International Journal of Marketing and Technology
Vol. 14 Issue 02, February 2024
ISSN: 2249-1058 Impact Factor: 6.559
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Advancing Edge Security: AI and ML Innovations for Robust Cyber Defense

Jatin Pal Singh

Abstract

All kinds of devices are connected to the internet these days. From phones and cars to refrigerators and lights, more and more devices have computers in them. While this connects our world in useful ways, it also opens doors for security problems. Hackers can access these devices and use them to cause trouble. We need ways to keep devices safe from these hackers. Researchers have started using artificial intelligence (AI) to help protect devices. AI systems can learn on their own from huge amounts of data. They get better at their jobs over time without being explicitly programmed. My research looks at how AI can help secure devices right where the user interacts with them, called 'the edge'. Edge security is important because attacks often happen at this point.

Introduction

Edge computing is one way that artificial intelligence (AI) is improving cybersecurity. Rather than sending all network data to a central location to be analyzed, edge computing processes data at the edges of a network, like individual devices, routers, and firewalls. Edge computing has become an important area of research as more "things" get connected to the internet. However, bringing computing power directly to devices also presents new security challenges that need solutions. The study looks at how AI can be used for security at the edges of networks and could impact security and privacy. It looks specifically at how helpful and difficult it would be to put AI security directly on devices at the edge of networks. Therefore, the study can help networks protect against data stop threats and preserve the private information of various consumers.

Literature Review

Several studies have looked at the growth of edge computing and the factors driving it. According to [1], the number of networked devices worldwide is predicted to triple to over 100 billion by 2025. Industries are deploying more sensors, machines, vehicles, and other "smart" systems with integrated processing ability. [2] found edge networks are expanding rapidly in areas such as manufacturing, healthcare, transportation, and infrastructure management due to the advantages of low latency, mobility support, and bandwidth savings over cloud-only solutions. As edge deployment expands, security concerns are rising. [3] point out that diverse edge devices have limited security resources compared to data centers. Traditional defenses like firewalls and anti-malware also do not readily apply at the network edge. [4] Note that attackers targeting edge systems pose growing threats, including intellectual property theft, safety hazards, and service disruptions. New "edge-native" security measures are needed.

AI is one approach that is gaining interest in strengthening edge defenses. [5] review how machine learning algorithms can learn normal behavior patterns to detect anomalies and threats automatically. [6] tested AI models for contextual behavior analysis to flag network intrusions. [7] demonstrated AI's capability for lightweight on-device malware detection. While research shows promise, integration of AI into full-edge security solutions remains limited. Most studies also focus on technical proofs rather than real-world deployments. [7] points out gaps in testing AI-based security under operational edge conditions over long periods. Some open questions include ensuring AI security approaches are robust, low-cost, and privacy-focused enough for mass edge adoption.

In summary, more devices using AI at the local level create new possibilities but also big risks if we fail to improve security together. Researchers still need to solve problems with speed, dependability, and privacy protection to help make AI security practical for widespread use. This is still an important area for ongoing cooperation between experts in technology, engineering, and law/policy. Working as a team, they can advance solutions to secure edge AI as its use expands.

AI & Edge security:

Overview:

Artificial intelligence (AI) is changing the way companies protect themselves from cyber-attacks. By using machine learning and deep learning, AI can identify and stop security threats better than humans. There are three main types of AI used in cybersecurity: **supervised learning**, **unsupervised learning**, and **reinforcement learning** [8]. Supervised learning uses example data that is already labeled to find patterns. For example, intrusion detection systems use examples of past hacking attempts that have been labeled as "intrusion" to learn how to spot new hacking attempts. Unsupervised learning does not need labeled example data. It looks for patterns in data on its own. Anomaly detection systems use unsupervised learning to find unusual activity on a network, like a denial of service (DDoS) attack, without being directly shown examples of attacks. Reinforcement learning trains an "agent" to make decisions by giving it rewards or punishments for its choices. Reinforcement learning can help companies respond to security incidents in real time by recommending the best actions during an attack.

