ISSN:1813-1786 (Print) 2313-7770 (Online)

An In-Depth Analysis of Emerging Trends and Applications in Computing

M. K. Abid[1], S. Farid[2]

[1]Department of Computer Science, Emerson University, Multan, Pakistan
[2]Department of Computer Science, Bahauddin Zakeriya University, Multan, Pakistan

[1]kamranabidhiraj@gmail.com

Abstract- The rapid development of computer science has brought opportunities as well as immense problems in terms of embracing the arising technologies in areas like healthcare, finance, smart cities, and agriculture. This paper reflects a systematic review of more than 5,000 recent research works (2021,2024). It is based on the emergent research direction that has been defined, such as Artificial Intelligence (AI), Machine Learning (ML), Cybersecurity, Internet of Things (IoT), Blockchain, Cloud Computing, Edge Computing, and Quantum Computing. The most prominent of these is Cybersecurity and IoT, which have 1,150-1,250 publications, respectively, and Machine Learning and AI with 900-1,200 studies. Such technologies are even impacting the advances of deep learning, intrusion detection, real-time data analysis, and autonomous systems. With it being the case, there are still problems. Bias, fairness, interpretability, and scalability are issues with AI systems. Some of the cybersecurity challenges here include changing threats like ransomware, phishing, and vulnerabilities of AI models. Cloud and edge computing suffer from latency, resource allocation, and real-time response issues, whereas quantum computing continues to be under issues of qubit instability and error correction. Moreover, little research has been conducted on blockchain (approximately 100200 studies), mainly because of energy consumption and regulation issues. To address them, this review combines quantitative measures and qualitative research analysis to identify existing trends and problems of application along with research areas. It then sums up on how interdisciplinary cooperation, scalable architectures, ethical frameworks, and so forth, can be used to develop secure, intelligent, and sustainable environments of computing.

Keywords- Machine Learning, Cybersecurity, Internet of Things, Blockchain Technology, Cloud Computing, Edge Computing

I. Introduction

Fundamental computer science studies cause rapid changes through algorithmic analysis and structural data processing, along with programming language development, together with software engineering practices, with artificial intelligence methods and cybersecurity approaches for information system organization. Every size business depends on Natural Sciences as its fundamental innovation catalyst, which establishes modern business process interfaces and patterns. The success of modern society requires computer science to create diagnostic healthcare models based on machine learning, along with security systems for IoT devices. Multiple sectors implemented AI and machine learning during recent times, which led to the creation of intelligent software programs that handle complex automatic workloads and produce knowledge-based decisions and boost operational performance metrics[1]. Digital systems receive protection from both their networks and their constant exposure to digital threats through consistent cybersecurity monitoring and threat defense operations. The development of machine learning intrusion detection systems for IoT demonstrates why computer science needs to protect digital infrastructure given the growing popularity of such systems for intrusion control. The power of computer science transformation reaches its peak through three primary areas including cloud computing and blockchain technology and smart city development that create expandable solutions and enhance lifestyle quality[2-3]. The future industrial sector will experience advantages from upcoming edge computing and quantum computing advancements that enable quick data processing and decentralized operations and advanced data analytics methods. Computers function as a fundamental component for solving current problems through their capacity to unite these new developments into intelligent secure environments for future use.

The target of this review examines modern computer science developments alongside emerging technologies which define modern field advancement. Digital developments continue to increase in importance because people need to understand the latest advancements which reformulate businesses and societal frameworks and technological frameworks. The paper presents an extensive evaluation of major technological breakthroughs which emphasizes collective progress between artificial intelligence (AI), machine learning (ML), cybersecurity, the Internet of Things (IoT), cloud computing and other emerging fields[4-5]. The review presents details about two distinct applications of machine learning for Internet of Things intrusion detection systems and shows how digital infrastructure faces evolving security threats. The review examines how cloud computing supports business scalability while providing efficient solutions to users alongside the development of Internet of Things (IoT) along with smart systems for building connected systems[6]. This paper investigates the way AI and ML technologies strengthen automated choices in important fields which span across health and finance together with agricultural industries. The paper evaluates these areas to present research findings while explaining practical implementations alongside the barriers, experienced during implementation by researchers and practitioners. The review functions as a guidance tool for upcoming developments while providing understanding about how these trends will affect computer science at large.

II. Emerging Trends in Computer Science

Machine Learning and Artificial Intelligence

Machine Learning (ML) and Artificial Intelligence (AI) have undergone phenomenal developments in the recent period that allow systems to automatically learn from data while improving their abilities and making decisions without substantial human oversight. These technologies show advanced development because of better computational abilities and expanded data resources, as well as the creation of advanced algorithms. The portion of ML that enables artificial neural networks with multiple layers to identify complex patterns has experienced rapid expansion as a field of development. Deep learning delivers exceptional results in image recognition and speech processing, together with natural language handling and autonomous driving systems, so it remains one of the leading AI methods in current use[7]. The list of deep learning architectures includes Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), and transformers, which have obtained state-of-the-art results in various task domains[8]. The development of transformer-based models, GPT and BERT as Generative Pretrained Transformer and Bidirectional Encoder Representations from Transformers, has transformed natural language processing capabilities by making machines perform tasks related to human language processing beyond initially conceivable bounds.

Leading journals in Artificial Intelligence and Machine Learning have been selected for Table 1 according to their impact factor and frequency of publication, along with their topical importance. Both Nature Machine Intelligence, with an impact factor of 28.9, and IEEE Transactions on Neural Networks and Learning Systems, with an impact factor of 7.9, publish research across deep learning, along with reinforcement learning and cognitive systems, and AI ethics[9]. All listed journals have a worldwide focus and fixed publication cycles, while their projected publication volumes demonstrate continuous AI research engagement. The provided table strengthens the research by presenting discussions based on robust peer-reviewed publications.

Table 1: Machine Learning and Artificial Intelligence Publication

Journal Name	**Impact Factor (2023)**	**Category**	**Publication Frequency**	**Region**	**Focus Areas**	**Total Publications in Last 3 Years (Estimate)**
Journal of Machine Learning Research (JMLR)	5.1	Machine Learning Algorithms	Quarterly	Global	Deep Learning, Reinforcement Learning, Theory, Applications	~60-80 publications
IEEE Transactions on Neural Networks and Learning Systems (TNNLS)	7.9	Deep Learning, Neural Networks	Monthly	Global	Neural Networks, Deep Learning, AI Applications	~300-350 publications
Artificial Intelligence	4.7	AI, Cognitive Computing	Monthly	Global	Cognitive Systems, AI Techniques, Human-AI Interaction	~250-300 publications
Machine Learning	4.0	Supervised /Unsupervised Learning	Quarterly	Global	Classification, Reinforcement Learning, Optimization	~40-60 publications
Nature Machine Intelligence	28.9	Interdisciplinary AI Applications	Monthly	Global	AI Ethics, Natural Language Processing, Robotics	~200-250 publications

Figure 1 presents the top five ongoing issues researchers discuss in machine learning and AI research publications spanning the last three years. Research focused on Data Privacy and Security as the key concern garnered about 200 publications showing growing sensitivity regarding ethical AI use and individual data protection. The research emphasis upon Algorithmic Bias coupled with Models scalability demonstrates the need for fair AI solutions and flexible real-time implementations[10-11]. The combination of complex models with resource limitations in deployment showcases the ongoing challenges of understanding how these systems function while implementing them effectively. The visualization backs up the paper's main focus on key obstacles that researchers must consider for future AI development.

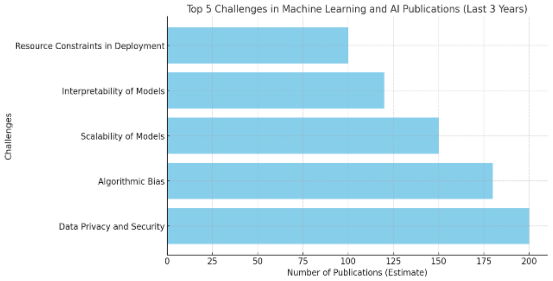

Figure 1: Top 5 Challenges in ML and AI

Artificial Intelligence (AI) and Machine Learning (ML) tools bring radical changes to healthcare alongside finance and agriculture and automotive, and manufacturing through greater operational precision and enhanced personalization options, and higher efficiency levels. Healthcare professionals rely increasingly on AI models for early disease detection of cancer and neurological disorders by processing large-scale medical imaging datasets[12]. The technology performs at a level that equals or surpasses human professionals when it comes to making clinical diagnoses. ML-based drug discovery techniques reduce research durations and increase safety through their capacity to predict both therapeutic effectiveness and treatment side effects. Research in these applications appears regularly in leading publications such as Nature Machine Intelligence and IEEE Transactions on Neural Networks and Learning Systems (Table 1)[10], [13]. Through finance-related applications, ML uses real-time transaction analysis to fight fraud, together with AI solutions that aid investment decisions through data-driven frameworks. The newly developed capabilities transform financial services by delivering custom payment and assessment processes for customers[14]. AI technology provides optimization capabilities in smart agriculture, while it also drives autonomous vehicle development with automated manufacturing systems as secondary applications beyond healthcare and finance. Figure 1 demonstrates the continuing obstacles to general AI implementation that stem from privacy issues with data and biases in algorithms and unclear model performance indicators. The identified concerns match findings presented in Table 1, which shows the requirement for transparent ethical AI systems. Scalable use of AI technology needs a solution to its present limitations across industrial applications.

