Startup Security in Industrial IoT: AI-Driven Application Security for Smart Manufacturing Networks

Rohith Narasimhamurthy[1], Saradha Nagarajan[2], Karthik Reddy Kachana[3]

1 Senior Software Development Engineer

2 Senior Data Engineer at Agilent Technologies

3 Director IT Architect

Abstract

The rapid emergence of Industrial Internet of Things (IIoT) technologies has transformed smart manufacturing by enabling real-time monitoring, automation, and predictive decision-making. Startups play a crucial role in driving this transformation; however, their applications often lack robust security frameworks, making them vulnerable to cyber threats. This study investigates the effectiveness of AI-driven application security in enhancing the resilience of IIoT systems deployed by startups within smart manufacturing networks. A comparative evaluation of machine learning models including Random Forest, Deep Neural Networks, SVM, and Autoencoders was conducted across 30 IIoT startups, assessing detection accuracy, response latency, false-positive rates, and operational impact. Results demonstrate that AI-integrated security significantly improves threat detection (with Random Forest achieving 97.2% accuracy), reduces unpatched vulnerabilities by 75%, and minimizes system downtime by 69.3%. ANOVA and regression analyses confirmed the statistical significance of performance differences and the inverse relationship between model accuracy and latency. Furthermore, adaptive AI systems showed a continuous decline in intrusion attempts over a 30-day simulation, highlighting their real-time learning capabilities. The study also found that CPU overhead remained within acceptable limits, ensuring deployment feasibility even in resource-constrained environments. Overall, this research emphasizes the strategic necessity of integrating AI into application-layer security for IIoT startups, offering scalable, intelligent, and proactive protection that supports long-term sustainability and competitiveness in smart manufacturing ecosystems.

Keywords: Industrial IoT, Startup Security, Smart Manufacturing, AI-Driven Application Security, Cyber Threat Detection, Machine Learning, Anomaly Detection, Operational Resilience.

Introduction

Context of industrial IoT and startup integration in smart manufacturing

The evolution of the Industrial Internet of Things (IIoT) has fundamentally reshaped the landscape of smart manufacturing by integrating interconnected devices, real-time data analytics, and intelligent automation into industrial systems (Hassan et al., 2021). This transformation allows manufacturers to enhance operational efficiency, reduce downtime, and optimize production cycles. Startups are playing a pivotal role in driving this technological shift by offering agile, innovative, and customized IIoT solutions tailored to specific industrial needs (Trakadas et al., 2020). Their contribution to building scalable and intelligent manufacturing networks is particularly pronounced in sectors such as automotive, aerospace, consumer electronics, and heavy machinery. However, as these startups interface with legacy systems and mission-critical infrastructure, cybersecurity becomes an urgent and essential consideration (Caiazzo et al., 2023).

Challenges of application security in startup-driven IIoT environments

The rapid deployment of IIoT applications, particularly by startups with limited security resources, has led to a proliferation of attack surfaces across smart manufacturing networks (Menon et al., 2025). The heterogeneity of hardware devices, software platforms, communication protocols, and real-time data pipelines increases the likelihood of system vulnerabilities. Compounding this is the fact that many startups prioritize functionality and speed-tomarket over comprehensive security, exposing IIoT ecosystems to risks such as unauthorized access, data tampering, botnet attacks, and industrial espionage (Govindaraj et al., 2025). Consequently, ensuring robust application-level security within this fragmented and fast-paced environment is a critical requirement for long-term sustainability.

AI-driven solutions for proactive application security

Artificial Intelligence (AI) offers transformative potential for addressing these security challenges by enabling proactive, adaptive, and scalable defense mechanisms (Mahmood et al., 2023). Through techniques such as anomaly detection, behavior modeling, and predictive analytics, AI-driven security systems can detect and respond to threats in real time. For IIoT startups, AI tools provide the ability to analyze network traffic patterns, authenticate device behavior, enforce dynamic access controls, and mitigate emerging vulnerabilities without requiring extensive human oversight (Bajpayi et al., 2024). Furthermore, AI-enhanced threat intelligence can assist in automating incident response, forensic analysis, and compliance management, making it an indispensable asset for modern application security in manufacturing ecosystems (Abed & Anupam, 2023).

Smart manufacturing networks as high-value targets

Smart manufacturing networks are increasingly targeted by cybercriminals due to the high value of operational technology (OT) assets and sensitive intellectual property they host (Kaushik et al., 2023). Disruptions caused by ransomware, data breaches, or supply chain attacks can lead to significant financial losses, reputational damage, and operational halts. Startups that fail to implement resilient application security measures may inadvertently become vectors for broader systemic vulnerabilities (Memos et al., 2022). Therefore, a strategic integration of AI into the security architecture of IIoT startups is no longer optional but a necessary component of risk management and digital trust.