Application of AI in Edge Security

Edge computing is one way that AI is improving cybersecurity. Rather than sending all network data to a central location to be analyzed, edge computing processes data at the edges of a network, like individual devices, routers, and firewalls. This has several security benefits, including:

a) **Threat detection and prevention**: AI models are placed at network edges to scan local data sources for threats in real-time [9]. For example, an AI agent on an employee's laptop analyzes webcam footage, documents, and browser history to detect malware, spyware, or data exfiltration. Network edge servers running AI can scan traffic for known threat patterns like malware communication protocols. When threats are found, prevention kicks in automatically by blocking harmful files/traffic from spreading further into the network.

b) **Anomaly Detection**: AI models at the edge are trained to recognize 'normal' behavior for users, devices, and network traffic, enabling them to detect deviations indicative of security threats. For example, an AI monitoring an IoT device might flag unusual activity outside typical operating hours. This rapid anomaly detection narrows the opportunity for attackers to exploit the network. Over time, AI learns the typical communication patterns of local users, applications, and devices, vigilantly identifying significant deviations. Such capabilities allow AI to quickly alert to potential compromises or unauthorized actions, like an employee suddenly accessing unusually large data volumes. By analyzing behaviors in real-time locally, AI enhances early threat detection and response at the edge.

c) **Enhanced Data Privacy:** AI-driven edge security significantly enhances data privacy by identifying and protecting sensitive information directly on local devices, reducing data breach risks. It employs algorithms to recognize and safeguard personal data, applying encryption and minimizing data retention in compliance with privacy regulations. Techniques like federated learning allow AI to continually improve its privacy measures without compromising data integrity. This localized, intelligent approach ensures robust protection against unauthorized access and adapts to evolving privacy needs, thereby strengthening trust and fortifying the security framework in edge computing environments.

d) **Adaptive Security Policies:** Adaptive security policies, powered by AI in edge environments, dynamically adjust protections based on real-time data analysis and risk assessment. This approach enables systems to tailor their defenses to current network conditions, user behaviors, and threat landscapes. As situations evolve, AI algorithms assess the level of risk and modify security parameters accordingly, ensuring optimal protection at all times. This might involve altering authentication requirements, adjusting access controls, or isolating potentially compromised nodes. By continuously learning and adapting, these intelligent policies ensure that security measures are both effective and efficient, providing robust, context-aware defenses against a variety of threats.

e) **Fraud Detection:** Fraud detection in edge computing, enhanced by AI, involves analyzing transactional and behavioral data in real-time to identify patterns or anomalies indicative of fraudulent activity. AI models, such as neural networks or anomaly detection algorithms, are trained on vast datasets to recognize legitimate and fraudulent behaviors. These systems can quickly and accurately flag unusual transactions, unauthorized access, or suspicious patterns, prompting immediate investigation or preventive measures. By implementing AI-driven fraud detection at the edge, organizations can rapidly respond to potential threats, minimize financial losses, and protect user integrity, all while maintaining high transactional throughput and user experience.

AI systems are also essential in providing real-time incident response. According to [10], real-time incident response refers to the ability to analyze, understand, and resolve security issues as they occur, reducing breach damage. AI now plays a key role in real-time response. For instance, in incident identification, many AI programs placed in different parts of the network constantly share the information they collect and any alerts to quickly find possible security issues happening across the whole system in real time. For example, if edge devices notice a big increase in failed login attempts, it could mean a widespread "credential stuffing" attack is happening, and a fast response is needed. Furthermore, AI is important to achieve automated response. AI response systems trained beforehand can take initial actions like separating affected areas from the rest or blocking known bad things without a person overseeing it. For instance, an AI system may recognize an "SQL injection attack" and automatically isolate vulnerable web servers within minutes to contain the intrusion in a small area. This "auto-pilot" means issues can start being addressed almost right away instead of waiting for analysts.

Edge Computing Infrastructure

Characteristics of Edge Computing

Edge computing puts processing power closer to where data is created and used. Instead of always sending information to a distant centralized server, edge computing allows for data to be analyzed locally. This brings important benefits over traditional network architectures that rely on transporting all data to the cloud. One advantage is speed. When data is processed near its source, there is less distance for it to travel over networks and wires. This reduces lag times, giving results and responses much faster [11]. Real-time interactions feel snappier when computation occurs close to the user or device generating information. Less bandwidth is also used with edge computing. Transporting data long distances over the internet takes up network capacity. By handling data locally, edge computing minimizes how much needs to be sent elsewhere. This saves on bandwidth usage costs. Reliability is another plus. Since edge nodes take care of local processing autonomously, the system is less dependent on maintaining an uninterrupted connection to remote resources. Even if a wider network connection is disrupted, edge devices can continue operating independently for periods. Edge computing distributes workloads across many decentralized nodes as well. This spread-out approach balances loads and prevents any single point from becoming a bottleneck or performance limitation. It also ensures redundancy in case any one node requires maintenance or replacement.

