desai H, Katapally T. Barriers and facilitators to the implementation of artificial intelligence enabled diabetes interventions in lower-middle-income countries: a systematic review protocol. 2025. https://doi.org/10.1101/2025.06.01.25328752

23. Farahmand F, Neu R. Ai safety for physical infrastructures: a collaborative and interdisciplinary approach. Fatigue Fract Eng Mater Struct. 2025;48(4):1919-28. https://doi.org/10.1111/ffe.14575

24. Khang A, Abdullayev V, Abuzarova VA, Khalilov M, Bagirli M. AI-aided data analytics tools and applications for the healthcare sector. In: AI and IoT-based technologies for precision medicine. IGI Global; 2023. p. 345–67. https://doi.org/10.4018/979-8-3693-0876-9.ch018

25. Hajimahmud V, Khang A, Abbas GL, Ismibayli R, Firudin JA. Application of artificial intelligence and internet of things in the manufacturing sector. In: Machine vision and industrial robotics in manufacturing: Approaches, technologies, and applications. CRC Press; 2024. p. 123–45. https://doi.org/10.1201/9781003438137-8

26. Abaszade RG, Mammadov AG, Bayramov IY, Khanmamadova EA, Kotsyubynsky VO, Kapush OA, et al. Structural and electrical properties of sulfur-doped graphene oxide/graphite oxide composite. Phys Chem Solid State. 2022;25(2):256–60. https://doi.org/10.15330/pcss.23.2.256-260

27. Boychuk VM, Zapukhlyak R, Abaszade R, Kotsyubynsky V, Hodlevsky M, Rachiy B, et al. Solution combustion synthesized NiFe2O4/reduced graphene oxide composite nanomaterials: morphology and electrical conductivity. Phys Chem Solid State. 2022;23(4):815–24. https://doi.org/10.15330/pcss.23.4.815-824

28. Ivanichok N, Kolkovskyi P, Ivanichok O, Kotsyubynsky V, Boychuk V, Rachiy B, et al. Effect of thermal activation on the structure and electrochemical properties of carbon material obtained from walnut shells. Materials. 2024;17:2514. https://doi.org/10.3390/ma17112514

29. Zapukhlyak RI, Kotsyubynsky VO, Boychuk VM, Rachiy BI, Abaszade RG, Hoi VT, et al. Structural evolution of porous carbon materials derived from hemp fibers: Raman spectroscopy studies. Phys Chem Solid State. 2025;26(1):132–9. https://doi.org/10.15330/pcss.26.1.132-139

30. Guliyeva NA, Abaszade RG, Khanmammadova EA, Azizov EM. Synthesis and analysis of nanostructured graphene oxide. J Optoelectron Biomed Mater. 2023;15(1):23–30. https://doi.org/10.15251/JOBM.2023.151.23

31. Myeka P. Data modeling best practices for ai-driven applications: architectures for scale and efficiency. World J Adv Eng Technol Sci. 2025;15(2):1263–74. https://doi.org/10.30574/wjaets.2025.15.2.0633

32. Singh M. Integrating artificial intelligence with legacy systems: a systematic analysis of challenges and strategic considerations. Eur J Comput Sci Inf Technol. 2025;13(32):38–45. https://doi.org/10.37745/ejcsit.2013/vol13n323845

33. Abaszade RG, Mammadov AG, Khanmamadova EA. Fundamentals of thermal management in renewable energy systems. In: Heat exchanger technologies for sustainable renewable energy systems. CRC Press; 2025. p. 30–51. https://doi.org/10.1201/9781003534785-2

34. Abaszade RG, Khanmammadova EA. Renewable energy sources and conversion technologies. In: Heat exchanger technologies for sustainable renewable energy systems. CRC Press; 2025. p. 52–72. https://doi.org/10.1201/9781003534785-3

35. Abaszade RG, Nuriev RA, Khanmamadova EA. Smart materials properties and characterization with mechatronics system approaches. In: Novel applications of functionally graded materials. 2025. p. 101-14.

36. Haghi AK, Abaszade RG. Carbon nanotube devices for nanoelectronics. Springer Nature; 2025. (Synthesis Lectures on Solid State Materials and Devices).