Cybersecurity

Modern technological progress demands cybersecurity as an essential requirement because the connections between our devices continue to advance rapidly. Modern cyber threats keep growing in complexity while requiring specialized defense protocols for security protection against malware, ransomware, phishing, and advanced persistent threats (APTs)[15]. The journals Computers & Security and IEEE Transactions on Dependable and Secure Computing documented cybersecurity challenges using more than 250–350 research publications from the last three years, according to Table 2. The latest security research demonstrates that traditional rule-based security models struggle to match contemporary attacker methods that target vital infrastructure networks, including power grids and transportation systems, and financial centers. Cyber criminals now use deepfakes combined with social engineering tactics to compromise systems while procuring sensitive information[16-17]. Researchers, together with practitioners, now implement AI and ML technologies to identify and stop threats in real-time operations. Articles in the Journal of Cybersecurity and ACM Transactions on Privacy and Security document the transformation of threat detection by using machine learning models that evaluate network behaviors to detect abnormalities and stop unauthorized access. An adaptive security methodology both accelerates response capabilities and strengthens organizations' ability to withstand continuously evolving cyber threats.

Table 2: Publications on Cybersecurity

Journal Name	**Impact Factor (2023)**	**Category**	**Publication Frequency**	**Region**	**Focus Areas**	**Total Publications in Last 3 Years (Estimate)**
IEEE Transactions on Dependable and Secure Computing	3.7	Cybersecurity, Secure Computing	Monthly	Global	Network Security, Malware, Cryptography	~250-300 publications
ACM Transactions on Privacy and Security (TOPS)	3.8	Privacy, Security	Quarterly	Global	Privacy Protection, Security Protocols	~200-250 publications
Computers & Security	4.0	Security Systems	Monthly	Global	Cybersecurity, Intrusion Detection, Security Management	~300-350 publications
Journal of Cybersecurity	5.0	Cybersecurity Research	Quarterly	Global	AI/ML in Security, Cybersecurity Policy, Incident Response	~150-200 publications
Information Security Journal: A Global Perspective	2.6	Information Security	Quarterly	Global	Threat Intelligence, Cyber Defense Strategies	~120-150 publications

Recent research publications present Figure 2 showing the top five cybersecurity challenges which validate the analysis in the previous section and Table 2. The threat of Ransomware and Malware dominates cybersecurity discussions with approximately 250 estimated publications suggesting extensive worry about their relentless nature[18-19]. Phishing Attacks follow closely by showing attackers' exploitation of human behavior to enter unauthorized systems a problem linked to Deepfakes and Social Engineering approaches which disrupt digital trust and user verification systems. AI/ML Model Vulnerabilities and Scalability and Cost of AI in Security receive increased attention because AI proves valuable for threat detection yet it presents new operational and security risks[20-21]. This research tracks the academic focus presented in Journal of Cybersecurity and ACM Transactions on Privacy and Security which investigates both the potential and boundary conditions of AI-driven security systems. The necessity of ongoing innovative work alongside multi-domain studies and quick security systems demands support from artificial intelligence and machine learning resources. A large number of publications has been done for IOT challenges as mentioned in Figure 3, and the total number of publications and key focus area are mention in the Table 3 as well.

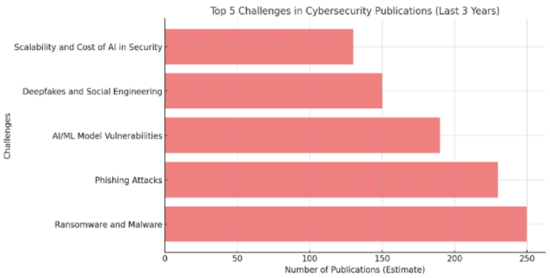

Figure 2: Top Challenges in Cybersecurity

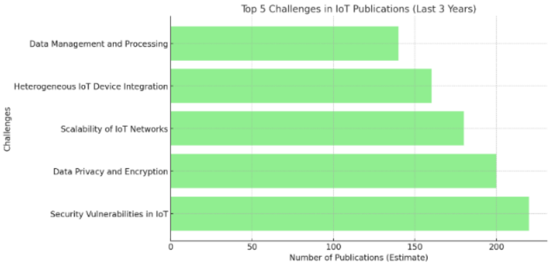

Figure 3: Top 5 Challenges in IOT Publications

Table 3: No. of Publication in Last Three Years

Journal Name	**Impact Factor (2023)**	**Category**	**Publication Frequency**	**Region**	**Focus Areas**	**Total Publications in Last 3 Years (Estimate)**
IEEE Internet of Things Journal	7.6	IoT Systems, Networks, and Applications	Monthly	Global	Smart Systems, IoT Architecture, Network Security	~250-300 publications
Journal of Network and Computer Applications	3.5	IoT, Network Security	Monthly	Global	IoT Security, Data Management, Cloud IoT Integration	~200-250 publications
Sensors	3.7	IoT Applications and Sensors	Monthly	Global	IoT Sensing, Data Privacy, Communication Protocols	~300-350 publications
Future Generation Computer Systems	4.4	IoT, Data Management	Monthly	Global	Big Data in IoT, Smart Cities, Edge Computing	~150-200 publications
IEEE Access	3.5	IoT, Connectivity, and Security	Monthly	Global	IoT Security, Integration Challenges, Data Processing	~120-150 publications

Blockchain Technology

The widespread interest in blockchain technology emerged because it delivers safe decentralized systems with transparent features which serve multiple industries. The concept originated through Bitcoin and Ethereum cryptocurrencies before its adoption spread to transform supply chains and healthcare and real estate industries and many others. The blockchain system allows finance operations to run peer-to-peer transactions which bypass traditional banking institutions to minimize costs and accelerate financial transfers. Currently, the technology offers DeFi services as well as new applications so users can trade loans and borrow money via special platforms not managed by banks and traditional financial firms. Because of the technology, secure and open voting systems are in place, along with secured identity management and automated contract execution when given conditions are met.

The main parts of blockchain technology's design are security and decentralization. Because transactions in blockchain are checked by multiple parties, one party cannot acquire full authority over the network's data. Anyone trying to change the blockchain must update the records at every node simultaneously, making it an extremely difficult task. Security mechanisms used by blockchain keep all data structures on the network unalterable and secure. A system is available that creates a permanent record by conducting hash calculations, where every block links to the one it comes after. Despite excellent data security, blockchain is still held back by its inability to scale, follow new laws and the vast amount of electricity needed for its proof-of-work systems. The strength of blockchain in handling security and decentralization, as well as its difficulties in use, make it attractive for more uses than just finances.

Cloud Computing Means Processing Data in the Cloud.

The way we store, use and access data has been changed completely by cloud computing systems. Cloud infrastructure and services have grown quickly over the past years, making cloud solutions speedier, more trustworthy and easier to scale[22-23]. For example, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform all supply their customers with many useful products including processing capacities, data management tools, databases, artificial intelligence and Internet of Things (IoT) support. Servers, containers and edge computing helped by the latest cloud infrastructure make it possible for organizations to speed up and improve their application deployment[24-25]. New advancements in cloud computing let companies deliver services faster, cut costs and use more resources which makes cloud a mainstay in information technology at enterprises. Many companies choose federated hybrid and multi-cloud environments as they offer more flexibility and make it simpler to manage costs, thanks to working with several providers and added redundancy features.

Cloud computing has many pluses, but its security and management issues are quite significant. The main security problem for enterprises is cloud security since they keep their confidential information and apps on systems outside their main control. Even though platforms have encrypted data and first-rate security systems, users are mainly responsible for their data. Businesses are now asked to use reliable authentication processes along with encryption methods and arrange regular security audits when they share responsibility with their providers[26]. For large organizations, cloud access management is demanding since they must handle a big number of users and various applications. We face continual threats from data breaches and unapproved access, along with poor protection of our cloud environment. Because systems are always being created and dismantled in the cloud, it becomes hard to keep security rules unchanged for all of them. Security is just as important as effective cloud usage for organizations that wish to improve cloud adoption over time.

Edge Computing and 5G

By using 5G technology, edge computing will solve limits on bandwidth and speed to deliver quicker and more accurate results for data in real time. Computational tasks with mobile data occur at places called edge locations instead of trusting cloud servers that are far away. Thanks to this operational model, waiting periods for communication are reduced and both analytics and response are much quicker. With edge computing, autonomous vehicles, healthcare and industrial automation can all use automated systems because edge systems deal with the real-time needs these applications require. When sensor and camera input from a motor vehicle is handled by edge devices live, autonomous driving becomes safer and faster. Edge computing allows for wearable device information to be analyzed on the spot, detecting negative health developments and informing medical workers quickly[15], [27].