Security Implications in Edge Infrastructure

Making all the different machines for edge computing secure can be challenging. With edge computing, information is handled by lots of different devices instead of just a few main servers. Each extra device gives hackers more chances to try and access information without permission. Edge machines are usually more spread out in different places than servers in a protected data center. Anyone near the devices might try to get into them without permission. If a hacker succeeds at taking control of an edge machine, they could then use it to attack the bigger networks [12]. In order to keep the edge machines protected, strong policies need to be set up on all the scattered devices. Rules limit who can log into devices and see information. Encryption is also important because it scrambles data as it moves between devices, making it unclear if a hacker intercepts a transmission.

Additionally, network managers need to check devices regularly. They need to make sure each machine has the latest updates to its programs and firmware [13]. Updates fix security problems that hackers could try to exploit if not patched. Always watching the devices is key to noticing strange activity quickly. Preventing problems early on better protects the whole system from disruption.

Integration of AI with Edge Devices

AI can give small devices like smart home appliances new abilities. AI trains computers to act smart, like how people think and learn. One use of AI is to have it look at information from sensors in real life. Devices can then make choices on their own and react right away based on what the AI understands from analyzing the current data According to [1]. AI could also help small devices protect themselves better. AI may be able to notice suspicious traffic on the network faster than regular security methods. By quickly finding possible problems, AI helps small devices respond sooner to issues.

However, adding AI is not without challenges. Small devices usually have less powerful processors and smaller storage than big servers. They may struggle to run complex AI models like cloud servers safely [14]. With fewer abilities, there are probably weaker protections for AI on small devices. Hackers could take advantage of weaknesses. Small systems with AI need to carefully think about security. Developers must understand the limits of small devices. Good security rules just for AI on small devices should be set up. Simply copying AI solutions from cloud servers may not protect small devices running AI tasks well enough. Careful planning is needed to use AI's benefits while also shielding small devices from risks.

Real World Implementation

Video Monitoring Systems: Smart video monitoring systems that use AI have been widely installed in public places like airports and companies. This helps improve security. These systems can notice unusual things happening in real time. And they can also recognize faces and set off alarms. As an example, the city of Chicago has implemented a smart monitoring system known as Operation Virtual Shield [15]. It uses artificial intelligence that watches over 25,000 cameras around the city. This system has assisted in lowering crime and making people safer.

Cybersecurity: Cyber threats can be detected early on with AI-based cybersecurity solutions. For instance, the company Darktrace uses AI algorithms to monitor network traffic and detect anything suspicious at once [16]. This makes it possible to anticipate and prevent cyber-attacks before any damage is caused.

Automation in Factories: In the automated industry, AI-powered security systems have been capped on important equipment to watch and protect. For example, GE Digital's Predix platform makes use of AI to monitor and secure industrial control systems [17]. It helps factories to run safely and smoothly.

Challenges and Lessons Learned

Threat to Private Information: Cases in point are AI-based security systems, which require a massive amount of data. However, this raises questions about the disclosure of private information. Privacy laws must be carefully observed in collecting, storing, and processing data.

False Alarms: False warnings are given by AI security systems, which result in wrong alarms and wasted resources. Hence, the AI algorithms must be refined to reduce the number of false alarms and improve accuracy in detection.

Internet Connection Dependency: AI security systems require an internet connection to operate properly. If the system is knocked offline, then it can be attacked. If the connection fails at any time, then backup plans are necessary.

Training and Maintenance: For this reason, AI security systems also need regular training and updates to be knowledgeable about the most current threats out there. Updates need to be done, and you have a team that goes out there every day to take care of the system.

Future Trends and Innovations

Evolving Landscape of Edge Security

Making Edge Devices Secure: As more internet-connected devices operate autonomously at the edge of networks, ensuring their security and the security of any data they collect or generate is critically important. Techniques like implementing strong authentication requirements during device startup, incorporating tamper-resistant hardware security mechanisms, and using robust end-to-end encryption can help bolster protections against both digital threats from hackers and physical dangers [18]. Edge networks also need verification of identity and permission-based access controls to confirm that only sanctioned devices and authorized users can join and exchange information on the network.

