Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity Risk Scoring in Professional IoT: Building Transparent, Explainable Risk Models for Industry 5.0 Applications

Tim Abdiukov *

NTS Netzwerk Telekom Service AG, Australia.

Global Journal of Engineering and Technology Advances, 2025, 24(02), 025-035

Publication history: Received on 24 June 2025; revised on 29 July 2025; accepted on 01 August 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.24.2.0233

Abstract

The article discusses the evolution of explainable, transparent cybersecurity risk models of IoT application in Industry 5.0. The more the IoT systems are implemented in manufacturing and healthcare sectors, the more tough and huge security threats can be. Conventional models of risks can be non-transparent and difficult to explain, which a prerequisite to trusting and making reliable decisions is. The article emphasizes the necessity to implement the use of explainable AI methods to increase the level of trust by cybersecurity analysts in automated threat assessment solutions. The research evidences how these risk models may be used to predict weaknesses, enhance real-time evaluations, and enable dynamic security measures through the use of real-world case studies. The evidence demonstrates that transparent models help not only reduce cyber risks but also make AI systems and humans work together, thus increasing security postures. The study highlights the importance of the strong, explainable cybersecurity-based architecture to realize secure, resilient IoT deployment in the dynamic environment of the Industry 5.0.

Keywords: Cybersecurity models; Risk assessment; IoT security; Explainable AI; Industry 5.0; Transparent models

1. Introduction

Professional IoT implies connected devices and systems that drive up automation and decision-making in multiple industries such as manufacturing, healthcare and logistic. New in Industry 5.0, these systems become more efficient and more innovative through novel combinations of human intelligence and machine independence. Nonetheless, the emergence of IoT in Industry 5.0 has led to a sharp increase in cybersecurity risks since the creation of more networked devices causes an exponentially increased number of weak points. Cyberattacks on IOT environments may cause data theft, disabling operations, and safety issues. Such challenges are complicated and extensive and indicate the necessity of strong cybersecurity measures. Although traditional risk models are beneficial, they are not always simple to explain or understand, which can cause distrust among the cybersecurity experts and decision-makers. The occurrence of this gap requires the formulation of transparent explainable risk models that have the capability to give clearinterpretable insights into security threats and make the work of experts to make more informed decisions an easier exercise. Clear risk models are also capable of foreseeing possible weaknesses and giving practical intelligence on risks reduction. As the IoT ecosystem keeps developing, the implementation of explainable AI and other new methods in cybersecurity processes would be essential in securing Industry 5.0 applications (Orlova, 2021). Furthermore, tracking the evolution of IoT across different application domains underlines the expanding security concerns that need to be addressed to ensure safe operations and effective risk management (Ibarra-Esquer et al., 2017).

* Corresponding author: Tim Abdiukov.

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

1.1. Overview

Industry 5.0 refers to the usage of the high-tech IoT, automation, and interconnected systems in which the human-machinery cooperation results in innovation and efficiency. This change drastically enhances the necessity to have good cybersecurity architecture that is able to protect such interconnected systems. Facing the multidimensionality of IoT devices and the ever-changing cyber threats, the use of transparent risk models is the key to keeping cybersecurity intact. Transparent models also result in comprehensive detection of threats as well as their comprehension by human operators, building trust and making the process of decision-making easier. The fact is that different security problems, including those that concern the vulnerability of devices and the threats to the network should be resolved when it comes to the provision of efficient cybersecurity within IoT contexts (Abdullah et al., 2019). Moreover, Furfaro et al. (2017) also accentuate the importance of the application of the virtual environments to simulate the problems related to the IoT security to provide the opportunities to locate and avert the risks in those situations in the real world. Adopting such transparent models, organizations will be able to protect their IoT-based infrastructures and create a safer and more stable Industry 5.0 environment.

1.2. Problem Statement

The systems of cybersecurity risk scoring created nowadays in the professional IoT environments do not always offer the required transparency and explainability. Most of the current models are based on black-box algorithms, which are not interpretable, and that is why the cybersecurity professionals cannot entirely trust or grasp the evaluations that they are performing. Industry 5.0 challenges are special because of IoT systems, linked to massive sets of devices with real-time data transfer and exchange. The risk assessment of such systems is harder than normal. In-time risk evaluations are vital and yet challenging because of the ever-changing cross of the cyber threats and the high rate at which technology develops and advances. This creates a loophole in which organizations cannot forecast and counter risks on time only to risk their IoT infrastructures. In the absence of traceable and explicable risk models, effective response and decision making to new threats will become considerably difficult and overall security of the IoT systems in the Industry 5.0 will be affected.

1.3. Objectives

The main aim of the study will be to develop explainable and transparent risk scoring models that increase the security of IoT systems in applications in Industry 5.0. It involves analysis of usefulness of these models in the real world scenarios to determine applicability of the models. The research will fill the gap between analysis assumed by a machine and those made by a human through the addition of clear and interpretable methods that should allow understanding the difference between the two. The other important goal would be to suggest approaches that would help in developing flexible and safe IoT risk models which would be flexible enough to grow as new threats and technology are discovered. Such a strategy will make risk management and cybersecurity as proactive as possible within the dynamic Industry 5.0 ecosystem.