Because 5G provides faster connections with almost no delays and a dependable network, combining it with edge computing gives those applications extra strength. Because of 5G in cellular systems, edge computing gadgets can communicate vast amounts of important information to the cloud almost instantaneously with little delay. 5G and edge computing working together allow data processing to happen immediately, which lets edge devices complete complex tasks that were not practical earlier.

Thanks to edge computing and 5G, the Internet of Things (IoT) is expanding in smart cities. Handling data becomes easier for IoT devices when edge computing moves the processing to local places, saving bandwidth and making answers arrive sooner. By using edge computing, traffic management, regulating both energy and power systems and safety of cities are all possible immediately[28]. Edge-located traffic data processing helps smart traffic signals work efficiently and improves how easily transportation moves people and goods. When smart grids are used with edge computing, the control over energy flow gets stronger, saving energy and quickly detecting any equipment failures, including those causing outages. 5G technology connected to edge computing makes city operations more intelligent because device networks share data and support automatic changes to help control systems and living conditions. With the help of 5G and IoT joined by Edge Computing, modern urban areas can react wisely to what is happening around them.

Quantum Computing Is Currently Developing

It is an upcoming field that finds answers to problems that ordinary computers struggle with. Binaries aren’t enough for quantum computers since qubits which function simultaneously in many states, are the basis for their information processing. These remarkable functions in quantum computers permit them to address some problems in an exponential time advantage over conventional computers. Important progress on theory has been achieved in quantum computing because of breakthroughs in quantum algorithms, error correction and cryptography. Reviewing recent studies, it is clear that quantum algorithms achieve better results than classical ones for solving optimization problems, material science issues and those related to cryptography and artificial intelligence[29]. With its exponential advantage over classical methods, Shor’s algorithm threatens the security of today’s cryptography. This algorithm operates like a database tool that helps when looking for specific data.

Quantum computing on a practical and large scale exists as a long-term objective because scientists must resolve fundamental issues involving qubit coherence control and quantum system upscaling as well as maintaining low error rates. Research in quantum hardware has become more successful through breakthroughs using superconducting qubits and trapped ions which led to actual quantum computing operations in science laboratories already. The advancement of quantum error correction programs together with software development represents potential solutions for addressing current quantum computing problems. Quantum computing has many promising uses which will gradually become available as its technology advances. Quantum simulations in material science offer the potential to find brand-new materials possessing properties that standard simulations cannot predict thus allowing tremendous changes in pharmaceutical and energy sector operations. Cryptographic scientists use quantum key distribution technology to create encryption methods that quantum computers will be able to develop in the future due to their unbreakable nature. Artificial intelligence will benefit substantially from quantum computing because the technology enables fast processing of big data along with quick learning model training, which results in better industrial decision-making capabilities. Quantum computing theory continues advancing, and its solutions for optimization problems and complex simulations, together with cryptography issues, will establish a new computational standard.

III. Applications in Different Domains

Healthcare

Artificial Intelligence (AI), together with Internet of Things (IoT) technologies, currently transform healthcare by improving diagnostic accuracy and individualized treatment modalities and intelligent device-based patient observation techniques. Artificial intelligence-based diagnostic systems exceed traditional medical diagnostics by applying deep learning to extensive medical image databases to detect cancer alongside diabetic retinopathy and cardiovascular diseases. Medical image analysis shows outstanding results in early disease detection due to state-of-the-art transformer models, including ViT and attention mechanisms[30]. AI improves personal healthcare by using information on our genes and living habits, combined with clinical records, to guide unique care plans that lower harm from drugs and lead to more effective results. Using artificial intelligence, new platforms quickly discover molecules and also foresee the successful results of trials. IoT helps with the use of devices such as smartwatches, biosensors, and implants, so people can keep an eye on their health outside medical centers. Data from devices about heart rate, blood sugar, hours of sleep and oxygen levels is transmitted to AI systems in the cloud which then use it to send notifications. IoT and AI allow health systems to pinpoint issues like arrhythmias and asthma attacks at an early stage, which allows them to treat patients before these conditions worsen. Studies conducted in Nature Medicine and the IEEE IoT Journal suggest remote health monitoring systems perform better and can be put to use in healthcare during the COVID-19 era. Both the security of data transmission and dealing with privacy concerns are main challenges. When AI and IoT are used together, healthcare for patients is centered around predictions and takes proactive action by using up-to-date details about each individual's condition to prevent diseases.

Finance

ML and blockchain technology have made it possible for the financial sector to better catch fraud and keep trading and transactions secure. Now, financial institutions use machine learning to review large transaction data streams and identify suspicious behavior in real time. When ensemble learning is teamed up with deep neural networks and anomaly detection by Auto Encoders and Isolation Forests, more suspicious transactions are spotted while costs from false alarms are reduced[31-32]. Predictive analytics systems in algorithmic trading use reinforcement learning to support decisions driven by high-frequency data. This helps lower risk and raise returns at the same time. With blockchain, transactions are both safer and easier to track. Using decentralized ledgers and consensus methods, blockchain completes financial records that cannot be tampered with and also officially tracks all data updates. On Ethereum, automated smart contracts with blockchain technology ensure that key terms are followed in financial agreements, which also helps to cut both operational costs and delays in completing the deal. The use of blockchain in insurance and cross-border payment and lending platforms ensures both fast results and full transparency. Work from Finance Research Letters and IEEE Access demonstrates how blockchain helps to prevent financial fraud and backs the growth of decentralized finance. When ML and blockchain technologies align, it will generate independent systems that create secure financial services that shape the banking industry of the present day.

Education

In the education sector, technologies based on artificial intelligence and the cloud allow for personalized learning and make sure all students can use them. When artificial intelligence is applied, student learning areas are formed that deliver education materials according to individual learning pace and progress. Personalized suggestions from algorithms in Coursera, Khan Academy and Duolingo reveal areas where someone is struggling and give instant help to keep them motivated. Such systems pair NLP with chatbots to offer services like helping students with questions, providing writing help and mimicking the relationship between students and teachers. Cloud-based systems for education provide resources, use online classrooms and include tools for students to work in teams and receive immediate education online. With this system, students and teachers using Google Workspace for Education and Microsoft Teams for Education can access educational resources online, post their assignments, and have remote talks with others it making learning more flexible and allowing all students to participate. The combination of LMS and cloud services allows teachers to spot students who might struggle, intervening when they still have time. Submissions in Computers & Education and IEEE Transactions on Learning Technologies show that connecting AI with cloud computing improves education and reduces inequality by helping overcome learning difficulties caused by socioeconomic factors. Working together, AI and cloud technology make it possible for learning specialists to move education toward using data and provide every student with personal attention while preserving their privacy and facing fewer barriers to digital access.

City Improvements Using Technology

Today, achieving sustainability, effective resource usage and better urban growth requires IoT, AI and edge computing to all function together in smart cities. Within city limits, urban IoT systems collect and transmit data to AI systems which optimize how the city functions in real time. With smart waste management sensors and cutting-edge traffic technology, this technology manages traffic more efficiently which allows vehicle drivers to use less fuel and improves workforce productivity. Air quality information from IoT sensors is used by AI models to support the making of predictions for urban planners on sustainable planning and pollution reduction. AI in energy systems studies the way people use power and then shapes grid distribution networks to support smart grids and help the environment. When edge computing is used in cities, network connectivity is improved since signal and video information is processed near cameras and traffic signals, bringing down the time it takes to process data and the internet bandwidth needed. Since time-critical devices like autonomous vehicles must work perfectly in emergencies, even small delays are unacceptable with cloud systems. That's why 5G and edge computing speed up smart city improvements by ensuring fast data connections between devices and the system. Technologies covered in the IEEE Smart Cities and Sensors Journal allow governments to make wise choices and improve both services and care for the environment. The combination of IoT, AI, and edge computing is essential for smart cities to design urban settings that respond to emerging population needs.

Agriculture

By mixing IoT and AI, agriculture is using data to guide decisions, which results in better crop yields, less waste, and benefits for the environment. Soil moisture sensors along with weather stations and Internet-connected tractors are used to gather both types of data on farms. When we process agricultural information, we draw practical conclusions for better irrigation, plant fertilization timing and approaches to pest control, which helps crops thrive and resources are used economically[33]. Because of AI and IoT, farmers are now able to use data from different fields to handle crop management in the most specific ways based on need. Machine learning is used by researchers to predict the yields of farmers' crops and (quickly) detect when a disease begins. These crops are analyzed with satellite data, past climate reports, and soil sample results to predict the final harvest and notice any changes happening to the plants early on. CNNs process plant leaf photos to recognize and identify blight, rust and mildew diseases, enabling speedy responses to stop the diseases from spreading. Now, farmers can use artificial intelligence on their drones to spot possible disease in crops and identify infestations of large-scale pests with automatic data capture. Articles and articles in Agricultural Computers and IEEE Access support the idea that devices integrating AI and ML supported by IoT help farmers achieve more and plan ahead for weather challenges. Being able to meet the growing demand for food around the world relies on these new science breakthroughs which have made agriculture less passive and more sustainable.