Using AI and Machine Learning at the Edge: With decentralization enabling data to be generated and processed locally all along the edges of networks by countless devices, AI and machine learning tools deployed directly on these endpoints will be needed to help analyze rapidly growing volumes of information in real time. Adding edge-based machine learning can help identify anomalies in network operations. Examples include cyberattacks, equipment health, and potential failures that require maintenance and optimization of building energy use based on changes to the operating environment.

Developing Standards and Best Practices: With edge computing infrastructure and the number of distributed data exchanges they facilitate taking off at a rapid clip, joint efforts are needed to create standardized technologies and common policies, as well as recommended security practices. Technological recommendations include uniform data transmission protocols and governance standards that cover device management or systems security. Privacy rules, terms of consent frameworks, and consensus on a secure boot sequence apply across all use cases.

Anticipated Developments in AI-Enabled Edge Security

Adopting 5G and Fast Wireless: High-speed 5G cellular networks of the next generation will be combined with other wireless technologies that enable high throughput and low latency connections, helping bring edge computing to life [1]. With such fast, solid connectivity at the corner of networks (i.e., near-to-end users), these new real-time interactive applications using huge volumes of bandwidth--advanced video monitoring; connected autonomous vehicles dependent on remote sensory data; telemedicine procedures relying on immediate patient biometrics and so forth will all be possible.

Increasing Cyber Threat Monitoring: As an enormous ecosystem of endpoints materializes at the network edge driven by countless disparate internet-linked devices and systems, the exposed attack surface for cyber threats multiplies enormously as well. Continuous threat intelligence gathering aided by machine learning scanning for anomalies against the massive flow of edge traffic will be crucial to identifying malicious patterns. Timely sharing of threats and vulnerabilities between industry peers and government entities can help strengthen common defenses.

Implications for Industry and Society

Edge computing has various benefits and limitations to the current economy. These range from economic and business implications to social and privacy concerns. Economic and business impacts of AI security at the edge- AI helps make edge security systems better by quickly looking at data where it is made. This can help find and fix problems faster and save money [19]. Take the example of AI security cameras that sense something out of place and report to authorities, leaving people forever watching over them. This can reduce labor costs and help run businesses more smoothly. Moreover, information and feedback that help businesses make good decisions can come from AI security systems.

This type of AI edge security does have its advantages, but it also brings up pressing social and privacy questions. The data gathered might be used for espionage on people or in other ways that are not respectful of privacy. Another theoretical danger is that the algorithms AI security systems use to pursue data will be biased. Companies must be transparent as to how they utilize AI security systems, and what is most important is that companies follow privacy laws. Companies should also reflect on how these systems may impact society and take preventive measures to reduce negative impacts. An example could be setting up fair use standards for AI and discussing with community groups, non-profit organizations, etc., to make sure the benefits of securing artificial intelligence reach all interested parties.

Methodology

The study looked at how Artificial Intelligence (AI) used for security at the edges of networks could impact security and privacy. It looked specifically at how helpful and difficult it would be to put AI security directly on devices at the edge of networks. Some examples of edge devices are phones, tablets, and smart home appliances. The study wanted to understand how well and easily AI security could work with current network security systems. The study employed different approaches to study this issue carefully. The goal was to learn more about the pros and cons of using AI directly on edge devices for security purposes. Therefore, the study could help networks protect data, stop threats and preserve the private information of various consumers.

Research Methodologies

The study considered how AI for network edge protection could affect security and privacy. It focused particularly on whether making AI security work directly at the edge of networks would be helpful or difficult. Examples of edge devices include phones, tablets, and smart home appliances. In particular, the study wanted to know whether and how well AI security could cooperate with today's network security systems. A case study research approach was utilized to study this problem. Case studies allowed for an in-depth **qualitative exploration of real-world examples** of AIES deployment. This provided insights that could not be gained through theoretical research alone. Several case studies were selected based on their relevance to the research question and their potential to reveal new perspectives on AIES feasibility and integration. Information was gathered from these cases through document analysis to gain a rich understanding of each situation.

Data Collection and Analysis

Data collection involved finding both primary and secondary sources. For secondary data, reports, academic papers, and whitepapers were located from reputable sources. This provided background knowledge and established context. For primary data, suitable case studies for deeper exploration were identified. The data analysis involved a thematic analysis approach. Common themes and ideas that emerged through close reading of the data were identified. How themes related and patterns appeared was examined to develop a conceptual understanding. This analysis offered a comprehensive view of AIES feasibility, advantages, and challenges at the edge from different perspectives.