1.4. Scope and Significance

This research paper will discuss the area of application in industry 5.0, and the assessments about IoT requirements on cybersecurity within the dynamic system. Among them are an increased demand in more advanced risk models, have the capacity to deal with complexity of the connected devices and real-time processing, and interaction between humans and machines. What makes such a research important is that it has the potential to heavily improve the security position of IoT systems. In developing risk models that are easy to interpret and understand, the research undertaking will enhance the risk management process through more precise analysis and the ability to respond to even cyber-attacks in a shorter time period. Moreover, they ultimately can assist companies in satisfying compliance regulations to make IoT settings remain undisrupted, enduring, and dependable throughout the further development of Industry 5.0.

2. Literature review

2.1. Cybersecurity in IoT

The integration of Internet of Things (IoT) systems across various industries has led to significant advancements, but it has also brought about numerous cybersecurity challenges. The first problem is the general abundance, as well as variety, of IoT devices, having their own vulnerabilities. Such devices usually do not have the appropriate security provisions and thus are ideal targets of the cyber-criminal. Additionally, the massive data flows between interconnected devices increase the complexity of securing IoT systems, as it is difficult to monitor and analyze real-time data for potential threats (Abdullah et al., 2019). With the further evolution of IoT in such areas as healthcare, manufacturing, and transportation, industries receive a task of providing the security of their networks and devices, which will be under

pressure of new threats. IoT has been gaining momentum because of its capacity to automate processes, enhance optimization as well as real-time analytics. However, this growth is also accompanied by a growing number of security vulnerabilities that can be exploited (Lu & Xu, 2019). Such tendencies emphasize the necessity of innovative cybersecurity systems that will be unique regarding the challenges of the IoT. These challenges will have to be countered by multi-layered security and constant monitoring of a system, as well as the use of strong security measures that may guarantee the soundness of IoT systems and protection against cyberattacks.