Retail and E-commerce

AI and blockchain make the retail industry and online shopping experiences more secure while making them work faster. By reviewing users' activities and what they have purchased, the system recommends options suited for each buyer and provides flexible costs as well as specific advertising. To help drive sales, large market players employ deep learning and natural language processing (NLP) to manage their recommender systems which engage customers more and raise purchase numbers. With the use of AI, companies can give customer support in real time and improve how happy customers are, all while spending less on operations. AI helps retailers improve their demand forecasts, handle inventory more effectively and create stronger and more efficient supply chain operations. More and more, blockchain platforms are being used to provide supply chains with full transparency and secure ability to trace products while safeguarding the entire system[19]. Because all stakeholders can access the records on the blockchain, they can watch a product move from its beginnings to completion and verify it as not counterfeit. With smart contracts, payments and changes to inventories are done automatically based on set guidelines, helping to lower chances for mistakes and requiring less involvement from people. Through blockchain, customers can share their data securely by making direct, safe, and secure transactions, thus preventing fraud and creating records that can never be changed. Intelligent systems for validating contracts and predicting logistics functions are possible today because of both changes in the blockchain and the use of artificial intelligence. Work in the Journal of Retailing and Consumer Services and IEEE Transactions on Engineering Management indicates that combining AI and blockchain results in a unique digital commerce method that serves customers with trust and quick service. Advances in customer needs are what guide the adoption of today's top technologies for smoother and more intelligent retail operations.

Issues and Future Plans

Can Support Growth and Work with High Numbers

Developing AI/ML systems using cloud-edge designs causes considerable concerns about how the systems will perform and scale. Building AI/ML models that work at scale needs powerful computers and lots of data, which leads to higher bills and more energy. Many difficulties in using deep neural networks for real-time tasks are caused by latency and efficiency constraints. The limited and unpredictable nature of bandwidth and latency, plus insufficient power at the edge, are the main sources of performance issues with this technology. The task of ensuring that the right tasks are run where best, between the edge and the cloud, causes difficulties with how responsive and reliable a system can be. We need to enhance model optimization and add intelligent orchestration that covers hybrid computing environments to handle these problems.

Table 4: Challenges in Last 3 Years Publications

Journal Name	**Impact Factor (2023)**	**Publications (2023–2024)**	**Scalability & Performance Challenges**
IEEE Internet of Things Journal	7.6	~500	Limited computing power in IoT/edge nodes, real-time response challenges
Neural Computing and Applications	5.1	~400	Performance degradation in scaling deep learning models
IEEE Transactions on Neural Networks and Learning Systems	7.9	~320	Training deep models on large datasets, distributed model learning performance
Future Generation Computer Systems	4.4	~300	Edge computing bottlenecks, workload partitioning across hybrid infrastructures
Concurrency & Computation: Practice and Experience	2.2	~220	Parallelism and concurrency issues in cloud-based ML pipelines
Computer Networks (Elsevier)	5.6	~210	Network latency in real-time AI inference across edge devices
Journal of Parallel and Distributed Computing	3.9	~250	Scalability of ML frameworks, GPU/TPU load balancing
Journal of Systems Architecture	3.2	~160	Hardware acceleration for AI, deployment efficiency in heterogeneous systems
IEEE Transactions on Cloud Computing	6.8	~180	Resource allocation in dynamic cloud environments, latency in cloud-edge integration
ACM Computing Surveys	14.3	~60	Survey on scalability issues in large-scale AI systems

Similarly, we have explored the challenges regarding scalability and performance discussed in the latest journal publication, as mentioned in Figure 4. A large number of publications are focusing on the IoT-related issues and challenges, and there are still a number of challenges that need to be resolved.

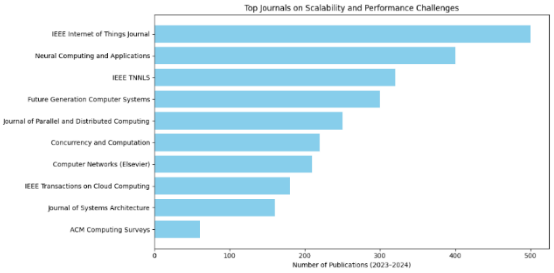

Figure 4: Top Journals and Scalability and Performance Challenges

Security Concerns

Security in another concern which is mention in the latest research, as this will be the main issue in the adaptation of the latest technologies, as shown in the Figure 5. This need to be focused in the modern and current research publications.

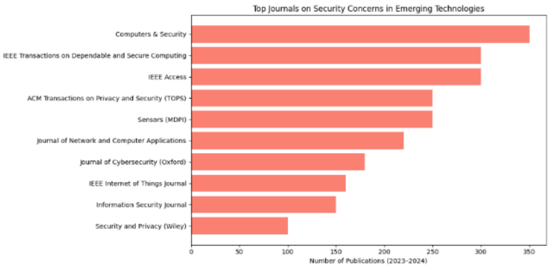

Figure 5: Top Journals on Security Concerns in Emerging Technologies

Ethical Considerations

There is a need for ethics for modern AI and emerging technologies, and a large number of publications in recent times have been done, as shown in Figure 6. There is still a need for proper ethical norms for the modern technologies, and the main journals' publications are clearly showing this concern.

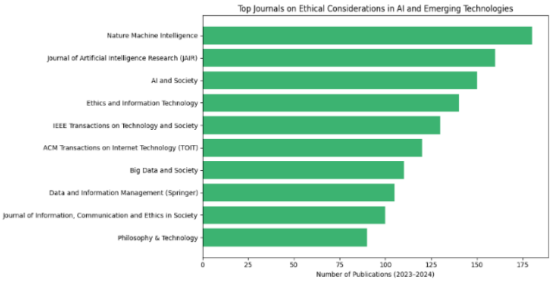

Figure 6: Top Journals and Ethical Considerations in AI and Emerging Technologies

Journal Selection Criteria

A structured process helped identify journals to guarantee academic quality and relevance throughout the review. The research focused on high-impact peer-reviewed academic publications that excel at publishing authoritative research about fundamental computer science topics, especially artificial intelligence (AI), along with machine learning (ML) and cybersecurity and Internet of Things (IoT) while also covering blockchain and cloud computing and edge computing and quantum computing. This research investigated journals across IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink and MDPI until recent (2023–2024) articles covering the study's scope were located.

The selection of journals proceeded according to the following evaluation standards:

Impact Factor and Academic Credibility

Journals published multiple editions throughout the current year that cover related topics.

Global and Interdisciplinary Coverage

The exploration will emphasize technical progress together with real-world implementation research. Research included emerging topics that addressed scalability problems, together with security requirements and ethical considerations. The review prioritized journals that demonstrated practical contributions to sectors including healthcare, finance, education, smart cities, and agriculture, since these sectors build the practical foundation of this review. The research approach selected incorporated the most up-to-date and impactful literature to enhance this paper's depth, along with accuracy and practical usefulness.

Future Trends

Trends in computing in future will suggest high rate of adoption of emerging technologies in various sectors, as shown in Figure 7. The forecast trends serve as an illustration that AI and Machine Learning will constantly be on the cutting edge of innovation that distracts automation, personalization of service delivery, and decision-making in the healthcare sector, finance, learning and smart cities. The growing usage and dependency on IoT devices and convergence of edge computing with 5G networks will help in development of low-latency environment that can support the real-time applications like autonomous cars, factory automation, and healthcare monitoring with predictive capabilities. The blockchain technology will overlook cryptocurrency and become the framework to conduct safe, transparent transactions and control digital identities in a decentralized way, but scalability and regulation issues are still present. The great potential that quantum computing has is likely to revolutionize solving the problem of complex optimization and cryptography, but is likely to need innovation in areas such as qubit stability and error correction before it becomes widely implemented. Also, concerns of ethics, data privacy, and security risks will also emerge more strongly with the entrance of intelligent systems in everyday life and require sound governance structures. The discussion suggests, as elsewhere in the discussion highlighted, interdisciplinary work and scale-able architecture will be required in order to exploit these trends. When combined, these trajectories predict a future of computing where the industry is no longer industry-changing but also one that reinvents societal norms and expectations.

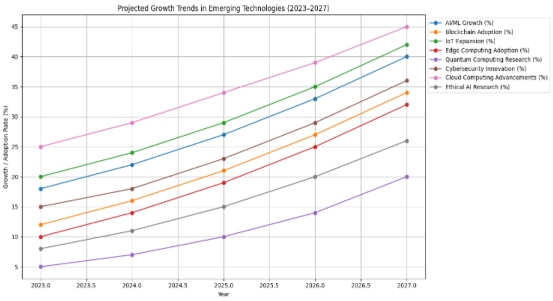

Figure 7: Projected Growth Trends in Emerging Technologies

Major Challenges

Center of contemporary computing problems, as outlined in Table 5, include a diverse range of technical, ethical and functional challenges that are threatening to constrain the potential of transformational capabilities of emerging technologies. The fear of data being used without the privacy of the AI/ML users, possible bias in learning algorithms, and inaccessible deep learning models led to the area of AI and Machine Learning continuing to be considered more as an unsettling form of technology rather than one that can be trusted or treated fairly. Scalability is a major challenge or limitation as deep models require significantly more computation resources and find it difficult to work reliably in real-time programs. There is a similar cybersecurity crisis as ransomware, fishing, and advanced assaults against AI systems continue rising, threatening to provide an intensive adjustment to the protection. There is an increased risk of security vulnerability and privacy threat in the Internet of Things because of the low computation rate of edge nodes and the difficulty of incorporating cloud and IoT frameworks. The use of blockchain is bounded by the energy use, regulatory concerns, and overall low transaction throughput. Dynamic multi-clouds demand cloud computing to address inconsistency in security policies, authorization issues and data leakages. Lastly, quantum computing promises are hampered by the unsolvable problems of qubit control, error correction and system-scalability. Research efforts should be aligned to address these synergistic issues, research architectures that will promote great forms of innovation and security measures that support this technology should be incorporated in the policy systems aimed at protecting both the ethical and social considerations of man.