Validity and Reliability

Several steps were taken to ensure the research findings would be valid and reliable. Using multiple case studies from different contexts and locations helped create a well-rounded picture instead of only examining a single situation. The diversified data sources reduced bias and limitations. The thematic analysis methodology facilitated the organization and interpretation of the data in a structured manner. Rigorous identification and use of case studies, alongside extensive analysis, strengthened the accuracy and trustworthiness of conclusions.

Limitations

While the case study research and mixed methods approach provided valuable insights, there were also some limitations to the current study. First, only three case studies were examined in depth due to resource constraints. More case studies may have revealed additional themes or perspectives regarding AIES implementation challenges. Additionally, the case studies were selected based on the availability of information and connections to contacts rather than statistically representative sampling. This could introduce some selection bias in the types of organizations and AIES projects included. Future research could aim for a randomized sample. Lastly, the scope was limited to edge deployments of AIES within network security applications. Other domains and implementation models were not included, limiting generalizability. Broader application domains and technical architectures represent opportunities for future research. While these limitations constrain what can be conclusively determined, the study still provides valuable initial insights into AIES adoption challenges to further understanding in this emerging field. Future research can build upon this work to address its limitations.

Conclusion

While research on AI-enabled security at the edge is still emerging, results so far are promising. Edge computing brings both opportunities and challenges for improving security through localized machine learning approaches. Studies have demonstrated AI's potential for fast, autonomous threat detection, anomaly identification, and behavioral analysis directly on devices. However, more work is still needed to fully realize this potential through deployments under real-world conditions that address reliability, privacy, and integration concerns. Standardized frameworks and comprehensive testing under operational constraints could advance the practical application of AI security solutions at scale. Addressing challenges around performance, data handling, and human oversight will also be important to gain user trust. Continued collaboration between computing experts, engineers, and policymakers can guide in these areas. As edge and IoT adoption expands rapidly, the need for robust localized security will become increasingly important. Further research integrating machine learning techniques into complete practical edge protection architectures could help unlock AI's advantages for making distributed infrastructures safer and more resilient in the future. Through the balanced consideration of technical and social factors AI has it in its power to make security at the edge even stronger.

Results

Case Study 1: IoT Platforms and Security

This case study explores IoT platforms, considering design principles and functions as well as security issues. The analysis covers a number of IoT platforms, examining their characteristics and shortcomings in terms of security. Here are key points from the case study:

IoT Platform Features: This case study examines the basic functions of IoT platforms. Interconnection solutions for advanced assets, cloud-based solution strategies to increase scalability, and interest in open-source software approaches that reduce costs and foster interoperability are among those emerging technologies addressed within this space.

Security Layer Analysis: Security functions on IoT platforms usually boil down to existing cryptographic protocols (HTTPS, TLS) and vendor-specific policies. The case study stresses the need to integrate security by design into every tier, component, and application of IoT platforms so as to reduce cyberattacks.

Considerations and Limitations: The IoT platforms provide many functions, but there are limitations. Additional security methods need to be considered. Their support for the hybrid cloud or edge computing architecture is limited; modeling tools and digital twins get short shrift in them.

Future Outlook: This case study indicates that more advanced security methods must be developed, and decentralized paradigms like edge computing need to be supported. It also points out that some IoT platforms are lacking in trustworthiness or even have a lack of information about their security mechanisms.

Learning Outcomes: Students will learn about the various characteristics of IoT platforms and understand how security is a key factor in their design. The case study serves to provoke analysis of shortcomings and considerations in IoT platform security while at the same time enticing students into speculating about future developments.

Case Study 2: Enabling Sustainable Development Through AI-Based Surveillance System on Cloud Platform

This case is about creating a surveillance system that is powered by AI. The aim is to strengthen security as well as streamline the work schedules. The way that the system works is by AI with cloud infrastructure [15]. It then gains the capability to distinguish between visitors, individuals, and intruders. The crucial aspects include:

Objectives and Challenges: From the case, challenges associated with large equipment in video management systems (VMS) are exemplified. This case study emphasizes that it is important to have separate server rooms to overcome these challenges. The reasoning is that a compact, flexible, and reliable security monitoring system that incorporates cloud computing and AI should be formed.

