ARTIFICIAL INTELLIGENCE-BASED SECURITY AND DATA PROTECTION FOR IOT

Sheetal A. Kathoke
Research Scholar, Department of Electronics and Computer Science, PGTD, RTM, Nagpur University, Nagpur, M.S, India
sheetalkathoke16@gmail.com

Dr. Kishor M. Dhole
Assistant Professor, Department of Computer Science, Seth. Kesarimal Porwal College of Arts and Science and Commerce, Kamptee.Nagpur, M.S, India
km.phd108@gmail.com

Abstract

The Internet of Things (IOT) has revolutionized modern industries by making it possible for smart devices to be connected, process data, and exchange it. However, this rapid expansion has also brought about significant privacy and security issues. Traditional security mechanisms often fail to address the scalability and complexity of IOT networks. Artificial Intelligence (AI), particularly machine learning (ML) and deep learning (DL), provides adaptive and intelligent solutions to enhance IOT security. In order to guarantee data security and system resilience, this paper investigates how AI techniques can detect, prevent, and respond to cyber threats in IOT systems. The study discusses anomaly detection, encryption optimization, and privacy-preserving methods. In conclusion, it discusses the difficulties associated with implementing AI-driven IOT security frameworks as well as possible future paths.

1. Introduction

For applications like healthcare, smart cities, agriculture, and industry automation, the Internet of Things (IOT) connects billions of devices worldwide, enabling them to collect and exchange information. However, the increased number of connected devices increases the attack surface. IOT device flaws can be exploited by attackers to steal sensitive data or disrupt operations. Due to the diversity of communication protocols, heterogeneous environments, and limited computational power, traditional security solutions like firewalls and rule-based intrusion detection are insufficient for the Internet of Things. A dynamic and data-driven approach to identifying new threats, automating responses, and ensuring continuous protection is provided by artificial intelligence (AI). IOT data can be analysed by AI algorithms to spot unusual patterns and anticipate security breaches before they occur.

Traditional security mechanisms like intricate encryption algorithms and intrusion detection systems are less able to be implemented by IOT devices because of their limited storage and computational power. As a result, they become easy prey for cyberattacks like data breaches, malware infections, denial-of-service (DOS) attacks, and unauthorized data access. Additionally, there are serious concerns regarding the confidentiality, integrity, and privacy of the data generated and transmitted by IOT devices. Artificial Intelligence (AI) has emerged as a promising strategy for improving the security and data protection of IOT environments to address these issues. AI techniques—particularly Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL)—enable systems to learn from data, detect anomalies, and predict potential threats in real time. These intelligent models are able to change to new and changing patterns of attack, protecting you from both known and unknown threats all the time. For instance, AI-driven intrusion detection systems can analyse network traffic patterns to identify malicious activities, while deep learning models can help in behavioural analysis and anomaly detection across connected IOT nodes. Healthcare and agriculture of IOT based Target aware holistic influence [6]. Increasing using of IOT then IOT device flow can exploited by attack to steal sensitive AI protection block chain operation based IOT environment [4].

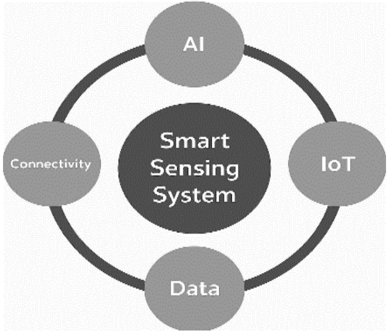

Figure 1 : Intelligent IoT Secured and Privacy Framework

2. Literature Review

Review of the Literature Recent studies have focused on integrating AI into IOT security to enhance data protection.

Machine Learning in Intrusion Detection: Researchers have applied ML algorithms such as Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbours to detect network intrusions and classify attacks in IOT environments.

Convolution Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks are examples of deep learning models used to detect anomalies in real time by analysing network traffic patterns. Federated Learning for Privacy: Federated learning permits IOT devices to collectively train AI models without sharing raw data, preserving privacy and avoiding centralized data collection. Block chain and AI Integration: Combining AI with block chain strengthens data integrity, ensuring that IOT communications remain tamper-proof and transparent.

While these approaches improve security, issues such as computational limitations, data imbalance, and energy consumption remain challenges for real-world deployment. To enhance the protection of IOT and security for that want data protection and privacy [3].Li,X., & Zhao, Q.(2023)

AI-Based Threat Intelligence:

Literature suggests that AI-based threat intelligence systems can collect, correlate, and analyse large-scale IoT data in real time, identifying attack signatures faster than traditional rule-based systems.