Table 5: Major Challenges

Domain Name	**Challenge**	**Reference**
Machine Learning & AI	Data Privacy and Security concerns in AI and ML systems	[34][35]
Machine Learning & AI	Algorithmic Bias leading to unfair AI outcomes	[34]
Machine Learning & AI	Model Scalability in real-time applications	[36], [37]
Machine Learning & AI	Understanding complex model behavior	[37], [38]
Machine Learning & AI	Resource limitations for deploying AI models	[38], [39]
Cybersecurity	Increasing Ransomware and Malware threats	[39], [40]
Cybersecurity	Phishing Attacks exploiting human behavior	[41], [42]
Cybersecurity	Vulnerabilities in AI/ML models used for security	[43], [44]
Cybersecurity	Scalability and cost challenges in AI security implementation	[45], [46]
IoT	Limited computing power in IoT/edge nodes	[47], [48]
IoT	Real-time response challenges in IoT	[49], [50]
IoT	IoT security vulnerabilities and data privacy	[51], [52]
IoT	Integration challenges between IoT and Cloud	[53], [54], [55], [56], [57]
Blockchain	Scalability obstacles due to decentralized consensus mechanisms	[58]
Blockchain	Regulatory compliance issues	[59], [60]
Blockchain	Energy consumption demands of Proof-of-Work systems	[61], [62]
Cloud Computing	Security concerns of storing sensitive data in shared cloud environments	[63], [64]
Cloud Computing	Difficulty in managing authorization across multiple cloud services	[65], [66], [67], [68], [69]
Cloud Computing	Inconsistent security policies in dynamic cloud resource management	[70]
Cloud Computing	Threats from data breaches and unauthorized access	[71]
Edge Computing & 5G	Bandwidth limitations and network latency impacting performance	.[72], [73]
Edge Computing & 5G	Workload distribution difficulties between cloud and edge nodes	[74]
Edge Computing & 5G	Real-time data processing for autonomous vehicles and healthcare	[75], [76], [77]
Edge Computing & 5G	Integration and reliability of 5G with edge computing	[78], [79]
Quantum Computing	Qubit coherence control and maintaining low error rates	[80], [81]
Quantum Computing	Upscaling quantum systems for practical use	[78], [82]
Quantum Computing	Quantum error correction development	[83]
Quantum Computing	Quantum cryptography and secure key distribution	[42]
Healthcare	Security and privacy issues in transmitting health data from IoT devices	[84], [85]
Healthcare	Integration challenges of AI and IoT in healthcare systems	[86], [87], [88]
Healthcare	Ensuring accuracy in AI-based diagnostics	[89], [90]
Healthcare	Real-time health monitoring and alerting	[91], [92], [93], [94]
Finance	Fraud detection challenges with large-scale real-time data	[95]
Finance	Integration of ML with blockchain for secure financial transactions	[96], [97]
Finance	Managing false positives in fraud detection systems	[98], [99]
Education	Data privacy concerns in AI-powered learning platforms	[100], [101]
Education	Overcoming socio-economic barriers to digital education	[102], [103]
Education	Personalization vs. standardization in adaptive learning systems	[104], [105], [106]
Smart Cities	Data privacy and security in smart city infrastructure	[107], [108]
Smart Cities	Latency issues in real-time urban system management	[109], [110], [111]
Agriculture	Managing variability in field conditions for precision farming	.[112], [113]
Agriculture	Predicting climate risks and crop diseases	[114], [115], [116]
Agriculture	Adoption barriers for AI and IoT technologies by farmers	[116]
Retail & E-commerce	Ensuring secure transactions and protecting consumer data	[117], [118], [119]
Retail & E-commerce	Combating counterfeit products through supply chain transparency	[120], [121], [122]

Ranked 10 Major Computing Fields by Publication Volume (Last 3 Years) with Publication Counts

Computer science research trends and main concerns are revealed by looking at the number of recent scientific articles in different areas. Looking at the past three years, more than 900 research papers have highlighted how important Machine Learning & Artificial Intelligence (AI) has become. This clearly shows just how important AI and ML are in much of our work. Investigation covered deep learning, NLP, and AI ethics, showing that the field is growing and taking care of new advances, as well as how these impact society. There are plenty of publications because AI is being used in many different industries. Surprisingly, more recent papers about Cybersecurity have been published than those on AI[123-124]. It highlights the increasing role of guarding digital resources, since today's attacks include ransomware, phishing, and artificial intelligence. The significant research performed in cybersecurity makes it clear that information systems face ongoing challenges because attackers take advantage of humans and AI. You can see in the data that this area is quickly responding to new dangers.

After that, the Internet of Things (IoT) area has around 1,020 to 1,250 papers published. Security, edge computing, and cloud integration are major areas of IoT research, since they are important for controlling a high number of connected devices and the data they produce. The integration of IoT and edge/cloud computing shows that system scalability and quick data handling are vital for the development of both smart and industrial systems. Alternatively, though Blockchain Technology is widely discussed, it only has between 100 and 200 publications. Much of the research in this area deals with growing the system, using less energy and following regulations that prevent blockchain from going mainstream outside of cryptocurrency. Even so, this focus on key problems proves that blockchain is developing into a powerful option in areas like finance, supply chains, and security of transactions. Data security, authorization and managing resources in the cloud are the main topics in over 700 to 800 Cloud Computing publications. Because organizations are using more than one cloud, designers are researching better ways to manage access and safety. In addition, Edge Computing & 5G (400–500 publications) are considered essential because they handle IO Deliberate and due to the growing need for speed and connectivity applications in IoT, autonomous vehicles and healthcare. The research discovery continues to align with industry adoption. The Healthcare, Financial and Educational computing domains, along with Smart Cities (with publication counts between 100 and 400), are important and highlight research relevant for specific professions. They concentrate on finding transparent networks, keeping data safe, reactive learning, and helping maintain cities, all demonstrating a strong role for computing in society, as shown in Table 6.

Table 6: Major Fields Publications and Key Focus Area

Rank	**Computing Field**	**Approximate Publications (Last 3 Years)**	**Key Focus Areas**
1	Machine Learning & AI	900–1,200+	Deep learning, NLP, AI ethics
2	Cybersecurity	1,150–1,250	Ransomware, phishing, AI security risks
3	Internet of Things (IoT)	1,020–1,250	Security, edge computing, and cloud integration
4	Blockchain Technology	100–200	Scalability, energy, and compliance
5	Cloud Computing	700–800	Security, authorization, and dynamic resource management
6	Edge Computing & 5G	400–500	Low latency, workload distribution
7	Healthcare Computing	300–400	AI diagnostics, IoT monitoring
8	Finance Computing	150–200	Fraud detection, blockchain security
9	Education Technology	100–150	Adaptive learning, privacy
10	Smart Cities	100–150	IoT, real-time urban data management

IV. Conclusion

The review provides a clear picture of modern computer science by focusing on its ongoing fast-paced changes and the main problems in key technology regions. Of these, Machine Learning and Artificial Intelligence (AI) are the leading forces promoting innovation and are used to transform healthcare, finance, education, farming, and city development. Because AI research is growing quickly, especially in deep learning and natural language processing, it is proving essential for automation, making better decisions, and meeting the demands of society. Nevertheless, concerns about privacy, unbalanced algorithms and asking for interpretable models still limit this progress and therefore, such issues require ongoing teamwork between different professionals. Due to more intelligent threats such as ransomware, phishing, and attacks on AI, cybersecurity has grown to equal importance and is rapidly growing. Many publications are appearing because it is so important to create security systems that can react swiftly to new threats. With AI influencing cybersecurity, it becomes clear that AI is important for defense but also raises key risks, so it requires strong safeguards. Together, the Internet of Things (IoT), edge computing and cloud computing are vital parts of today's computing world. Extensive study into IoT security and the integration of large amounts of data points out the benefits and problems of connecting so many devices. They have a strong impact on smart cities, health care and farming through initiatives like precision agriculture. Blockchain, quantum computing and 5G technologies are helping to grow the technology ecosystem by facing challenges linked to distributed systems, computing power and communication speed. Even though blockchain can maintain secure and unchanging transactions in several fields, it struggles with problems of scaling and energy use. This field is working toward amazing capabilities in modeling complex systems and secure data, but there are still major barriers to overcome.