System Architecture and Components: The case study proposes a system that is able to detect weak points as well as intruders through its AI capabilities [15]. The system is built on cloud platforms. IoT device synchronization ensures efficient collaboration [15].

Testing and Results: Snapshots of the testing process are used to display the system's results. Based on reference photos used for training, the AI model is able to identify allowed individuals with success; it displays "No Match" when an authorized person is not present and "Match" when they are. When unknown or unauthorized individuals access the property, the system takes pictures and stores them in a Google Cloud Bucket.

Key Features: The project demonstrates how to integrate the Arduino Uno with the ESP32 Camera Module configuration, offering a dependable and small design. To strike a compromise between the algorithm's accuracy and speed of execution, OpenCV is widely utilized in software. Google Cloud Services is used to implement the cloud, proving that the surveillance system can be operated on a cloud platform.

Achievements: The successful development of an AI-powered surveillance system that can identify people inside a camera's range of vision is the report's capping achievement. The project is made more effective by the combination of software (OpenCV) and hardware (ESP32 Camera Module and Arduino Uno). The utilization of Google Cloud Services demonstrates the potential for cloud-based surveillance system implementations.

Learning Outcomes: By addressing issues with conventional systems, students may learn how artificial intelligence (AI) is being used practically in surveillance systems. The case study provides a real-world example of how IoT devices, artificial intelligence, and cloud platforms may be integrated for improved efficiency and security. ESP32 Camera Module, OpenCV, and Arduino are used to create a concrete example of hardware-software cooperation in practical applications.

Case Study 3: IBM and AI-Enhanced Security Operations

IBM, a leader in IT and cybersecurity, has integrated AI into its security operations to create a more robust, responsive, and intelligent security system. Recognizing the need for advanced defenses against increasingly sophisticated cyber threats, IBM has leveraged its Watson AI to enhance its security capabilities. IBM Watson for Cyber Security is a cognitive AI system that understands, reasons, and learns from security information. Watson is integrated with IBM's security products to analyze vast volumes of security data from structured and unstructured sources. By using natural language processing, Watson can understand the context and semantics of text in documents, websites, and news reports, helping security analysts make informed decisions faster.

Outcomes:

- **Enhanced Threat Intelligence:** Watson's AI analyzes thousands of documents per minute, providing real-time insights and threat intelligence to security analysts.
- **Reduced Response Times:** By automating the analysis of security incidents and providing actionable insights, Watson helps reduce incident response times significantly.
- **Improved Decision Making:** Watson provides security analysts with evidence-based recommendations, improving the accuracy and speed of decision-making.

Significance: The IBM case study demonstrates how AI can transform security operations, making them more proactive, efficient, and intelligent. It showcases the potential of AI to enhance threat detection, analysis, and response, contributing to more secure and resilient digital environments. This example aligns well with the research's exploration of AI in edge security, illustrating the broader implications and practical applications of artificial intelligence in cybersecurity.

References

[1] M. Vishwanath, "Convergence of 5G Technologies, Artificial Intelligence and Cybersecurity of Networked Societies for the Cities of Tomorrow & A Bio-inspired Hybrid Artificial Intelligence Framework for Cyber Security.," OSF, 2023. https://osf.io/preprints/wzyv3/ (accessed Dec. 17, 2023).

[2] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, and Q. Zhang, "Edge Computing in IoT-Based Manufacturing," IEEE Communications Magazine, vol. 56, no. 9, pp. 103–109, Sep. 2018, doi: https://doi.org/10.1109/mcom.2018.1701231.

[3] T. Nguyen, R. Novak, L. Xiao, and J. Lee, "Dataset Distillation with Infinitely Wide Convolutional Networks," Neural Information Processing Systems, vol. 34, pp. 5186–5198, 2021, Accessed: Dec. 17, 2023. [Online]. Available: https://proceedings.neurips.cc/paper/2021/hash/299a23a2291e2126b91d54f3601ec162-Abstract.html

[4] M. S. Ansari, S. H. Alsamhi, Y. Qiao, Y. Ye, and B. Lee, "Security of Distributed Intelligence in Edge Computing: Threats and Countermeasures," The Cloud-to-Thing Continuum, pp. 95–122, 2020, doi: https://doi.org/10.1007/978-3-030-41110-7_6.

[5] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of Artificial Intelligence and Machine Learning in Smart Cities," Computer Communications, vol. 154, pp. 313–323, Mar. 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.069.