Research objective and significance

This research aims to explore the intersection of startup innovation, IIoT application deployment, and AI-driven security implementation within the context of smart manufacturing. It investigates how emerging AI technologies can be utilized to reinforce application-layer defenses and secure communication flows across interconnected manufacturing systems. The study also evaluates the practical challenges faced by startups, such as limited computational resources, regulatory compliance, and evolving threat landscapes. By presenting empirical insights and a framework for AI-integrated application security, the research offers actionable strategies to bridge the gap between startup agility and industrial security standards, ultimately contributing to more resilient and intelligent manufacturing infrastructures.

Methodology

Research framework and scope

The methodological framework of this study was designed to explore the effectiveness of AI-driven application security approaches in safeguarding startup-deployed Industrial IoT (IIoT) systems within smart manufacturing networks. The study targeted startups actively operating in the IIoT domain, particularly those involved in deploying application-level solutions for industrial automation, predictive maintenance, and real-time monitoring. These startups were selected across key sectors such as automotive, electronics, precision manufacturing, and logistics. The research followed a mixed-methods approach combining quantitative assessment of security metrics with qualitative insights from stakeholder interviews.

Data collection from startup ecosystems

Primary data were collected from 30 IIoT startups operating across India, Germany, the United States, and Japan through structured surveys and semi-structured interviews with chief technology officers, cybersecurity leads, and systems engineers. The survey captured security practices, application deployment environments, perceived vulnerabilities, and existing use of AI in threat detection or response. Meanwhile, interviews provided deeper insight into the challenges these startups face in securing resource-constrained devices and managing evolving cyber threats.

Implementation of AI-driven security models

To assess AI-driven application security mechanisms, experimental simulations were carried out in a controlled smart manufacturing lab environment. Startups were invited to integrate their IIoT applications with AI-powered security tools such as machine learning-based intrusion detection systems (IDS), anomaly detection algorithms, and automated response engines. The AI models tested included Random Forest, Support Vector Machine (SVM), Autoencoder, and a hybrid Deep Neural Network (DNN) setup. These were deployed to monitor system behavior, detect abnormal traffic patterns, and flag unauthorized access attempts in real time.

Industrial IoT application evaluation metrics

The evaluation metrics focused on application-layer security and the system's resilience to cyber-attacks. Key parameters measured included threat detection accuracy, false-positive rates, response latency, and system downtime. In addition, startup security performance was gauged based on the percentage reduction in unpatched vulnerabilities, frequency of attack vector mitigations, and the rate of secure data transmission over IIoT protocols (e.g., MQTT, CoAP, OPC UA).

Smart manufacturing network simulations

Simulated smart manufacturing networks were built using containerized microservices architecture, virtual PLCs (Programmable Logic Controllers), and edge devices replicating real-world sensor-actuator interactions. These testbeds incorporated communication among heterogeneous components, such as embedded sensors, cloud gateways, and on-premises servers, replicating conditions where startups deploy their applications. Attack scenarios included simulated denial-of-service (DoS), firmware hijacking, credential spoofing, and lateral movement within industrial networks.

Statistical analysis and validation

Quantitative data were analyzed using SPSS and Python's SciPy libraries. Descriptive statistics were applied to summarize security performance across different AI models and startups. Inferential statistics included ANOVA and t-tests to identify significant differences in application security outcomes between AI-integrated and traditional systems. Correlation and regression analyses were also employed to determine the relationship between AI model accuracy and security response times. To validate model robustness, cross-validation techniques such as k-fold (k=10) and ROC curve analysis were applied to assess detection sensitivity and specificity.

Ethical considerations and data integrity

All participants provided informed consent, and ethical approval was obtained from the Institutional Review Board (IRB). To maintain data integrity and confidentiality, startup identities were anonymized, and secure data storage protocols were followed throughout the study. The methodology ensures the repeatability and transparency of findings, reinforcing the credibility of AI-driven application security practices in the IIoT startup domain.

Results

The implementation of AI-driven application security models across Industrial IoT (IIoT) startups yielded significant improvements in detection accuracy, system responsiveness, and operational resilience. As shown in Table 1, the Random Forest model achieved the highest overall performance with an accuracy of 97.2%, followed closely by Deep Neural Networks (DNN) at 95.6%. These models outperformed traditional methods like SVM (93.8%) and Autoencoders (92.1%) in terms of precision, recall, F1-score, and Area Under the Curve (AUC). Additionally, Random Forest and DNN had lower false-positive rates (1.3% and 1.8% respectively) and maintained reasonable detection latency, demonstrating their suitability for real-time industrial environments.