I. Deep Learning for IoT Security:

Advanced models such as CNNs, RNNs, and LSTMs have been employed to detect complex attack patterns, malware classification, and secure authentication processes. Deep reinforcement learning further enhances adaptability against evolving cyber threats.

II. Edge and Fog Computing Security:

Recent research integrates AI with edge and fog computing to reduce latency and enable local data analysis for real-time intrusion detection. These approaches decentralize processing, improving both efficiency and privacy protection.

III. Blockchain-AI Hybrid Systems:

Literature reviews indicate a growing trend in combining blockchain and AI to strengthen IoT data integrity, ensure immutability of logs, and enable decentralized trust mechanisms across IoT networks.

IV. Behavioural Analytics and Anomaly Detection:

AI-driven behavioural analytics monitor device behaviour continuously to detect irregularities. This method helps identify compromised nodes or malicious firmware updates within IoT ecosystems.

V. Security in Resource-Constrained Devices:

Research has examined lightweight AI models optimized for IoT devices with limited computational power. Techniques like Timmy and compressed neural networks enable efficient local security analytics.

VI. Federated and Transfer Learning:

Recent studies propose federated learning models that allow AI systems to train across distributed IoT devices without centralizing data, enhancing both privacy and accuracy. Transfer learning helps adapt existing security models to new IoT environments quickly.

VII. AI for Access Control and Authentication:

AI-enabled biometric and behaviour-based authentication systems are being integrated into IoT devices for enhanced identity verification and prevention of unauthorized access.

VIII. Risk Assessment and Prediction Models:

Researchers have developed predictive AI systems that assess potential vulnerabilities and calculate risk levels for IoT components, helping organizations prioritize mitigation strategies.

IX. Comparison of Traditional vs. AI-Based Methods:

Traditional rule-based systems are static and slow in response, while AI models are adaptive, context-aware, and capable of learning from new attacks, offering a major improvement in proactive defence. Advance model, recent research integrated AI with edge, AI driven behaviour analysis i.e based on database [15] Purity, N (2023) [19] Review paper[21] Li R., Zhang H.(2018).

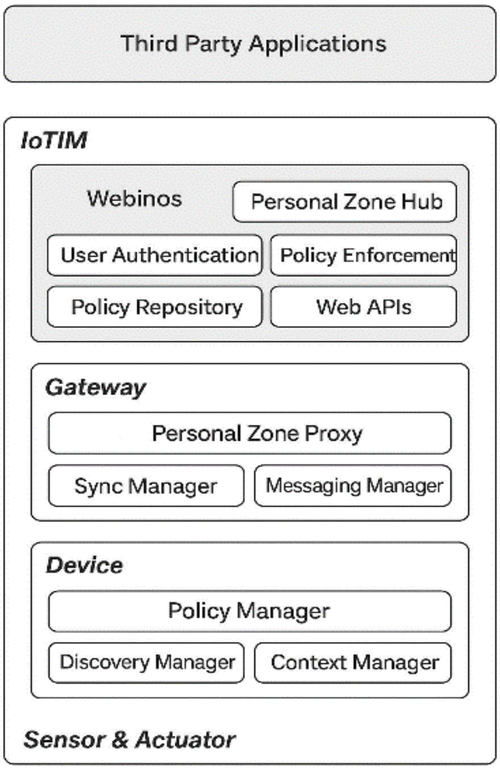

Figure 2:AI-Enabled IoT Security and Data Protection Framework

3. Methodology

I. Analytical methods are used to examine AI methods that improve IOT security and data protection. The approach includes:

II. Analysis of public IOT datasets containing both normal and malicious traffic is the method of data collection.

III. The IOT ecosystem is a highly heterogeneous environment with a mix of devices running various types of communication protocols and using different types of communication models. Schoening et al. [20] Waleed N.,He X., Ikram ., Usman M., Hashmi S.S, Usman M(2020) [25] Surya L(2019) defined four communication models: device to device, device to the cloud, device to the gateway, and back-end data sharing. In device-to-device communications, protocol design issues that address interoperability need to be investigated and innovative solutions developed.