[6] B. Mahbooba, R. Sahal, W. Alosaimi, and M. Serrano, "Trust in Intrusion Detection Systems: An Investigation of Performance Analysis for Machine Learning and Deep Learning Models," Complexity, vol. 2021, pp. 1–23, Mar. 2021, doi: https://doi.org/10.1155/2021/5538896.

[7] N. Moustafa, “A New Distributed Architecture for Evaluating AI-based Security Systems at the Edge: Network TON_IoT DatasetsNourMoustafaa1⍰TON_IoT datasets: A distributed architecture for evaluating Artificial Intelligence-based security systems in IoT networks,” Sustainable Cities and Society, vol. 72, p. 102994, May 2021, doi: https://doi.org/10.1016/j.scs.2021.102994.

[8] R. Geetha and T. Thilagam, “A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security,” Archives of Computational Methods in Engineering, vol. 28, Sep. 2020, doi: https://doi.org/10.1007/s11831-020-09478-2.

[9] F. Khan, Mian Ahmad Jan, Ateeq Ur Rehman, Spyridon Mastorakis, Mamoun Alazab, and P. A. Watters, “A Secured and Intelligent Communication Scheme for IIoT-enabled Pervasive Edge Computing,” IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5128–5137, Jul. 2021, doi: https://doi.org/10.1109/tii.2020.3037872.

[10] J.-H. Huh and Y.-S. Seo, “Understanding Edge Computing: Engineering Evolution With Artificial Intelligence,” IEEE Access, vol. 7, pp. 164229–164245, 2019, doi: https://doi.org/10.1109/access.2019.2945338.

[11] K. Cao, Y. Liu, G. Meng, and Q. Sun, “An Overview on Edge Computing Research,” IEEE Access, vol. 8, pp. 85714–85728, May 2020, Accessed: Dec. 17, 2023. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/8948470/09083958.pdf

[12] P. Tedeschi and S. Sciancalepore, “Edge and Fog Computing in Critical Infrastructures: Analysis, Security Threats, and Research Challenges,” 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 1–10, Sep. 2019, Accessed: Dec. 17, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Edge-and-Fog-Computing-in-Critical-Infrastructures%3A-Tedeschi-Sciancalepore/77b5a928e6aec2a984456b068100c15c1037333c

[13] N. Hassan, K. Yau, and C. Wu, “Edge computing in 5G: A review.,” IEEE Access, vol. 7, pp. 127276–127289, 2019, Accessed: Dec. 17, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Edge-Computing-in-5G%3A-A-Review-Hassan-Yau/350352a67270bf968350db7789634d9d7bdcf36a

[14] R. Feng, S. Chen, X. Xie, G. Meng, S.-W. Lin, and Y. Liu, “A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1563–1578, 2021, doi: https://doi.org/10.1109/tifs.2020.3025436.

[15] A. Kharbanda, V. Rana, N. Baghela, and M. Fatima, “Enabling Sustainable Development Through Artificial Intelligence-Based Surveillance System on Cloud Platform.,” International Conference on Sustainable Development through Machine Learning, AI and IoT, Nov. 2023, Accessed: Dec. 17, 2023. [Online]. Available: https://www.researchgate.net/publication/375751688_Enabling_Sustainable_Development_Through_Artificial_Intelligence-Based_Surveillance_System_on_Cloud_Platform

[16] M. Qumer and S. Ikrama, “Poppy Gustafsson: redefining cybersecurity through AI.,” The Case for Women, 2022.

[17] G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, and G. Spezzano, “IoT Platforms and Security: An Analysis of the Leading Industrial/Commercial Solutions,” Sensors, vol. 22, no. 6, p. 2196, Mar. 2022, doi: https://doi.org/10.3390/s22062196.

[18] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, “Secure data storage based on blockchain and coding in edge computing,” Mathematical Biosciences and Engineering, vol. 16, no. 4, pp. 1874–1892, 2019, doi: https://doi.org/10.3934/mbe.2019091.

[19] F. Al-Doghman, N. Moustafa, I. Khalil, Z. Tari, and A. Zomaya, “AI-enabled Secure Microservices in Edge Computing: Opportunities and Challenges,” OPUS at UTS, Jan. 2022, Accessed: Dec. 17, 2023. [Online]. Available: https://opus.lib.uts.edu.au/handle/10453/167672