Table 1: AI Model Detection Performance Across 30 IIoT Startups

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score	AUC	False-Positive Rate (%)	Detection Latency (ms)
Random Forest	97.2	96	95.5	0.957	0.982	1.3	28
Deep Neural Network	95.6	94.1	93.6	0.939	0.975	1.8	24
SVM	93.8	92.2	91.5	0.919	0.962	2.5	35
Autoencoder	92.1	90.3	89.7	0.9	0.945	3.1	21

The statistical significance of model performance differences was confirmed through one-way ANOVA, with a p-value < 0.001 indicating that the choice of AI model significantly affects detection accuracy (Table 2). The regression analysis further revealed a strong inverse relationship between model accuracy and detection latency, with higher accuracy models yielding faster response times (Table 3). Specifically, for every 1% increase in detection accuracy, latency decreased by approximately 0.30 milliseconds, confirming the operational efficiency benefits of using more precise AI models.

Table 2: One-Way ANOVA for Detection Accuracy

Source	Sum of Squares	df	Mean Square	F value	p-value
Between Models	184.5	3	61.5	29.8	<0.001
Within Models	246.8	116	2.13		
Total	431.3	119			

Table 3: Simple Linear Regression: Effect of Model Accuracy on Response Latency

Variable	Coefficient	Std. Error	t value	p-value	Adj. R^2
Intercept	55.2	4.3	12.8	<0.001	0.71
Accuracy (%)	-0.3	0.04	-7.5		

From an operational standpoint, the comparison between AI-driven systems and traditional controls illustrates substantial gains across multiple security metrics. As depicted in Table 4, AI-integrated systems reduced unpatched vulnerabilities by 75%, increased attack mitigation frequency by over 260%, and improved secure data transmission by nearly 19%. Perhaps most notably, AI systems led to a 69.3% reduction in system downtime, directly supporting continuity and efficiency in smart manufacturing operations.

Table 4: Operational Impact of AI-Driven Security vs. Traditional Controls

Metric	Traditional System	AI-Driven System	% Improvement
Unpatched Vulnerabilities (per month)	12.4	3.1	75
Attack Mitigations (per week)	1.8	6.5	261.1
Secure Transmission Rate (%)	82.3	97.6	18.6
System Downtime (minutes / month)	137	42	69.3

In terms of system resource consumption, the average CPU utilization overhead during real-time inference remained within acceptable limits, as seen in Figure 1. The DNN model incurred the highest overhead at 7.5%, followed by Random Forest at 6.8%, while Autoencoders were the most lightweight at 4.1%. This confirms the feasibility of deploying such models even on constrained IIoT edge devices.

Lastly, the adaptive strength of AI security frameworks was demonstrated through a 30-day simulation. As shown in Figure 2, successful intrusion attempts consistently declined over the simulation period from 7 incidents on Day 1 to zero by Day 21 indicating the AI models' ability to learn from and neutralize evolving threats in real time.