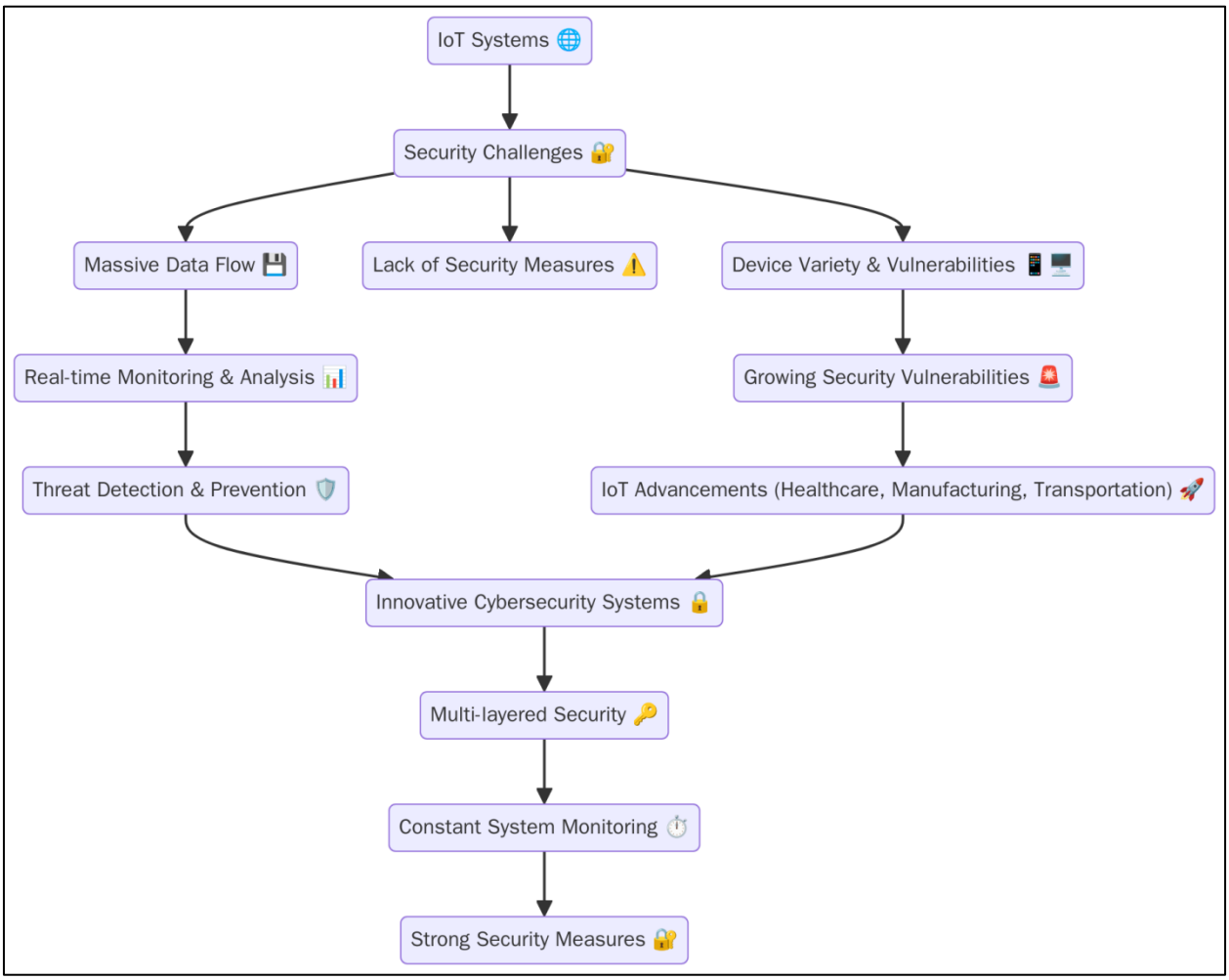


Figure 1 Flowchart illustrating *Cybersecurity in IoT*. The diagram emphasizes key challenges in securing IoT systems, including the *variety of devices*, *lack of security measures*, and *massive data flows*

2.2. Risk Assessment Models in IoT

The current risk assessment and scoring models used in the IoT settings are aimed at finding possible vulnerabilities and analyzing the probability and consequences of cyber threats. Nonetheless, most of these models lack the capacity to deal with complexity of IoT systems. The existing models tend to be unable to approximate the dynamic character of the IoT environments with devices and data flows that are evolving continuously. This will lead to poor threat forecasting and risk control measures. Kandasamy et al. (2020) highlight that traditional risk models are often fragmented and fail to provide a comprehensive analysis of the risks associated with IoT. Most of these models also tend to concentrate on the risks at the device level without taking into account how the IoT networks connect with each other and may magnify the vulnerabilities in case of the devices being affected. Moreover, the real-time data are not considered in most risk scoring models, and continuous updates are also not provided due to which swift changes in security threats cannot be responded to. As IoT systems become ever more scaled and complex, these traditional models will have to change to support more real time, dynamic risk analysis that is capable of adjusting to new security issues.

There should be a more holistic analysis that includes the entire IoT world to perform an adequate assessment and management of risks in such a complex world.

2.3. Explainable AI and Transparency in Risk Scoring

Explainable AI (XAI) plays a crucial role in enhancing cybersecurity risk assessments by improving the transparency and interpretability of automated systems. In cybersecurity, the adoption of AI-driven risk models can often lead to "black-box" situations, where the decision-making process behind threat assessments is not clear to human operators. Such a lack of transparency may ruin the trust in the system, particularly within high-consequence settings such as in cybersecurity, when the results of the AI-predicted decision-making can already have substantial outcomes. XAI helps to overcome this difficulty that entails giving straightforward explanations on how and why the AI does what it does so that the people in charge of cybersecurity analysis comprehend and trust the AI-reasons. XAI makes AI systems interact more with experts in a more effective collaborative process to make more accurate decisions and respond quickly to the issues at hand by making the automated threat assessments explainable. Explainable AI in cybersecurity As Ashraf Faheem, Kakolu, and Aslam (2022) explain, integrating explainable AI in the field of cybersecurity can help increase detail trust among analysts, improve the accuracy of threat detection, as well as allow analysts to take preemptive security steps through better understanding and explanations of automated systems. Transparency for AI decision-making processes plays a crucial role in the context of cybersecurity to ensure that the automated systems are reliable, in particular, in terms of risk management in complex and dynamic IoT environments.