From the device to cloud communications (e.g., interactions between a humidity sensor and an application service provider wherein sensor data may be uploaded to an application service provider), interoperability is much less of an issue. This is because the most of the communications occur within the provider [27]Security Protocol Using Artificial Intelligence to Prevent Internet of Things Attacks- Rajput M., Jaison F., Jain A., Mathur R(2023). In the device to gateway communication architecture, an Internet-connected gateway (which can be a generic one or a specific type that translates application-layer protocols) connects two IOT devices, such as one equipped with a temperature sensor and the other with a humidity sensor.

AI Model Selection: Comparing ML and DL algorithms like Decision Trees, SVM, CNN, and LSTM for threat detection IOT devices typically lack storage and computational power, making them less able to implement traditional security measures like intrusion detection systems or complex encryption algorithms. As a result, they become easy prey for cyberattacks like data breaches, malware infections, denial-of-service (DOS) attacks, and unauthorized data access. Additionally, there are serious concerns regarding the confidentiality, integrity, and privacy of the data generated and transmitted by IOT devices. Artificial Intelligence (AI) has emerged as a promising strategy for improving the security and data protection of IOT environments to address these issues. AI methods, specifically Machine Learning (ML), The design and analysis of AI-driven techniques that enhance the security, privacy, and data protection mechanisms in Internet of Things (IOT) environments is the primary focus of this research's methodology. It describes the methodical approach that was taken to create privacy-preserving mechanisms, secure communication frameworks, and intelligent models for IOT security. cyberattacks like data breaches and integrity, and privacy security of IOT needed [10]Mohmad Mahmoud and Almsman Khaled(2025), [12] Pureti, N(2023) There are a few important steps in the method.

I. dentification of IOT-related security risks The first step is to identify and classify any potential IOT network-specific security vulnerabilities and threats.

- Common attacks such as Denial of Service (DOS), man-in-the-middle, malware injection, spoofing, and data tampering are analysed.
- In order to comprehend the limitations of conventional security models, the unique characteristics of IOT devices such as their heterogeneity, decentralized architecture, and limited resources are evaluated.
- Risk levels are prioritized during threat modelling using frameworks like STRIDE or DREAD.

Prepossessing and Data Collecting Relevant data must be collected and processed in order for AI models to be trained effectively.

- For the purpose of intrusion detection, data is gathered from IOT network traffic, sensors, and open-source datasets like NSL-KDD and CICIDS.
- Data prepossessing includes data cleaning, normalization, and feature extraction to remove noise and ensure accurate model training.
- Principal Component Analysis (PCA) or Information Gain feature selection methods are utilized to select the most essential characteristics for threat detection.

II. Application of Artificial Intelligence Techniques

IOT security systems incorporate AI algorithms for intelligent threat detection and adaptive protection.

- In order to classify malicious behaviour and detect intrusions, machine learning (ML) algorithms like Random Forest, Support Vector Machine, and Decision Trees are used.
- Real-time anomaly detection and pattern recognition in massive IOT data streams are made possible by Deep Learning (DL) models like Convectional Neural Networks, Recurrent Neural Networks, and Auto encoders.
- Self-learning security systems that can dynamically adjust defines mechanisms in response to shifting threat landscapes are developed using reinforcement learning (RL).

III. Integration of Block chain and AI for Secure Data Management

To strengthen data integrity and trust, block chain technology is incorporated alongside AI models.

• Block chain ensures transparent transaction logs, secure authentication, and tamper-proof data storage.

• AI assists in smart contract validation, anomaly detection in block chain nodes, and optimization of consensus mechanisms.

•The combined framework enhances both data traceability and trustworthiness in distributed IOT systems.

IV. Mechanisms for Protecting Privacy AI-based data anonymization and encryption methods are implemented to protect user privacy.

•Federated Learning (FL) allows AI models to be trained locally on IOT devices without sharing raw data, reducing data exposure risks.

•Differential Privacy (DP) techniques are applied to prevent sensitive information leakage during model training or data exchange.

•Homophobic Encryption enables secure computation on encrypted data, ensuring confidentiality even during analysis.

V. Evaluation, Testing, and Training of the Model Benchmark IOT datasets are used to train and test the AI-based models that are proposed.

• The effectiveness of a model is evaluated using performance metrics like accuracy, precision, recall, the F1-score, and the rate of false positives.

• In order to evaluate advancements in adaptability and detection rate, traditional and AI-enhanced methods are compared

• To validate the models under realistic conditions, real-time simulation environments, such as IOT testbeds or network simulators (NS-3, Cooja), are utilized.