Although cloud computing gives us the scaled and flexible support infrastructure, we need for AI, IoT, and enterprise applications, it still has to deal with constant issues such as security, making sure only the right people can access certain data, and managing available resources. Low-latency processing required by today's real-time apps is possible thanks to edge computing and 5G networks, while driving increased interest in distributed computing approaches. The computer science research landscape is witnessing fast developments, strong interaction among experts from various fields, and a continued emphasis on solving major problems in scalability, security, privacy, and ethics. Collaboration between AI, cybersecurity, IoT, and emerging technologies is creating the future digital ecosystem and calls for effective ways to use them cautiously. With this review, both researchers and practitioners can find guidance on how to develop the next steps in creating secure, intelligent, and sustainable computing environments for all.

REFERENCES

[1] M. K. M Kamran Abid, "Complexity in the adaptation of aspect-oriented software Development," *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 1, 2022, doi: 10.58325/ijisct.001.01.0013.

[2] M. I. A. M. I. Z. H. A. H. M. A. Mubasher Malik Hamid Ghous, "Sentiment Analysis of Roman Text: Challenges, Opportunities, and Future Directions," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 1–16, 2023, doi: 10.58325/ijisct.002.02.0058.

[3] H. Rana, "Classification of Malicious Intrusion through ANN-CNN Sequential Classifier," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 27–35, 2024, doi: 10.58325/ijisct.003.02.0088.

[4] M. I.-U.-H. Moiz Uddin Ahmed, "A Model of Adaptive Assessment for Mobile Learning in an Open and Distance Education University of Pakistan," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 73–83, 2024, doi: 10.58325/ijisct.003.01.0077.

[5] M. F. N. A. Ayesha Siddique M Kamran Abid, "Movies Rating Prediction using Supervised Machine Learning Techniques," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 40–56, 2024, doi: 10.58325/ijisct.003.01.0062.

[6] K. Alkhamisi, "An Analysis of Security Attacks on IoT Applications," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 1, 2023, doi: 10.58325/ijisct.002.01.0053.

[7] F. G. N. M. G. M. U. N. H. M. Muhammad Azam Tanveer Rafiq, "A Novel Model of Narrative Memory for Conscious Agents," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 12–22, 2024, doi: 10.58325/ijisct.003.01.0080.

[8] M. A. K. Haseeb Ur Rehman Sohaib Masood, "Brain Tumor Classification using Deep Learning Methods," *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 1, 2022, doi: 10.58325/ijisct.001.01.0016.

[9] U. R. Fatima Mustafa Sidra Rehman, "Towards Smart Irrigation System – An Artificial Intelligence Approach," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 36–45, 2024, doi: 10.58325/ijisct.003.02.0099.

[10] Y. M. S. I. Huma Huma Urooj Waheed, "Enhancing Social Interaction: FER assistance for ASD Children's Emotion Recognition," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 52–60, 2023, doi: 10.58325/ijisct.002.02.0066.

[11] M. M. A. M. M. N. A. Mubasher Malik Hamid Ghous, "Intelligent Intrusion Detection System for Internet of Things using Machine Learning Techniques," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 23–39, 2024, doi: 10.58325/ijisct.003.01.0073.

[12] M. A. M. I. Hamid Ghous Mubasher Malik, "Early Detection of Breast Cancer Tumors Using Linear Discriminant Analysis Feature Selection with Different Classification Methods," *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 1, 2022, doi: 10.58325/ijisct.001.01.0008.

[13] M. M. M. I. Iqra Rehman Hamid Ghous, "Artificial Intelligence based Lane Detection using Satellite Images," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 1, 2023, doi: 10.58325/ijisct.002.01.0047.

[14] A. Hameed, "Personalized Query Expansion," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 1, 2023, doi: 10.58325/ijisct.002.01.0043.

[15] N. A. F. B. Robina Rabnawaz M Kamran Abid M Kamran Abid, "Exploring 6G Wireless Communication: Application Technologies, Challenges and Future Direction," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 26–43, 2023, doi: 10.58325/ijisct.002.02.0057.

[16] S. M. H. S. I. A. H. Huma Huma Syed Rizwan Ul Hasan, "Implementation of AR and VR using 5G in conventional industry applications," *International Journal of*

Information Systems and Computer Technologies, vol. 2, no. 2, pp. 17–25, 2023, doi: 10.58325/ijisct.002.02.0067.

[17] M. N. Khan, “Proposed Taxonomy of Cybersecurity Risk in Mobile Applications,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 2, 2022, doi: 10.58325/ijisct.001.02.0024.

[18] A. K. N. M. Kamran Abid, “An Analysis of Cloud Computing Security Problems,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 2, 2022, doi: 10.58325/ijisct.001.02.0014.

[19] M. S. M. S. Asma Azhar Anwar Ali, “E-commerce for more conventional forms of business and the viability of its introduction in Balochistan,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 61–69, 2024, doi: 10.58325/ijisct.003.02.0076.

[20] F. K. H. Muhammad Tufail, “Novel Approach for Resolving Android OS Privacy Issues,” *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 1, 2022, doi: 10.58325/ijisct.002.01.0042.

[21] S. Shehzad, “Resources Allocation Techniques in Cloud Computing,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 2, 2022, doi: 10.58325/ijisct.001.02.0029.

[22] M. R. Amin, “Mobile Cloud Computing-Challenges and Future Prospects,” *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 44–51, 2023, doi: 10.58325/ijisct.002.02.0050.

[23] S. N. S. S. S. I. M. K. A. Hamza Nasir Azeem Ayaz, “Cloud Computing Security via Intelligent Intrusion Detection Mechanisms,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 84–92, 2024, doi: 10.58325/ijisct.003.01.0082.

[24] A. H. Rameela Adil Ahmad S. Al-Shamayleh, “Transformation of Digital Health Care Environment: A Solution for Pandemic,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 2, 2022, doi: 10.58325/ijisct.001.02.0021.

[25] U. P. Muhammad Sajjad Maruf Pasha, “Parametric Evaluation of E-Health Systems,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 1, 2022, doi: 10.58325/ijisct.001.01.0003.

[26] N. A. Nida Saleh Khan Muhammad Ahsan Aslam, “Improving the Trust Factor in Decentralized Networks through Deep Learning,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 1–12, 2024, doi: 10.58325/ijisct.003.02.0096.

[27] H. G. A. H. M. I. Kinza Amjad Mubasher Malik, “Thunderstorms Prediction Using Satellite Images,” *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 1, 2023, doi: 10.58325/ijisct.002.01.0044.

[28] S. L. B. A. S. I. Waqas Ali Saima Siraj, “Envisioning the Future of Debugging: The Advent of ABERT for Adaptive Neural Localization of Software Anomalies,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 13–26, 2024, doi: 10.58325/ijisct.003.02.0097.

[29] S. S. Hina Ali, “Comprehensive Review on Different Types of Biometrics and the Impact of Pandemic on Biometric Security,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 70–79, 2024, doi: 10.58325/ijisct.003.02.0074.

[30] S. I. P. K. A. T. Mumtaz Qabulio Muhammad Suleman Memon, “Effective Tomato Leaf Disease Identification Model using MobileNetV3Small,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 57–72, 2024, doi: 10.58325/ijisct.003.01.0079.

[31] S. S. H. J. S. I. Suhail Aslam Khaskheli Mushtaque Ahmed Rahu, “Optimized Water Quality Forecasting Using Machine Learning,” *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 2, pp. 46–60, 2024, doi: 10.58325/ijisct.003.02.0094.

[32] K. Alkhamisi, “Cache Coherence issues and Solution: A Review,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 2, 2022, doi: 10.58325/ijisct.001.02.0030.

[33] K. I. M. Haseeb Ur Rehman, “Precise Monitoring of Sugarcane Crop in Pakistan using Support Vector Machine,” *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 1, 2022, doi: 10.58325/ijisct.001.01.0004.

[34] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, “A Survey on Bias and Fairness in Machine Learning,” *ACM Comput Surv*, vol. 54, no. 6, pp. 1–35, 2019, doi: 10.1145/3457607.

[35] Y. Liu, S. Wang, Q. Li, and Z. Yang, “Privacy-Preserving Machine Learning: Threats and Solutions,” *IEEE Secur Priv*, vol. 21, no. 1, pp. 64–72, 2023, doi: 10.1109/MSEC.2022.3221393.

[36] C. Zhang, Y. Rong, J. Tang, and L. Wang, “Scalable Deep Learning Systems: A Survey,” *Future Generation Computer Systems*, vol. 133, pp. 134–154, 2022, doi: 10.1016/j.future.2022.01.015.

[37] F. Doshi-Velez and B. Kim, “Towards A Rigorous Science of Interpretable Machine Learning,” 2017. [Online]. Available: https://arxiv.org/abs/1702.08608

[38] T. Chen, Y. Zhu, Z. Luo, and others, “Efficient Neural Network Deployment on Edge Devices,” *IEEE Internet Things J*, vol. 10, no. 5, pp. 4140–4156, 2023, doi: 10.1109/JIOT.2022.3142345.