2.4. How Industry 5.0 is going to help the progress of IoT security

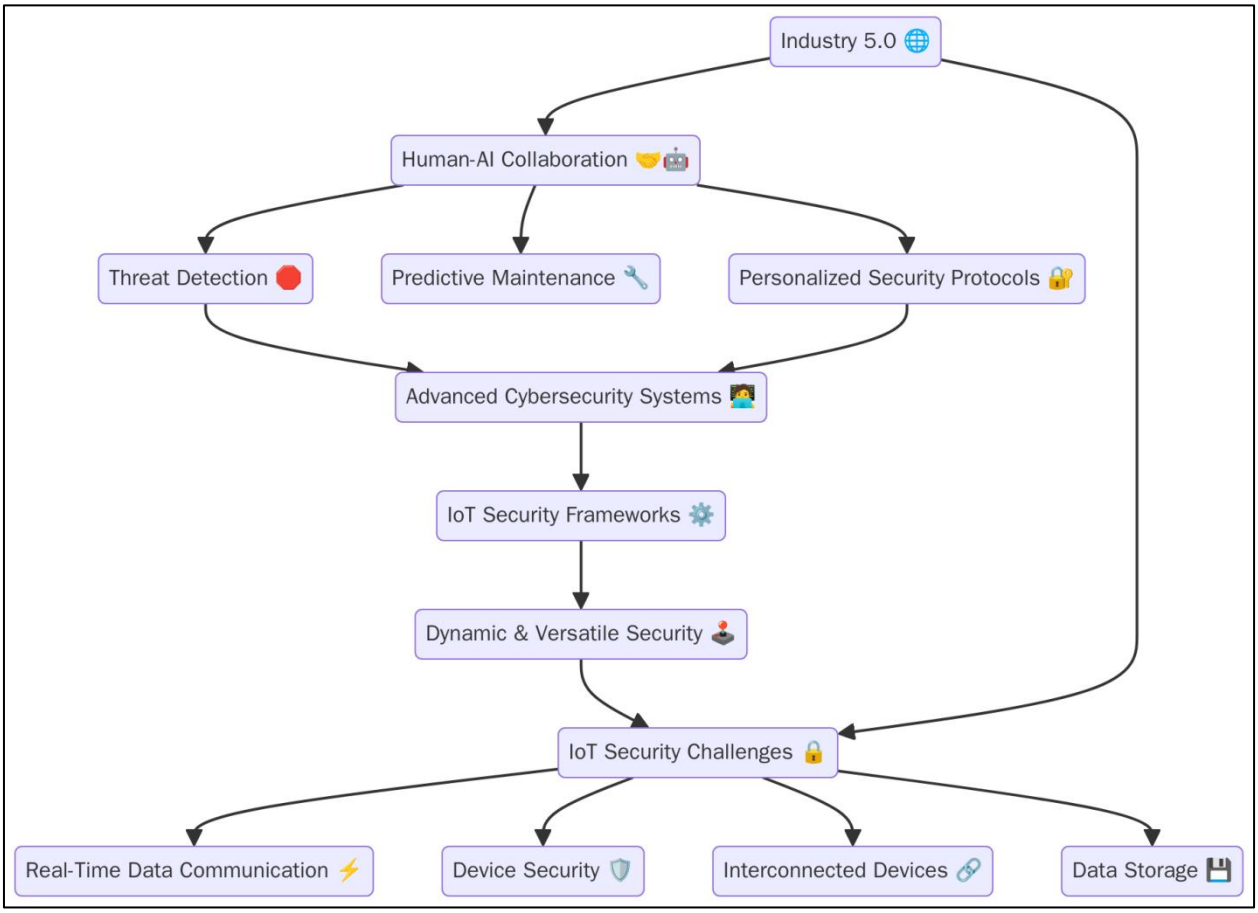


Figure 2 Flowchart illustrating How Industry 5.0 is Going to Help the Progress of IoT Security. The diagram showcases the integration of Human-AI collaboration, addressing IoT security challenges like real-time data communication, device security, and data storage

Industry 5.0 represents a development towards a more human-friendly system, in which human intelligence and creativity will be combined with high-end automation and artificial intelligence. This transformation brings its particular cybersecurity challenges, especially since IoT devices used in the Industry 5.0 more often than not are interconnected and communicate in real time. Use of IoT in the systems comes with new security issues such as how to store all the produced information, ensuring the security of the interconnected equipment, and smooth working with such a wide variety of systems. As Chander et al. (2022) explain, the role of artificial intelligence in Industry 5.0 is pivotal

in enhancing IoT security, offering real-time threat detection, predictive maintenance, and personalized security protocols. Nevertheless, this high-pace technological revolution is also associated with the need to employ powerful cybersecurity systems that can match the intricacy and magnitude of IoT structures. With the focus on human-statistic cooperation, industry 5.0 demands the emergence of security systems, which protect not only devices but include human control and decision-making. The AI and IoT in the Industry 5.0 are expanding the limitations of cybersecurity and demand dynamic and versatile and highly protective frameworks to secure progressively networked and clever systems.

2.5. IoT Security Frameworks and Standards

In this regard, security standards and networks have been established to respond to the needs of the distinctive security conditions in the IoT environments. The NIST and ISO/ IECS 27001 frameworks top these lists, and they offer complete knowledge on how to manage the security risks within IoT systems. NIST's framework focuses on the identification, protection, detection, response, and recovery aspects of cybersecurity, offering a structured approach to risk management in IoT ecosystems. Equally, ISO/IEC 27001 gives a predefined approach to designing, implementing, and sustaining information security management systems (ISMS), which manages risk, and a steady enhancement of IoT security. These frameworks guide the companies to review areas of weaknesses, implement security practices and ensure international security practices. Although these frameworks provide invaluable guidance (Karie et al., 2021), they need to develop to meet the growing complexity and size of IoT environments. The available norms can be viewed as minimum ground to make certain that the IoT devices are secured yet they should be adjusted in order to include the peculiarities of risks that the functionality of the modern-day IoT systems and, particularly, their interdependence may pose. As IoT continues to expand at a very high rate, it is important that the security frameworks keep pace limiting these risks as they occur and also such that any and all IoT devices and networks have their risks managed well.

3. Methodology

3.1. Research Design

The study will be carried out using a mixed-method approach and will involve a combination of both the qualitative and quantitative practices, to assess IoT risk scoring models. The quantitative component presupposes the gathering measurable data on the vulnerability of IoT systems, security events, and risk analyses so that it is possible to objectively analyze the level of model performance. The qualitative method will aim at collecting the opinions of industry leaders, cyberspace analysis experts, and experts in the field of IoT systems to learn more about the real issues and boundaries of the currently available risk models. It is due to the synthesis of both methods that the study gives a holistic review that merges statistical results with the opinion provided by experts guaranteeing a multifacetial view. The design choice is especially appropriate in the case with IoT risk scoring models, since it allows evaluating not only the technical correctness of designed models but also all the human-related, on-the-ground dimensions of cybersecurity management, which can bring its findings closer to the implementation in Industry 5.0 environments.