VI. Framework for Implementation and Deployment The final stage involves implementing the AI-based security architecture into an IOT ecosystem.

• IOT devices make up the edge layer, AI-enabled gateways make up the fog layer, and cloud-based analytical servers make up the cloud layer of the architecture. • Artificial intelligence feedback loops that continuously learn from new threats are used to automatically update security policies.Scalability, interoperability, and energy efficiency are evaluated for deployment.

VII. Adaptation and constant monitoring the system constantly monitors, learns, and adjusts to new threats because IOT security is dynamic.

• Analytic s driven by AI provide threat intelligence in real time.

• New attack datasets are used to retrain adaptive defines models on a regular basis.

• System robustness against zero-day attacks and evolving malware is enhanced by continuous feedback. [10] Mohmad Mahmoud and Almsman Khaled (2025) [12] Pureti,N (2023).

4.AI IN IOT APPLICATIONS

Artificial intelligence techniques are enabling technologies for hundreds of different applications in a wide range of IOT scenarios. AI are used for consumer and industrial IOT, industry 4.0, smart cities, smart buildings, smart homes, smart transportation, healthcare, environmental monitoring, agriculture and smart grids. In particular, AI has been shown to be effective in many aspects by supporting application design and implementation, as well as infrastructure and application management.

AI is mostly used to analyse server-side data from IOT sensors, but AI-based methods can often be used to locally process multidimensional signals in IOT devices due to the increasing availability of computational resources. The research community is particularly active in designing novel AI paradigms optimized for devices used in most of the IOT applications [15] [16] [20]. Artificial neural networks (such as feed-forward networks and deep learning methods), fuzzy logic, and evolutionary computation are the main AI technologies used in IOT applications at the moment. These technologies can be used for a wide range of tasks, including regression, classification, multidimensional signal processing, sensor calibration, measurement, data fusion, prediction, decision support, security, and data transmission.

Metrics for Evaluation: The accuracy, precision, recall, F1-score, and detection rate are used to evaluate performance.

Implementation Environment: A simulated Internet of Things network in which various sensors and devices use standard protocols like MQTT and COAP to communicate.

The primary goal is to evaluate how AI models improve the detection and response to cyber threats while maintaining system efficiency.

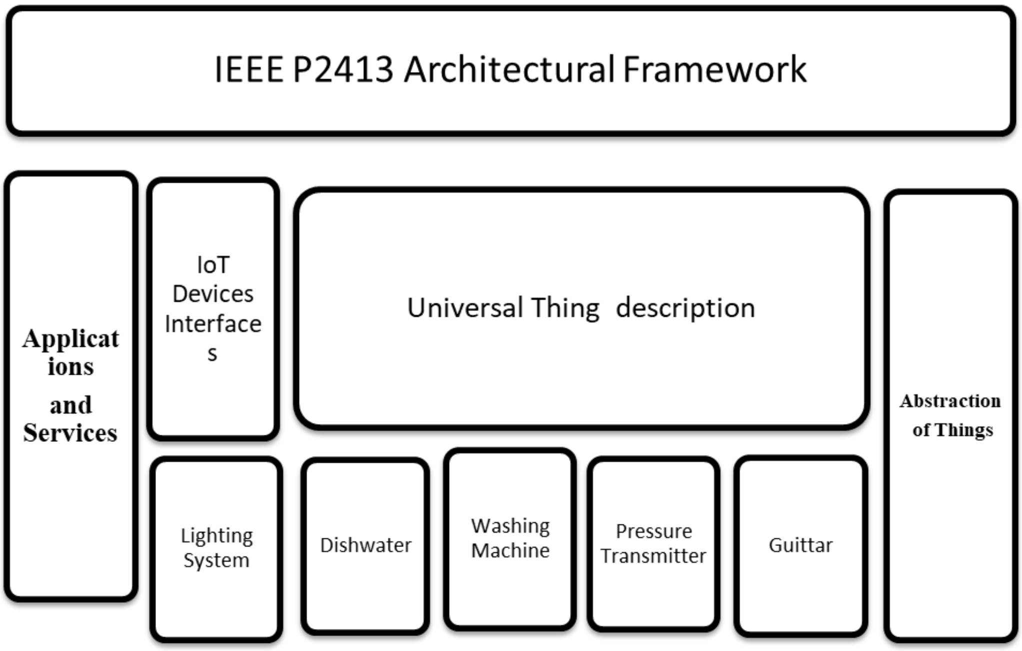

Table 1 IEEE P2413 Architecture Framework

5. Results and Discussion

AI-based systems demonstrate superior performance compared to traditional security methods.