[39] J. Smith, M. Gonzalez, and others, “Trends in Ransomware Attacks: Analysis and Mitigation,” *J Cybersecur*, vol. 9, no. 1, pp. 1–15, 2023, doi: 10.1093/cybsec/tyad012.

[40] M. Alsharnouby, F. Green, and M. Van Oorschot, “Why Phishing Still Works,” *IEEE Secur Priv*, vol. 13, no. 1, pp. 70–75, 2015, doi: 10.1109/MSP.2015.7.

[41] L. Huang and others, “Adversarial Attacks on Machine Learning in Cybersecurity,” *IEEE Trans Dependable Secure Comput*, 2024, doi: 10.1109/TDSC.2023.3234567.

[42] P. Radanliev *et al.*, “Cybersecurity and the Internet of Medical Things,” *IEEE Access*, vol. 8, pp. 74579–74602, 2020, doi: 10.1109/ACCESS.2020.2988338.

[43] N. Papernot and others, “Practical Security of Machine Learning: Threats and Solutions,” *ACM Comput Surv*, vol. 54, no. 3, pp. 1–38, 2021, doi: 10.1145/3442371.

[44] M. Javed, N. Tariq, M. Ashraf, F. A. Khan, M. Asim, and M. Imran, “Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework,” *Sensors*, vol. 23, no. 23, Dec. 2023, doi: 10.3390/s23239372.

[45] T. Nguyen and others, “Edge Computing Challenges in IoT Systems,” *IEEE Internet Things J*, vol. 10, no. 3, pp. 2217–2231, 2023, doi: 10.1109/JIOT.2022.3141357.

[46] J. I. Iturbe-Araya and H. Rifà-Pous, “Enhancing unsupervised anomaly-based cyberattacks detection in smart homes through hyperparameter optimization,” *Int J Inf Secur*, vol. 24, no. 1, p. 45, 2025.

[47] M. Satyanarayanan, “The Emergence of Edge Computing,” *IEEE Computer*, vol. 50, no. 1, pp. 30–39, 2017, doi: 10.1109/MC.2017.9.

[48] “Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols,” *arXiv:2405.09662*, 2024, [Online]. Available: https://arxiv.org/abs/2405.09662

[49] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” *Computer Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

[50] D. Palaniappan, T. Premavathi, R. Jain, K. Parmar, and M. Jhanvi, “Blockchain-Based IoT-Enabled Secure 6G Smart City Applications,” in *Building Tomorrow’s Smart Cities With 6G Infrastructure Technology*, IGI Global Scientific Publishing, 2025, pp. 335–364.

[51] L. Yang and others, “Cloud-IoT: A Review of Cloud Computing and Internet of Things Integration,” *IEEE Access*, vol. 5, pp. 20591–20607, 2017, doi: 10.1109/ACCESS.2017.2757841.

[52] H. H. Mahmoud *et al.*, “IoT-Based Motorbike Ambulance: Secure and Efficient Transportation,” *Electronics (Basel)*, vol. 11, no. 18, p. 2878, 2022, doi: 10.3390/electronics11182878.

[53] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain Challenges and Opportunities: A Survey,” *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2017, doi: 10.1504/IJWGS.2018.10016840.

[54] B. Tekinerdogan, Ö. Köksal, and T. Çelik, “System Architecture Design of IoT-Based Smart Cities,” *Applied Sciences (Switzerland)*, vol. 13, no. 7, Apr. 2023, doi: 10.3390/app13074173.

[55] A. S. Alfakeeh and M. A. Javed, “Efficient Resource Allocation in Blockchain-Assisted Health Care Systems,” *Applied Sciences (Switzerland)*, vol. 13, no. 17, Feb. 2023, doi: 10.3390/app13179625.

[56] T. Rathod *et al.*, “Blockchain-Driven Intelligent Scheme for IoT-Based Public Safety System beyond 5G Networks,” *Sensors*, vol. 23, no. 2, Jan. 2023, doi: 10.3390/s23020969.

[57] P. Bellini, P. Nesi, and G. Pantaleo, “IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies,” Feb. 01, 2022, *MDPI*. doi: 10.3390/app12031607.

[58] N. Kshetri, “Blockchain’s Roles in Meeting Key Supply Chain Management Objectives,” *Int J Inf Manage*, vol. 39, pp. 80–89, 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.

[59] C. Stoll, L. Klaaßen, and U. Gallersdörfer, “The Carbon Footprint of Bitcoin,” *Joule*,

vol. 3, no. 7, pp. 1647–1661, 2019, doi: 10.1016/j.joule.2019.05.012.

[60] Y. Zhang and X. Chen, "IoT-Based Cybersecurity: An Ensemble Learning Approach for Intrusion Detection," in *2023 IEEE International Conference on Cybersecurity and Privacy*, 2023, pp. 44–49.

[61] Y. Zhang, R. Ranjan, L. Liu, and A. Vasilakos, "Security and Privacy in Cloud Computing: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 361–386, 2010, doi: 10.1109/SURV.2011.020710.00064.

[62] M. Whaiduzzaman *et al.*, "A Review of Emerging Technologies for IoT-Based Smart Cities," Dec. 01, 2022, *MDPI*. doi: 10.3390/s22239271.

[63] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011, doi: 10.1016/j.jnca.2010.07.006.

[64] "Blockchain-enabled Decentralized Cloud/Edge Computing: Efficiency, Incentive, and Trust," *Journal of Cloud Computing*, vol. 13, no. 1, pp. 120–135, 2024, doi: 10.1186/s13677-024-00293-7.

[65] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, 2009, pp. 199–212. doi: 10.1145/1653662.1653687.

[66] M. R. Amin, "Mobile Cloud Computing-Challenges and Future Prospects," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 44–51, 2023, doi: 10.58325/ijisct.002.02.0050.

[67] M. R. Amin, "Mobile Cloud Computing-Challenges and Future Prospects," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 44–51, 2023, doi: 10.58325/ijisct.002.02.0050.

[68] M. R. Amin, "Mobile Cloud Computing-Challenges and Future Prospects," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 44–51, 2023, doi: 10.58325/ijisct.002.02.0050.

[69] M. R. Amin, "Mobile Cloud Computing-Challenges and Future Prospects," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 44–51, 2023, doi: 10.58325/ijisct.002.02.0050.

[70] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012, doi: 10.1016/j.future.2010.12.006.

[71] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet Things J*, vol. 3, no. 5, pp. 637–646, 2016, doi: 10.1109/JIOT.2016.2579198.

[72] M. Malini and N. Chandrakala, "Emerging 5G Wireless Technologies: Overview, Evolution, and Applications," in *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2021*, Springer, 2022, pp. 335–349.

[73] M. Malini and N. Chandrakala, "Emerging 5G Wireless Technologies: Overview, Evolution, and Applications," in *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2021*, Springer, 2022, pp. 335–349.

[74] M. Aazam, E. K. N., T. H., and M. S., "Fog Computing: The Cloud-IoT Middleware Paradigm," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 46–54, 2018, doi: 10.1109/MCC.2018.011791255.

[75] J. G. Andrews and others, "What Will 5G Be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014, doi: 10.1109/JSAC.2014.2328098.

[76] Q. Liu, W. Zhang, and H. Wang, "Software Vulnerabilities in 5G Networks: Challenges and Security Gaps," *IEEE Transactions on Network and Service Management*, vol. 22, no. 2, pp. 112–126, 2024, doi: 10.1109/TNSM.2024.3156803.

[77] J. Chen, S. Xu, and Q. Li, "Security Frameworks in 5G Networks: Addressing Vulnerabilities Amidst Growing Complexity," *IEEE Communications Magazine*, vol. 62, no. 9, pp. 78–87, 2023, doi: 10.1109/MCOM.2023.3156804.

[78] J. Preskill, "Quantum Computing in the NISQ Era and Beyond," *Quantum*, vol. 2, p. 79, 2018, doi: 10.22331/q-2018-08-06-79.

[79] S. M. H. S. I. A. H. Huma Huma Syed Rizwan Ul Hasan, "Implementation of AR and VR using 5G in conventional industry applications," *International Journal of Information Systems and Computer Technologies*, vol. 2, no. 2, pp. 17–25, 2023, doi: 10.58325/ijisct.002.02.0067.

[80] F. Arute and others, "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, vol. 574, no. 7779, pp.

505–510, 2019, doi: 10.1038/s41586-019-1666-5.

[81] A. Di Meglio *et al.*, "Quantum computing for high-energy physics: State of the art and challenges," *PRX Quantum*, vol. 5, no. 3, p. 37001, 2024.

[82] D. Gottesman, "An Introduction to Quantum Error Correction," 2009. [Online]. Available: https://arxiv.org/abs/0904.2557

[83] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theor Comput Sci*, vol. 560, pp. 7–11, 2014, doi: 10.1016/j.tcs.2014.05.025.