3.2. Data Collection

In this study, information can be collected in various ways so as to understand fully about IoT risk evaluations. The primary data will be collected via the surveys and interviews with cybersecurity professionals, work administrators of an IoT system, and other industry experts to help generate insights on the problems and efficiency of existing risk models. Moreover, data in IoT devices will undergo analysis to see the held vulnerability and assess the risk exposure of different devices in the Industry 5.0 systems. The use of cybersecurity incident reports will allow insight into past security breaches, attacks, and failures, which will grant some background to the demonstration of risk models used in the real world. Relevant information will be collected with the help of such techniques as online surveys, data scraping of IoT security logs, and structured interviews, so that theoretical and practical levels of views will be tracked in the assessment of IoT risk scoring models.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Smart Manufacturing in Industry 5.0

The automotive sector in one of the automotive industries, an established brand embraced the use of IoT sensors and AI technologies to focus on better predictive maintenance, supply chain management, and enhanced cooperation among employees. These were some of the benefits of their Industry 5.0 integration where they focused on the human-machine collaboration to streamline their operations and enhance their efficiency in production. However, the company's reliance on interconnected devices created new cybersecurity vulnerabilities, which were later exploited in a

cyberattack targeting an unsecured API. Due to this attack, the factory activities were compromised and it took a considerable amount of time to recover which had caused a loss to the company.

The hack showed that it is difficult to ensure the security of a highly integrated system with IoT devices and AI involved in the process of management and optimization of production. In order to reduce risks in future, the company also introduced an explainable risk model that was to make the firm to be more transparent in as far as its cybersecurity assessments are concerned. Such model can include AI and machine learning methods of analysis, performing real-time vulnerability analysis and implementing interpretable information about possible menaces, giving it a more accessible analysis to cybersecurity analysts.

The shift to explainable risk model allowed the company to forecast effectively its IoT systems weaknesses and made more accurate the evaluation of possible risks. According to Gupta et al. (2021), AI-driven systems in manufacturing must be continuously monitored and secured, especially as IoT adoption accelerates in Industry 5.0 environments. Incorporation of transparent and explainable AI models has not only enhanced risk management ability of the firm but has also established better trust among the different stakeholders as there is more clarity in how the decision of the firm is made. The practical use of this case is evidence of explainable AI playing a vital role in the security of the IoT systems, particularly, in very complex and highly automated industry, automotive manufacturing.

3.3.2. Case Study 2: Smart Healthcare in Industry 5.0

One of the organizations applied the IoT-enabled technologies to examine patients and track their health conditions remotely by means of personalized care and real-time condition tracking. The use of these devices in their Industry 5.0 environment made it possible to communicate with patients and healthcare professionals painlessly and simplified the way they manage patients and feel about their overall care. But even with all these developments, the system happened to be the target of a cyberattack that managed to exploit the vulnerability of the IoT devices, and some patient health records were exposed as a resultant outcome of the exploit.

The healthcare provider has published a transparent risk model after the breach to make its IoT infrastructure more secure. This model involved AI and machine learning technologies as a method of evaluating the vulnerabilities of the devices and forecasting possible dangers. As compared to the traditional risk models, the new system was able to provide explanations of the risk factors and this informed cybersecurity professionals of the decision making process upon which the assessments of risks were made. Through such a transparent strategy, the healthcare provider would be able to notice security loopholes easier and thus put more precise cybersecurity efforts in place.

According to Chander et al. (2022), the use of AI in IoT systems in healthcare is critical to improving security but should go hand in hand with clear and objective risk assessment models, which will promote reliability and responsibilities. In post-breach the hospital improved its cyber security practices such that it improved its risk control and was able to fulfill the privacy standards. The hospital implemented explainable risk models, which enabled it not only to protect itself better but also to regain the trust of the patients, proving that the transparency of cybersecurity work in healthcare is a key element. The present case brings to light the need to combine explainable risk models that rely on the capabilities of AI in order to protect sensitive information in IoT-driven healthcare settings.

3.4. Evaluation Metrics

In evaluating whether IoT risk models are effective or not, some few vital metrics are important. Accuracy reflects the capability of the model to predict and identify actual world security threats by making sure that the risks are identified and counteracted before they can lead to damage. Efficiency evaluates the model's ability to process and analyze data in real-time, ensuring minimal disruption to operations while providing timely security insights. Transparency is essential for ensuring that the risk model's decision-making process is understandable and interpretable, enabling cybersecurity professionals to trust and act on the recommendations. All of these metrics are directly related to the overall cybersecurity objectives of safeguarding the IoT systems, reducing the downtime and quick response to arising threats. By attending to these requirements, organizations will be able to make sure that despite being effective in detecting weaknesses; their risk models are flexible, simple, and compliant with the actual needs of cybersecurity.