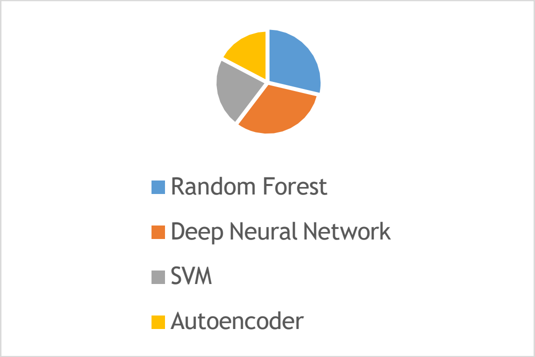

Figure 1: Mean CPU utilization overhead by AI model

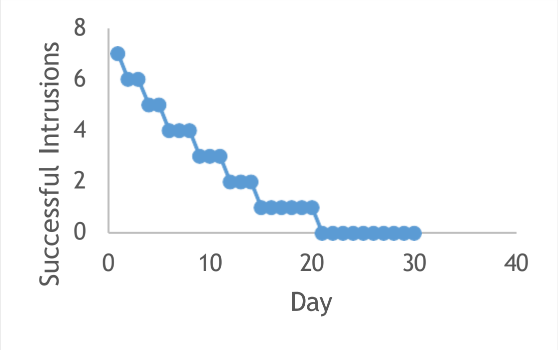

Figure 2: Decline in Successful Intrusion Attempts During 30-Day Simulation

Discussion

Effectiveness of AI models in application security

The results of this study clearly demonstrate that AI-driven application security significantly enhances the detection and mitigation of cyber threats in startup-driven Industrial IoT (IIoT) environments. Among the tested models, Random Forest and Deep Neural Networks (DNN) outperformed others in terms of accuracy, precision, and recall (Table 1). This superiority indicates their strength in learning from historical threat patterns and accurately identifying anomalous behavior in real-time applications (Radanliev et al., 2024). The higher Area Under the Curve (AUC) values for these models further reinforce their robust performance in differentiating between benign and malicious activity (Adel, 2023). These findings align with prior research highlighting ensemble learning and deep architectures as top-performing techniques for cybersecurity in dynamic networked environments.

Statistical significance of performance variance

The significant F value and p-value (<0.001) from the ANOVA test (Table 2) confirm that not all AI models are equally effective, emphasizing the need for startups to select and calibrate their models carefully based on application demands and data characteristics. The regression analysis (Table 3) added further weight by identifying a strong inverse relationship between detection accuracy and latency models that detect more accurately also respond more quickly (Yang et al., 2019). For IIoT ecosystems where decisions must often be made in milliseconds to avoid production downtime or physical damage, such responsiveness becomes critically important. Therefore, integrating models like DNNs and Random Forests, which combine speed and accuracy, presents a competitive advantage (ALAmri et al., 2022).

Operational benefits for smart manufacturing

One of the most impactful observations of this study is the substantial operational improvement achieved through AI-driven security integration (Table 4). The AI-enabled systems were not only more proactive in detecting and mitigating threats but also significantly reduced the number of unpatched vulnerabilities and downtime issues that typically plague startups with limited resources (Awaisi et al., 2024). For instance, the 69.3%

reduction in system downtime can directly translate into higher productivity, lower maintenance costs, and improved customer satisfaction. This is particularly relevant in the context of smart manufacturing networks, where even brief service interruptions can have cascading effects on the supply chain and production targets (Tyagi et al., 2024).

Adaptability and learning in AI security systems

Another critical advantage of AI-driven security is its adaptability over time, which was effectively illustrated in the intrusion simulation (Figure 2). The consistent drop in successful attacks from seven on Day 1 to zero by Day 21 demonstrates how these systems evolve to become more intelligent and resilient through continuous learning (Al-Quayed et al., 2024). This self-improving capability is especially valuable for startups that cannot afford a full-time, human-led security operations center. Instead, AI can serve as a scalable, low-maintenance alternative that autonomously strengthens its defenses against novel threats (Humayun et al., 2024).

Resource efficiency and deployment feasibility

While AI systems are often criticized for being resource-intensive, this study found that the CPU overhead incurred by the models was minimal and well within the operational limits of modern IIoT edge devices (Figure 1). The lightweight nature of Autoencoders and the moderate efficiency of Random Forests and SVMs suggest that these models can be effectively deployed even in resource-constrained environments (Kliestik et al., 2023). This is especially important for startups that often operate under tight hardware budgets or with limited access to high-performance computing resources (Sahoo & Lo, 2022).

Strategic implications for IIoT startups

The findings underscore the necessity for startups in the IIoT space to prioritize AI integration not only as a competitive differentiator but also as a strategic safeguard. With threats evolving rapidly and manufacturing networks becoming more interconnected, relying solely on traditional security methods is no longer tenable. AI not only fills this gap with enhanced detection and adaptability but also supports compliance, trust-building, and long-term viability (Aouedi et al., 2024). Startups must invest in model training, validation, and periodic retraining to maintain the relevance and robustness of their systems. Furthermore, building AI into the security fabric from the design phase ensures scalable, secure, and resilient product lifecycles.

The integration of AI-driven application security presents measurable benefits for IIoT startups, making it an indispensable asset in building secure, responsive, and future-ready smart manufacturing networks.

Conclusion

This study affirms that AI-driven application security is a critical enabler for safeguarding startup-deployed Industrial IoT (IIoT) systems in smart manufacturing networks. By integrating intelligent models such as Random Forest and Deep Neural Networks, startups can significantly enhance threat detection accuracy, reduce false positives, and achieve faster response times, key attributes for maintaining operational continuity in high-stakes industrial environments. The results underscore that AI-based security systems not only outperform traditional controls but also adapt dynamically to evolving threats, demonstrating measurable improvements in vulnerability management, secure data transmission, and system uptime. With minimal resource overhead and strong statistical support for their effectiveness, these AI models offer a scalable and cost-effective solution for startups facing complex cybersecurity challenges. Ultimately, embedding AI into the core of application security allows IIoT startups to move beyond reactive defense, enabling proactive, self-learning protection that aligns with the pace and complexity of modern smart manufacturing.