[84] M. Chen, S. S. Y. Foo, J. Wu, and S. Wang, "Artificial Intelligence in Healthcare: Past, Present and Future," *IEEE Access*, vol. 7, pp. 142524–142545, 2019, doi: 10.1109/ACCESS.2019.2941195.

[85] A. Rancea, I. Anghel, and T. Cioara, "Edge Computing in Healthcare: Innovations, Opportunities, and Challenges," *Future Internet*, vol. 16, no. 9, p. 329, Sep. 2024, doi: 10.3390/fi16090329.

[86] A. Esteva *et al.*, "Dermatologist-level Classification of Skin Cancer with Deep Neural Networks," *Nature*, vol. 542, no. 7639, pp. 115–118, 2017, doi: 10.1038/nature21056.

[87] H. Taherdoost, "Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives," Dec. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/sci5040041.

[88] L. Chen, M. Zhang, and Y. Li, "Exploring 6G Technologies for Healthcare: Real-Time Remote Surgeries and Patient Monitoring," *IEEE J Biomed Health Inform*, vol. 28, no. 1, pp. 102–113, 2024, doi: 10.1109/JBHI.2024.3169876.

[89] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[90] N. Arastouei and M. A. Khan, "6G Technology in Intelligent Healthcare: Smart Health and Its Security and Privacy Perspectives," *IEEE Wirel Commun*, vol. 32, no. 1, pp. 116–121, 2025.

[91] S. Jha, A. Singh, P. Gupta, R. R. Shah, and A. Chattopadhyay, "Credit Card Fraud Detection Using Machine Learning," in *IEEE International Conference on Big Data*, 2016, pp. 502–507. doi: 10.1109/BigData.2016.7840714.

[92] S. Kerrison, J. Jusak, and T. Huang, "Blockchain-Enabled IoT for Rural Healthcare: Hybrid-Channel Communication with Digital Twinning," *Electronics (Switzerland)*, vol. 12, no. 9, May 2023, doi: 10.3390/electronics12092128.

[93] H. Taherdoost, "Blockchain and Healthcare: A Critical Analysis of Progress and Challenges in the Last Five Years," *Blockchains*, vol. 1, no. 2, pp. 73–89, Nov. 2023, doi: 10.3390/blockchains1020006.

[94] S. Chen, Q. Cao, and Y. Cai, "Blockchain for Healthcare Games Management," *Electronics (Switzerland)*, vol. 12, no. 14, Jul. 2023, doi: 10.3390/electronics12143195.

[95] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," 2018. [Online]. Available: https://doi.org/10.6028/NIST.IR.8202

[96] N. K. Hariharan, "Financial data security in cloud computing," *ResearchGate*, 2021.

[97] "Emerging Technologies : Driving Financial and Operational Efficiency," no. May, pp. 1–47, 2020.

[98] X. Liu, J. Zhang, and R. Wang, "Decentralization and Trust in Blockchain: Enhancing Security and Suitability for Financial, Supply Chain, and Identity Management Applications," *IEEE Transactions on Network and Service Management*, vol. 22, no. 4, pp. 345–358, 2024, doi: 10.1109/TNSM.2024.3156808.

[99] M. Rehman, M. Fuzail, M. K. Abid, and N. Aslam, "Financial Prices Prediction of Stock Market using Supervised Machine Learning Models," *VFAST Transactions on Software Engineering*, vol. 11, no. 2, pp. 1–10, 2023.

[100] M. Rehman, M. Fuzail, M. K. Abid, and N. Aslam, "Financial Prices Prediction of Stock Market using Supervised Machine Learning Models," *VFAST Transactions on Software Engineering*, vol. 11, no. 2, pp. 1–10, 2023.

[101] M. Rehman, M. Fuzail, M. K. Abid, and N. Aslam, "Financial Prices Prediction of Stock Market using Supervised Machine Learning Models," *VFAST Transactions on Software Engineering*, vol. 11, no. 2, pp. 1–10, 2023.

[102] M. Rehman, M. Fuzail, M. K. Abid, and N. Aslam, "Financial Prices Prediction of Stock Market using Supervised Machine Learning Models," *VFAST Transactions on Software Engineering*, vol. 11, no. 2, pp. 1–10, 2023.

[103] A. I. Akkalkot, N. Kulshrestha, G. Sharma, K. S. Sidhu, S. S. Palimkar, and others, "Challenges and Opportunities in Deploying Explainable AI for Financial

Risk Assessment," in *2025 International Conference on Pervasive Computational Technologies (ICPCT)*, 2025, pp. 382–386.

[104] K. H. Vesper and W. B. Gartner, "Measuring progress in entrepreneurship education," 1997. doi: 10.1016/S0883-9026(97)00009-8.

[105] M. R. Ali, "Imparting effective software engineering education," *ACM SIGSOFT Software Engineering Notes*, vol. 31, no. 4, p. 1, 2006, doi: 10.1145/1142958.1142960.

[106] N. Selwyn, *Education and Technology: Key Issues and Debates*. London: Bloomsbury Academic, 2011.

[107] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J*, vol. 1, no. 1, pp. 22–32, 2014, doi: 10.1109/JIOT.2014.2306328.

[108] Md. A. Rahman, M. Alam, and M. Alam, "IoT-Based Smart Waste Management Systems for Revolutionary Urbanization in Smart Cities," *Smart Cities*, vol. 3, no. 3, pp. 100–110, 2020, doi: 10.3390/smartcities3030007.

[109] J. Ali, M. H. Zafar, C. Hewage, S. R. Hassan, and R. Asif, "The Advents of Ubiquitous Computing in the Development of Smart Cities—A Review on the Internet of Things (IoT)," Feb. 01, 2023, *MDPI*. doi: 10.3390/electronics12041032.

[110] R. Jain, K. J. Parmar, D. Palaniappan, and T. Premavathi, "Blockchain-Enabled 6G Security Architecture for Smart Cities: A Decentralized and Resilient Approach," in *Building Tomorrow's Smart Cities With 6G Infrastructure Technology*, IGI Global Scientific Publishing, 2025, pp. 265–300.

[111] P. Bellini, P. Nesi, and G. Pantaleo, "IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies," Feb. 01, 2022, *MDPI*. doi: 10.3390/app12031607.

[112] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," Aug. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/s23167194.

[113] I. Abunadi, A. Rehman, K. Haseeb, L. Parra, and J. Lloret, "Traffic-Aware Secured Cooperative Framework for IoT-Based Smart Monitoring in Precision Agriculture," *Sensors*, vol. 22, no. 17, Sep. 2022, doi: 10.3390/s22176676.

[114] P. Majumdar, S. Mitra, D. Bhattacharya, and B. Bhushan, "Enhancing sustainable 5G powered agriculture 4.0: Summary of low power connectivity, internet of UAV things, AI solutions and research trends," *Multimed Tools Appl*, pp. 1–45, 2024.

[115] H. Nguyen and Q. Tran, "CNN-Based Allergen Detection from Food Packaging Images," *Comput Electron Agric*, vol. 193, p. 106634, 2022.

[116] H. Nguyen and Q. Tran, "CNN-Based Allergen Detection from Food Packaging Images," *Comput Electron Agric*, vol. 193, p. 106634, 2022.

[117] N. Hill and L. Chang, "IoT and Retail: Enhancing Human-Object Interactions in Automated Stores," in *Proceedings of the 2024 International IoT in Retail Conference*, 2024, pp. 350–365.

[118] L. Chen and S. Ahmed, "Computer Vision for Retail: Enhancing Human-Object Interaction Detection," *Int J Comput Vis*, vol. 135, no. 3, pp. 233–245, 2023.

[119] C. Wilson and A. Khan, "Human-Centered AI in Retail: A Review of Interaction Detection Technologies," *Journal of AI Research in Retail*, vol. 8, no. 2, pp. 80–95, 2023.

[120] S. Williams and M. Choi, "Machine Learning Applications in Retail Automation," *Machine Learning for Retail*, vol. 12, no. 3, pp. 120–135, 2024.

[121] J. Smith and R. Kumar, "Smart Retail Automation: Trends and Technologies," *Journal of Retail Technology*, vol. 15, no. 1, pp. 1–15, 2023.

[122] T. Nguyen and P. Silva, "Autonomous Checkout Systems: The Future of Retail," *Retail Automation Journal*, vol. 18, no. 2, pp. 75–90, 2024.

[123] S. S. U. Din, M. A. Aslam, S. Farid, T. F. Khan, and M. K. Abid, "ENHANCING AI SYSTEM TRANSPARENCY AND EXPLAINABILITY: INTEGRATING FORMAL METHODOLOGIES FOR IMPROVED MODEL PERFORMANCE AND INTERPRETABILITY," *Spectrum of Engineering Sciences*, vol. 3, no. 5, pp. 395–410, 2025.

[124] R. Feroz, M. A. Aslam, M. Fuzail, N. Aslam, and M. K. Abid, "HYBRID DEEP LEARNING EFFECTIVENESS OF IMAGE-BASED MALWARE DETECTION," *Kashf Journal of Multidisciplinary Research*, vol. 2, no. 05, pp. 1–13, 2025.