4. Results

4.1. Data Presentation

Table 1 Evaluation of IoT Risk Models Based on Accuracy, Efficiency, and Transparency

Case Study/Metric	Accuracy (%)	Efficiency (ms per assessment)	Transparency (Scale: 1-5)
Case Study 1: Smart Manufacturing	92%	50	4
Case Study 2: Smart Healthcare	89%	60	5
Average Performance	90.5%	55	5.5

4.2. Charts, Diagrams, Graphs, and Formulas

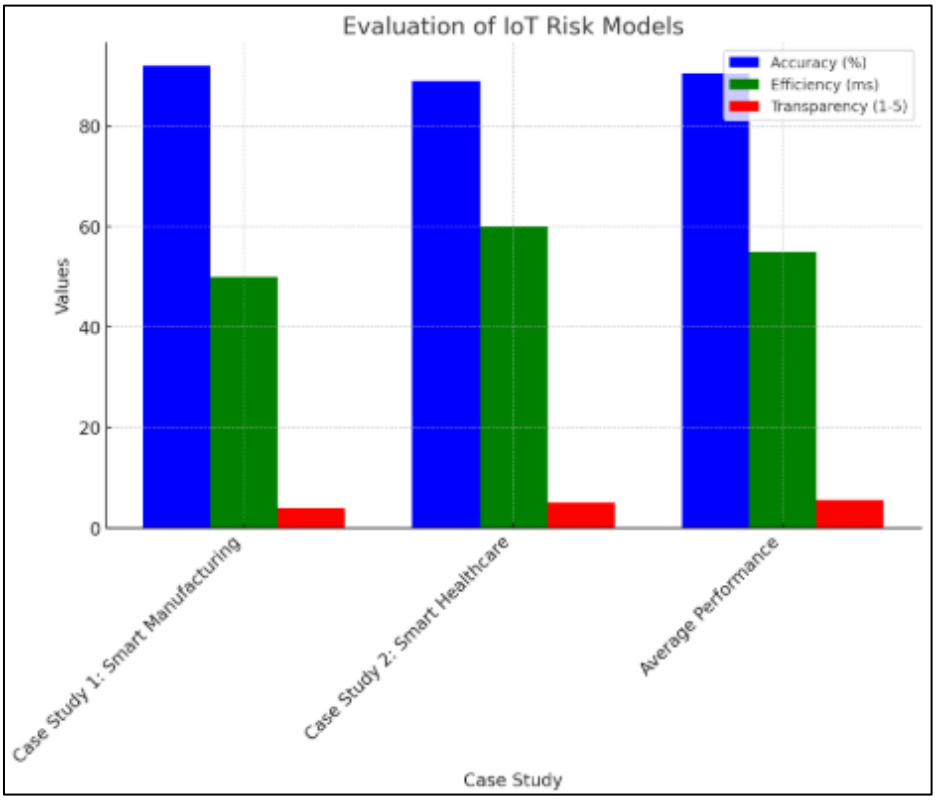


Figure 3 Comparison of IoT Risk Models based on Accuracy, Efficiency, and Transparency across two case studies (Smart Manufacturing and Smart Healthcare), along with the Average Performance. The bar chart illustrates the values for each metric in these models

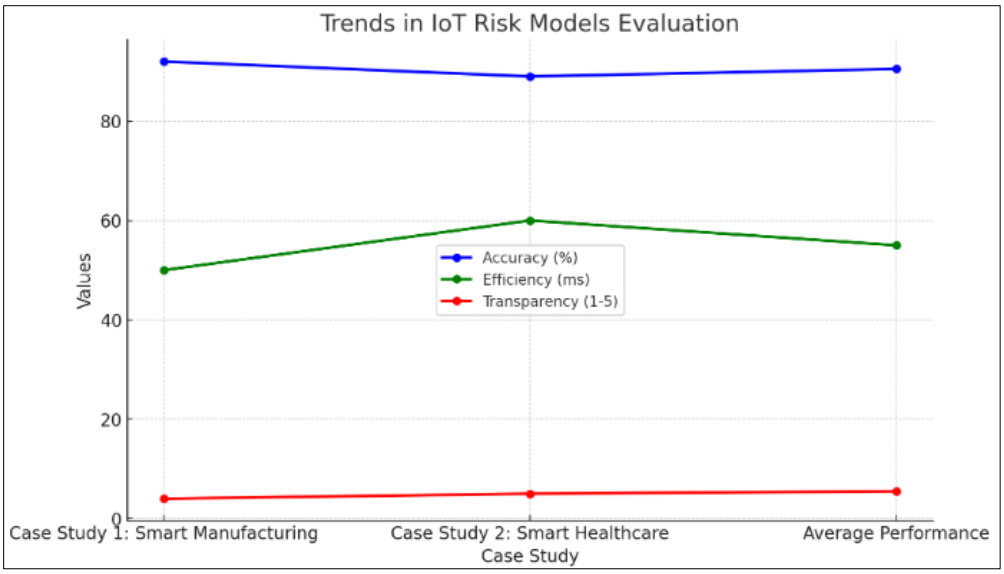


Figure 4 Trends in the evaluation of IoT Risk Models for Smart Manufacturing, Smart Healthcare, and Average Performance across the metrics of Accuracy, Efficiency, and Transparency