37. Zakhmi K. Evolving zero trust architectures for ai-driven cyber threats in healthcare and other high-risk data environments: a systematic review. Cureus. 2025. https://doi.org/10.7759/cureus.85446

38. Samuels A. Examining the integration of artificial intelligence in supply chain management from industry 4.0 to 6.0: a systematic literature review. Front Artif Intell. 2025;7. https://doi.org/10.3389/frai.2024.1477044

39. Abaszade RG, Aliyev EM, Babanli MB, Kotsyubynsky VO, Zapukhlyak RI, Mamedov AG, et al. Investigation of thermal properties of carbon nanotubes and carboxyl group-functionalized carbon nanotubes. Phys Chem Solid State. 2023;24(3):530–5. https://doi.org/10.15330/pcss.24.3.530-535

40. Abaszade RG, Mammadova AG, Khanmammadova EA, Bayramov IY, Namazov RA, Popal KhM, et al. Electron paramagnetic resonance study of gadoliniumum doped graphene oxide. J Ovonic Res. 2023;19(2):259–63. https://doi.org/10.15251/JOR.2023.193.259

41. Abaszade RG, Babanli MB, Kotsyubynsky VO, Mammadov AG, Gür E, Kapush OA, et al. Influence of gadolinium doping on structural properties of carbon nanotube. Phys Chem Solid State. 2023;24(1):153–8. https://doi.org/10.15330/pcss.24.1.153-158

42. Abaszade RG, Mammadov AG, Bayramov IY, Khanmamadova EA, Kotsyubynsky VO, Gur EY, et al. Modeling of voltage-ampere characteristic structures on the basis of graphene oxide/sulfur compounds. Tech Phys Probl Eng. 2022;14(2):302–6.

43. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowl Inf Syst. 2025. https://doi.org/10.1007/s10115-025-02429-y

44. Nazim S, Alam M, Rizvi S, Mustapha J, Hussain S, Su'ud M. Advancing malware imagery classification with explainable deep learning: a state-of-the-art approach using shap, lime and

grad-cam. PLoS One. 2025;20(5):e0318542. https://doi.org/10.1371/journal.pone.0318542

45. Rahmati M. Adversarially robust ai for real-time cyber threat detection: a reinforcement learning approach. 2025. https://doi.org/10.21203/rs.3.rs-6198488/v1

46. Al-E'mari S, Sanjalawe Y, Fataftah F. Zero-day attacks using generative ai. 2025:277–308. https://doi.org/10.4018/979-8-3373-0832-6.ch012

47. Stetsenko MO, Abaszade RG. X-ray phase analysis of carbon nanotubes obtained by the arc discharge method. UNEC J Eng Appl Sci. 2023;3(1):15–20. https://doi.org/10.61640/ujeas.2023.0503

48. Moradi R, Pour Khalili N, Khanmamadova E, Abaszade R. Functionalized carbon nanostructures for flexible electronics. In: Handbook of functionalized carbon nanostructures. Springer; 2024. p. 2581–614. https://doi.org/10.1007/978-3-031-14955-9_71-1

49. Herawati R, Pradana A, Shariffuddin N. Integrating artificial intelligence (ai) into sustainable tourism management in indonesia and the impact on customer experience: a literature review. 2025:36. https://doi.org/10.1117/12.3058730

50. Khanmammadova EA, Abaszade RG. Advanced design, materials, and manufacturing techniques for next-generation antennas. In: Advanced antenna technologies for aerial platforms: From design to deployment. IGI Global; 2025. p. 49–92. https://doi.org/10.4018/979-8-3693-6035-4

51. Khanmammadova EA, Abaszade RG. The evolution of green mobility: A critical comparison of pure electric and hybrid electric vehicles. In: Hybrid electric vehicles and distributed renewable energy conversion: Control and vibration analysis. IGI Global; 2025. p. 187–251. https://doi.org/10.4018/979-8-3693-5797-2.ch011

52. Khanmamadova E, Abaszade R, Moradi R. Hydrophobic and hydrophilic behavior of multifunctional thin film. In: Multi-scale and multifunctional coatings and interfaces for tribological contacts. CRC Press; 2025. p. 83–102. https://doi.org/10.1201/9781032635347-6

53. Khanmamadova E, Abaszade R, Moradi R. Antiviral thin surface and surface life. In: Multi-scale and multifunctional coatings and interfaces for tribological contacts. CRC Press; 2025. p. 121–34. https://doi.org/10.1201/9781032635347-8

54. Figarova SR, Aliyev EM, Abaszade RG, Figarov VR. Negative thermal expansion of sulphur-doped graphene oxide. Adv Mater Res. 2023;1175:55-62. https://doi.org/10.4028/p-rppn12

55. Chen S, Ding Y. Precision agriculture current progress from a novel bibliometric method. World Food Policy. 2025;11(1). https://doi.org/10.1002/wfp2.70004

56. Khang A, Abdullayev V, Hahanov V, Shah V. Preface. In: Advanced IoT technologies and applications in the Industry 4.0 digital economy. IGI Global; 2024. p. x–x.