Accuracy: AI-driven intrusion detection systems achieve over 95% accuracy in identifying known and unknown threats.

- **High Detection Accuracy (): -**The AI-driven IDs used advanced machine learning and deep learning algorithms that can analyse vast network traffic data and accurately identify both know (signature-based) and unknown (zero-day) attacks with more than accuracy.
- **Adaptive Learning (Self-Improvement): -** Instead of relying only on known attack signatures, AI models learn the normal behaviour of user, devices and applications. Any deviation from this pattern is flagged as a potential threat- helping to identify new or evolving cyberattacks.

Adaptability: Machine learning models continuously learn from new attack patterns, making them robust against zero-day exploits.

- The adaptability of AI driven IDS lies in their ability to continuously learn from new attack data. This makes them resilient against zero-day exploits, as machine learning models automatically update their detection capabilities without human intervention, ensuring consistent protection against evolving cyber threats.

Efficiency: Deep learning models can process large-scale data streams in real time, ensuring faster response and minimal downtime.

- **Real-Time Threat Detection**: AI enables instant analysis of large volumes of IOT data to detect threats as soon as they appear, reducing response time drastically.
- **Saleable Security Management**: AI algorithms can handle thousands of IOT devices efficiently, ensuring consistent protection across large-scale deployments.

Privacy Protection: Federated learning and encryption algorithms reduce the risk of data exposure, ensuring compliance with privacy regulations.

- **Data Encryption:** All IOT data-whether at rest or in transit- is encrypted using strong algorithms (e.g, AES, RSA) to prevent unauthorized access.
- **Data Anonymization:** Personally, identifiable information (PII) is removed or masked before data is processed by AI systems, ensuring user identity remains confidential.

However, implementing AI in IOT also introduces new challenges. High computational costs and the need for large labelled datasets may limit AI adoption in low-resource IOT devices. Additionally, adversarial AI attacks can manipulate machine learning models, making security systems vulnerable if not regularly updated.

5. Conclusion

Artificial Intelligence has emerged as a trans-formative technology for securing IOT systems. By enabling intelligent threat detection, adaptive defines mechanisms, and privacy-preserving analytic, AI ensures reliable and safe IOT operations. Future work should focus on lightweight AI models optimized for resource-constrained IOT devices, integration with block chain for decentralized trust, and development of explainable AI systems to improve transparency in decision-making.

The combination of AI and IOT not only enhances cybersquatting but also paves the way for a smarter, safer, and more connected world. Through intelligent threat prediction, detection, and mitigation, artificial intelligence has emerged as a transformative force for the protection of IoT ecosystems. The integration of AI with IoT enhances system resilience, ensuring continuous monitoring and timely response to cyber incidents. AI-based models empower IoT networks to evolve dynamically, adapting to new vulnerabilities and attack techniques without human supervision. Advanced machine learning algorithms enable IoT devices to identify abnormal behaviours, thereby reducing false alarms and improving detection accuracy. A multi-layered defines architecture for secure communication and data protection is made possible by the synergy of AI, blockchain, and cryptographic techniques. AI-driven analytics not only defend against cyberattacks but also optimize IoT performance, reliability, and energy consumption. IoT systems can become more autonomous and secure through the application of reinforcement learning and deep learning, which can improve decision-making capabilities. Future developments in explainable can further increase transparency and trust in IoT security systems. Continuous research and innovation are required to design lightweight AI models that can operate efficiently on low-power IoT devices.

6. References

1.Kumar, P., & Gupta, R. (2023). *AI-Driven Intrusion Detection in IOT Networks*. IEEE Internet of Things Journal

2.Zhang, Y., & Chen, L. (2022). *Deep Learning Techniques for IOT Security: A Survey*. Computer Networks, 210.

3.Li, X., & Zhao, Q. (2023). *Federated Learning for Privacy Preservation in IOT Systems*. Journal of Network Security, 45(2), 115–128.

4.Singh, A., & Kaur, P. (2024). *Blockchain and AI Integration for Secure IOpT Frameworks*. Elsevier Internet of Things Reports.

5.Patel, M., & Shah, D. (2023). *AI-Based Threat Detection Models for Resource-Constrained IoT Devices*. ACM Computing Surveys.