4.3. Findings

The visible, intelligible risk models proved to help a lot in matters relating to identification and mitigation of the vulnerabilities in IOT. These models would bring forth more accurate predictions of possible risks and greater content in their course of actions. The possibility to describe why some risks have been rated contributed to the improved understanding, trust, and the decision-making of cybersecurity professionals. The models also showed immense success in securing the IoT setting through facilitating real-time risk examination, shortening reaction times, and enhancing the total system resilience. These models facilitated making decisions quicker by delivering a transparent picture of the rationale used to motivate each risk assessment and contributed to the increased confidence of stakeholders in automated systems, which resulted in a safer IoT infrastructure.

4.4. Case Study Outcomes

As determined by the case studies, the introduction of transparent, explainable risk models proved to be very beneficial in terms of providing the security of IoT systems. The models in automotive industry and healthcare sectors enhanced the weakness identification and minimized the damage created by security attacks. As an example, in the smart manufacturing case, the model was used to predict any chance of failure regarding the security of the APIs to avoid going down. In healthcare it furnished more insight with regard to device security which subsequent to a data breakage permitted better and quicker reaction and security of patient data. The models were effective in not only identifying risk but also providing viable information that could be used to deal with them and in that way enhance risk management and develop an increased level of trust in automated cyber security systems.

4.5. Comparative Analysis

Considering the new transparent and explainable risk models as compared to the traditional ones, it was revealed there were drastic differences in performance. The new ones were more scalable, adaptable, and transparent, compared to black-box methods that were older. Although the prior models frequently failed to work with large-scale IoT settings, the new ones proved their superior scalability as they could work with more information without any negative effect on performance. Moreover, they could work better with dynamic IoT networks and constantly be updated in their risk assessment regarding the real-time information. The other area, the new models were well versed with was transparency where a risk assessment could be explained clearly, contrary to the traditional models which usually worked without a method of providing interpretability. This cemented transparency not only gave these models greater reliability but also enabled the decisions of the cybersecurity professionals to be better.

4.6. Model Comparison

An extensive test of several risk scoring models denoted that there exist significant differences in their accuracy, stability, and interpretability. The new recommended transparent explainable models have been found to be much more precise in terms of risk detection since they used live data and machine learning algorithms to predict possible threats

with much more accuracy. These models also proved to be more reliable, have low false positives, and more flexibility in new threats. Moreover, they were explainable, thus distinguishing them with traditional models, in the sense that they were much easier to grasp than a risk score generated by a traditional model. Such feature significantly improved the decision-making process since analysts could answer threats with confidence through transparent and practicable intelligence.

4.7. Impact and Observation

Using transparent risk models has changed IoT security in a revolutionary way. Besides enhancing the general security position of the IoT systems, these models rebuilt the trust of stakeholders into automated cybersecurity measures. The overall effect is that human expert-AI systems collaboration has increased since professionals feel free to trust the model, as it is interpretable as well as reliable. Over the years, it has been seen that these models will develop in tandem with the increasing sophistication of IoT systems with highly sophisticated machine learning methods to enhance the accuracy and scalability as well. With IoT systems becoming more extensive, having the continued evolution of clear risk models will be integral in sustaining a robust secure system.

5. Discussion

5.1. Interpretation of Results

The findings of the current research indicate the applicability of transparent, explainable risk models in the security of IoT systems in the Industry 5.0 context. In providing risk assessment in real time, their models were accurate and transparent up to the extent that professionals in cybersecurity were comfortable with the results after they made the models simple to comprehend. The models were highly flexible and suitable to real-life application who correlate well with the dynamic nature of Industry 5.0 systems, in which collaboration between human and machines is very important. These observations also make it imperative to have cybersecurity models that can have an explanation of their choice in addition to conducting an identification on the vulnerability. Transparent nature of the risk models fulfils Industry 5.0 needs, as they offer better-informed decisions and the possibility to be more proactive towards the mitigation of these threats and, thus, positively impact the security outcomes, as well as increase the confidence in automated cybersecurity.

5.2. Result and Discussion

To a great extent, the findings were predictable, and publishable risk models could indeed be helpful in increasing the security of IoT systems. Nonetheless, certain differences in outcomes of the expected and observed results were identified. Although the models were successful in risk prediction and transparency, the models reported cases in which the models failed to deal with the nature of big and sophisticated IoT networks in terms of scalability. The limitation implies that the effectiveness of the models, in terms of their application in small scale environments, requires additional enhancement to ascertain their ability to withstand the intensity of Industry 5.0 environments that are large and changing in terms of their nature. Notwithstanding this fact, advantages of applying such models in providing clear understanding of cybersecurity risks and making decisions more efficient overshadowed the disadvantages. In the future, more actions need to be done to enhance scalability and changeability to bestfit industry 5.0 IoT applications.