57. Khang A, Abdullayev V, Hahanov V, Shah V. Advanced IoT technologies and applications in the Industry 4.0 digital economy. CRC Press; 2024. https://doi.org/10.1201/9781003434269

58. Khang A, Hajimahmud AV, Triwiyanto T, Abuzarova VA, Ali RN. Cloud platform and data storage systems in the healthcare ecosystem. In: Medical robotics and AI-assisted diagnostics for a high-tech healthcare industry. IGI Global; 2024. p. 345–67. https://doi.org/10.4018/979-8-3693-2105-8.ch021

59. Khang A, Hajimahmud V, Abuzarova VA. Wastewater treatment for environmental sustainability. In: Revolutionizing automated waste treatment systems: IoT and bioelectronics. IGI Global; 2024. p. 23–45. https://doi.org/10.4018/979-8-3693-6016-3.ch002

60. Khang A, Hajimahmud V, Ali RN, Hahanov V, Avramovic Z, Triwiyanto T. Role of machine vision in manufacturing and industrial revolution 4.0. In: Machine vision and industrial robotics in manufacturing: Approaches, technologies, and applications. CRC Press; 2024. p. 1–20. https://doi.org/10.1201/9781003438137-1

61. Khang A, Hahanov V, Hajimahmud VA, Litvinova E, Ali RN, Abuzarova V. The impact of the cyber-physical environment and digital environment on the socialization environment. In: Revolutionizing the AI-digital landscape: A guide to sustainable emerging technologies for marketing professionals. CRC Press; 2024. p. 345–67. https://doi.org/10.4324/9781032688305-22

62. Sun Z, Qin Z. Status and prospects of mechanical precision machining technologies: an econometric analysis of literature based on 2019–2024. 2025:66. https://doi.org/10.1117/12.3054434

63. Abaszade R, Khanmammadova E. Specific applications for unmanned aerial vehicles (UAVs) and aerial robotics. In: Advanced antenna technologies for aerial platforms: From design to deployment. IGI Global; 2025. p. 117–58. https://doi.org/10.4018/979-8-3693-6035-4

64. Abaszade RG, Aliyev EM, Mammadov AG, Khanmamadova EA, Guliyev AA, Aliyev FG, et al. Investigation of thermal properties of gadolinium doped carbon nanotubes. Phys Chem Solid State. 2024;25(1):142–7. https://doi.org/10.15330/pcss.25.1.142-147

65. Sharma B, Singh A, Sharma A, Dubey A, Gupta V, Abaszade RG, et al. Synthesis and characterization of zinc selenide/graphene oxide (ZnSe/GO) nanocomposites for electrochemical detection of cadmium ions. Appl Phys A. 2024;130:297. https://doi.org/10.1007/s00339-024-07472-0

66. Abaszade RG, Mammadov AG, Khanmamedova EA, Aliyev FG, Kotsyubynsky VO, Gür E, et al. Photoconductivity of functionalized carbon nanotubes. Dig J Nanomater Biostructures. 2024;19(2):837–43. https://doi.org/10.15251/DJNB.2024.192.837

67. Mammadov AG, Abaszade RG, Babanli MB, Kotsyubynsky VO, Gur E, Soltabayev BD, et al. Photoconductivity of gadolinium-doped carbon nanotubes. Int J Tech Phys Probl Eng. 2023;15(3):53–8.

FINANCING
None.

CONFLICT OF INTEREST
None.

AUTHORSHIP CONTRIBUTION

Conceptualization: Fuad Abaszadeh, Taleh Asgarov, Rashad Ismibayli, L.R. Priya, Malikov Ziyodullo Abdurayim, Abduraxmonov Muhammad Sulaymon.

Data curation: Fuad Abaszadeh, Taleh Asgarov, Rashad Ismibayli, L.R. Priya, Malikov Ziyodullo Abdurayim, Abduraxmonov Muhammad Sulaymon.

Formal analysis: Fuad Abaszadeh, Taleh Asgarov, Rashad Ismibayli, L.R. Priya, Malikov Ziyodullo Abdurayim, Abduraxmonov Muhammad Sulaymon.

Drafting - original draft: Fuad Abaszadeh, Taleh Asgarov, Rashad Ismibayli, L.R. Priya, Malikov Ziyodullo Abdurayim, Abduraxmonov Muhammad Sulaymon.

Writing - proofreading and editing: Fuad Abaszadeh, Taleh Asgarov, Rashad Ismibayli, L.R. Priya, Malikov Ziyodullo Abdurayim, Abduraxmonov Muhammad Sulaymon.