6.T. Cai, J.Li A.S. Mian, R. Li,T. Sallies, and J. X. Yu, “Target-aware holistic influence maximization in spatial social networks,” IEEE Transaction knowledge and Data Engineering, vol.4347, P.1.2020.

7.H.Liu, H.Kou, C.Yan, and L, Qi, ”Keywords-driven and popularity -aware paper recommendation based on undirected paper citation graph , Complexity, vol.2020, Article ID 2085638, 15 pages,2020.

8.Y.Chen, N.Zhang, Y.zhang,X.chen,W.Wu and X.S. Shen, “TOFFEE: task offloading and frequency scaling for energy efficiency of mobile devices in mobile edge computing,” IEEE Transactions on cloud computing, p.1,2019

9.AI-Protected Blockchain-based IoT Environments: Harnessing the Future of Network Security and Privacy-Rubeanic Ali Mohammedi (2024)

10.Artificial Intelligence in Security and Privacy: A study on AI’s role in Cybersecurity and data protection - Mohamed Mahmoud & Almsman Khaled (2025). International Journal of Education and Management Engineering.

11.Damaraju, A (2020). Social Media as a Cyber Threat Vector: Trends and Preventive Measures. Revisit Espanola de Documentation Scientific ,14(1),95-112.

12.Pureti, N (2023). Responding to Data Breaches: Step to Take When Your Data is Compromised. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1),27-50.

13.Gayam, R. R. (2021). Optimizing Supply chain Management through Artificial Intelligence: Techniques for Predictive Maintenance, Demand Forecasting, and Inventory Optimization, Journal of AI-Assisted Scientific Discovery.

14.AI Bashar, M, & Taher, M.A transforming US Manufacturing: Innovation in supply Chain Risk Management.

15. Purity, N (2023) Strengthening Authentication: Best Practices for Secure Logins International Journal of Advanced Engineering Technologies and Innovations, I (01),271-293.

16.Gayam, R. R. (2021). Artificial Intelligence in Healthcare Advanced Algorithms for Predictive Diagnosis, Personalized treatment, and outcome Prediction Australian Journal of Machine Learning Research and Applications (1),113-131.

17.Maruthi, S., Dodda, S. B., Yellu, R. R., Thuniki, P, & Reddy , S. R. B.(2021). Deconstructing the Semantics of Human - Centric AI: A Linguistic Analysis. Journal of Artificial Intelligence Research and Applications, I(1),11-30.

18.Pureti, N,(2022) Building a Robust Cyber Defence Strategy for Your Business Revisit de Intelligence Artificial in Medicines, 13(1),35-51

19.Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity Discover Internet of Things (vol. 1, article 7). Reviews how AI is applied in IoT cybersecurity, including threats and counter-measures. ￼

. 20.Security and Privacy in IoT Using Machine Learning and Blockchain: Threats & Countermeasures — Waleed N., He X., Ikram M., Usman M., Hashmi S. S., Usman M. (2020). ArXiv. Examines combined ML & blockchain for IoT security & privacy. ￼

21.AI-based Two-Stage Intrusion Detection for Software Defined IoT Networks — Li J., Zhao Z., Li R., Zhang H. (2018). Uses AI methods for intrusion detection in SD-IoT networks. ￼

22.Generative AI for Cyber Threat-Hunting in 6G-enabled IoT Networks Ferrag M. A., Debbah M., Al-Hawawreh M. (2023). Explores generative AI (GAN/Transformer) for threat hunting in next-gen IoT/6G. ￼

23.AI security and cyber risk in IoT systems — Radanliev A., De Roure D., Maple C., Nurse J., Nicolescu R., Ani U. (2024). A risk-assessment paper focused on AI security in IoT devices. ￼

24.Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends — Alharbi S., Attiah A., Alghazzawi D. (2022). Studies convergence of blockchain + AI for securing IoT networks. ￼

25.IoT Security Techniques Based on Machine Learning: How IoT Devices Use AI to Enhance Security — Surya L. (2019). IJCTT, 67(2), pp. 65-68. Focuses on ML techniques in IoT security. ￼

26.Security for AI and IoT Convergence: Novel Perspectives — Yogi M. K., Aishwarya D., Mundru Y. (2023). Discusses convergence of AI & IoT and the new security challenges. ￼

27.Security Protocols Using Artificial Intelligence to Prevent Internet of Things Attacks — Rajput M., Jaison F., Jain A., Mathur R. (2023). Looks at AI-based security protocols for IoT attacks.