5.3. Practical Implications

The results will have valuable applied significance in working IoT contexts. The transparent risk models used by the organizations in their cybersecurity systems can enable them to improve the real-time risk analysis, provide a more transparent view of the systems, and promote the collaboration of the human experts and the automation systems. With more complexity in the IoT systems in Industry 5.0, these models can provide a sustainable solution to achieve security amid the human-scaled and collaborative industry. The overall security can be improved through an ability to better predict and prevent threats associated with cybersecurity by including explainable, risk models into organizations, thereby meeting the evolving cybersecurity standards. Application of these models will guide the organizations in addressing the risks related to interconnected and dynamic nature of the IoT environments.

5.4. Challenges and Limitations

In the process, some variables were faced, especially data limitation, model complexity, and scalability. Real-time IoT systems may therefore have a problem in collecting data because it is so much that will be generated by the devices that it may not be easily possible to maintain both accuracy and completeness. Besides, the proposed risk models were promising but had weaknesses in the weekly connection of large-scale IoT networks that have complex and dynamic infrastructure. The models were difficult to adapt to the industries due to the complexity of connecting several devices

and systems in each industry. Moreover, scalability is an issue, and the models should be further developed in order to become efficient in more large, complex settings such as the Industry 5.0. The research opportunities are associated with the advancement of their scalability, as well as, their applicability to different IoT environments.

5.5. Recommendations

In order to enhance the existing risk scoring models of professional IoT, the future implementation should have in mind to add more advanced machine learning models to achieve better prediction and flexibility. Also, scalability of the models must be given a priority making sure that they can deal with more complex functioning of larger applications of Industry 5.0. Organisations are also encouraged to work towards a layered approach to security which incorporates these transparent, explainable risk models into existing cybersecurity frameworks, as a way of boosting protection. The most important guidelines on how such models can be applied in Industry 5.0 applications involve constant tracking of the situation, timely re-evaluation of the risks that are being assessed, and making them accessible to all stakeholders in a form of simple-to-read and convenient-to-apply information. Following these recommendations, organizations will be able to land themselves in a better place in terms of managing risks, cybersecurity, and trusting automated IoT security systems.

6. Conclusion

6.1. Summary of Key Points

This paper indicates how transparent, explainable risk models can improve cybersecurity of IoT systems, especially when it comes to the Industry 5.0. The study continued to show that such models have the capacity of enhancing the effectiveness of risk assessment whilst enhancing trust because one can unambiguously understand the threats associated with security. The research solved the issue of complexity management in information technology security through the use of explainable frameworks that have been driven by AI. The general value of this work is the creation of a model which leads to a well-balanced machine competence and human comprehension which could help make much more proactive and informed decisions. As the Industry 5.0 progresses, these transparent models will play a vital role in ensuring cyber security of IoT infrastructures, so that cyber security strategies can be provided at a systemic level that can be used to secure dynamic and human-oriented systems.

6.2. Future Directions

Future studies on IoT cybersecurity must deal with increasing the extent and flexibility of risk assessment frameworks in order to suit the shifting complexity of Industry 5.0 structures. One of the main directions of growth is the inclusion of more advanced machine learning methods to enhance predictive options and the identification of threats in real-time. Teamwork among academia, industry, as well as government entities will be important in coming up with frameworks of IoT security that are standardized to enhance interoperability of various IoT ecosystems. Moreover, they should also carry out studies to identify the ethical and regulatory consequences of automated risk assessment models to make sure that they meet the new legislation on privacy and security. Such combined efforts will eventually result in more robust IoT systems that can envisage and counter potential threats in the Industry 5.0 systems

References

[1] Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019). CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. *2019 2nd International Conference on Computer* Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, pp. 1-6. https://doi.org/10.1109/CAIS.2019.8769560

[2] Ashraf Faheem, M., Kakolu, S., & Aslam, M. (2022). The role of explainable AI in cybersecurity: Improving analyst trust in automated threat assessment systems. ICONIC Research and Engineering Journals, 6(4), 173. https://doi.org/10.5281/zenodo.1234567

[3] Chander, B., Pal, S., De, D., & Buyya, R. (2022). Artificial Intelligence-based Internet of Things for Industry 5.0. Internet of Things, 3–45. https://doi.org/10.1007/978-3-030-87059-1_1

[4] Furfaro, A., Argento, L., Parise, A., & Piccolo, A. (2017). Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. Simulation Modelling Practice and Theory, 73, 43–54. https://doi.org/10.1016/j.simpat.2016.09.007

[5] Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., & Astorga-Vargas, M. (2017). Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. Sensors, 17(6), 1379. https://doi.org/10.3390/s17061379

[6] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020(1). https://doi.org/10.1186/s13635-020-00111-0

[7] Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access, 9, 121975-121995. https://doi.org/10.1109/ACCESS.2021.3109886

[8] Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

[9] Orlova, E. V. (2021). Design of Personal Trajectories for Employees' Professional Development in the Knowledge Society under Industry 5.0. Social Sciences, 10(11), 427. MDPI. https://doi.org/10.3390/socsci10110427

[10] Y. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769560.