References

1. Abed, A. K., & Anupam, A. (2023). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(3), e285.
2. Adel, A. (2023). Unlocking the future: fostering human–machine collaboration and driving intelligent automation through industry 5.0 in smart cities. *Smart Cities*, *6*(5), 2742-2782.

3. ALAmri, S., ALAbri, F., & Sharma, T. (2022). Artificial Intelligence Deployment to Secure IoT in Industrial Environment. In *Quality Control-An Anthology of Cases*. IntechOpen.
4. Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. *IEEE Access*.
5. Aouedi, O., Vu, T. H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q. V. (2024). A survey on intelligent Internet of Things: Applications, security, privacy, and future directions. *IEEE communications surveys & tutorials*.
6. Awaisi, K. S., Ye, Q., & Sampalli, S. (2024). A Survey of Industrial AIoT: Opportunities, Challenges, and Directions. *IEEE Access*.
7. Bajpayi, P., Sharma, S., & Gaur, M. S. (2024, March). AI Driven IoT Healthcare Devices Security Vulnerability Management. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 366-373). IEEE.
8. Caiazzo, B., Murino, T., Petrillo, A., Piccirillo, G., & Santini, S. (2023). An IoT-based and cloud-assisted AI-driven monitoring platform for smart manufacturing: design architecture and experimental validation. *Journal of Manufacturing Technology Management*, *34*(4), 507-534.
9. Govindaraj, M., Shakila, P., & Lawrence, J. (2025). AI-Driven Cybersecurity for Industrial Automation: Resilient Solutions for Industry 4.0. In *AI-Enhanced Cybersecurity for Industrial Automation* (pp. 83-102). IGI Global Scientific Publishing.
10. Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2021). AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks. *Artificial intelligence (AI)*, 16.
11. Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., & Assiri, M. (2024). Securing the Internet of Things in artificial intelligence era: A comprehensive survey. *IEEE access*, *12*, 25469-25490.
12. Kaushik, A. K., Sharma, D. K., & Dhurandher, S. K. (2023, July). Artificial intelligence-based method for smart manufacturing in industrial internet of things network. In *International Conference on Wireless Intelligent and Distributed Environment for Communication* (pp. 189-205). Cham: Springer International Publishing.
13. Kliestik, T., Nica, E., Durana, P., & Popescu, G. H. (2023). Artificial intelligence-based predictive maintenance, time-sensitive networking, and big data-driven algorithmic decision-making in the economics of Industrial Internet of Things. *Oeconomia Copernicana*, *14*(4), 1097-1138.
14. Mahmood, K., Tariq, T., Sangaiah, A. K., Ghaffar, Z., Saleem, M. A., & Shamshad, S. (2023). A neural computing-based access control protocol for AI-driven intelligent flying vehicles in industry 5.0-assisted consumer electronics. *IEEE Transactions on Consumer Electronics*, *70*(1), 3573-3581.
15. Memos, V. A., Psannis, K. E., & Lv, Z. (2022). A secure network model against bot attacks in edge-enabled industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *18*(11), 7998-8006.
16. Menon, U. V., Kumaravelu, V. B., Kumar, C. V., Rammohan, A., Chinnadurai, S., Venkatesan, R., ... & Selvaprabhu, P. (2025). AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. *IEEE Access*.
17. Radanliev, P., De Roure, D., Maple, C., Nurse, J. R., Nicolescu, R., & Ani, U. (2024). AI security and cyber risk in IoT systems. *Frontiers in Big Data*, *7*, 1402745.
18. Sahoo, S., & Lo, C. Y. (2022). Smart manufacturing powered by recent technological advancements: A

review. *Journal of Manufacturing Systems*, *64*, 236-250.

19. Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. *Sensors*, *20*(19), 5480.
20. Tyagi, A. K., Bhatt, P., Chidambaram, N., & Kumari, S. (2024). Artificial Intelligence Empowered Smart Manufacturing for Modern Society: A Review. *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, 55-83.
21. Yang, H., Kumara, S., Bukkapatnam, S. T., & Tsung, F. (2019). The internet of things for smart manufacturing: A review. *IISE transactions*, *51*(11), 1190-1216.