THE IMPACT OF EMERGING TECHNOLOGY ON CYBERSECURITY AUDIT METHODOLOGY: A LITERATURE PERSPECTIVE

[1]Rivo Juniandra Rumadi, [2]Galang Talkhis Fuady, [3]Yoga Budi Santoso, [4]Zaky Permana Putra [5]Dimas Febriawan
[1-5]Universitas Muhammadiyah Prof Dr Hamka, Jalan Tanah Merdeka 6 13830 Jakarta Timur,
[1]2203015126@uhamka.ac.id, [2]2203015141@uhamka.ac.id, [3]2203015047@uhamka.ac.id,
[4]2203015115@uhamka.ac.id, [5]dimas.febriawan@uhamka.ac.id

Abstrak

Evolusi yang cepat dari teknologi yang muncul, seperti Kecerdasan Buatan (AI), Pembelajaran Mesin (ML), Blockchain, Internet of Things (IoT), dan Digital Twins (DT), telah secara signifikan mengubah berbagai industri, termasuk lanskap keamanan siber. Meskipun teknologi ini menawarkan peluang yang belum pernah ada sebelumnya untuk efisiensi, otomatisasi, dan peningkatan kemampuan, teknologi ini secara bersamaan memperkenalkan risiko keamanan siber yang baru dan kompleks. Tinjauan literatur ini menyelidiki dampak dari teknologi yang muncul ini pada metodologi audit keamanan siber tradisional. Dengan menganalisis literatur ilmiah dan industri yang ada, makalah ini mengidentifikasi kerentanan baru dan vektor serangan yang dibawa oleh AI, ML, Blockchain, IoT, dan DT. Selain itu, makalah ini juga membahas bagaimana metodologi audit harus beradaptasi untuk menilai dan memitigasi ancaman-ancaman canggih ini secara efektif. Temuan ini menyoroti kebutuhan penting bagi auditor untuk memperoleh keterampilan baru, merangkul alat audit yang digerakkan oleh AI / ML, dan mengintegrasikan pendekatan yang lebih dinamis dan adaptif untuk memastikan keamanan siber yang kuat dalam sistem yang semakin terhubung dan cerdas.

Kata kunci: Keamanan Siber, Metodologi Audit, Teknologi yang Sedang Berkembang, Kecerdasan Buatan, Pembelajaran Mesin, Blockchain, Internet of Things, Kembaran Digital

Abstract

The rapid evolution of emerging technologies, such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Internet of Things (IoT), and Digital Twins (DTs), has significantly transformed various industries, including the landscape of cybersecurity. While these technologies offer unprecedented opportunities for efficiency, automation, and enhanced capabilities, they simultaneously introduce novel and complex cybersecurity risks. This literature review investigates the impact of these emerging technologies on traditional cybersecurity audit methodologies. By analyzing existing scholarly and industrial literature, this paper identifies the new vulnerabilities and attack vectors brought forth by AI, ML, Blockchain, IoT, and DTs. Furthermore, it explores how audit methodologies must adapt to effectively assess and mitigate these advanced threats. The

Article History:
Received: June 2025
Reviewed: July 2025
Published: July 2025

Plagirism Checker No 234
Prefix DOI :
10.8734/Kohesi.v1i2.365

findings highlight the critical need for auditors to acquire new skills, embrace AI/ML-driven audit tools, and integrate a more dynamic and adaptive approach to ensure robust cybersecurity in increasingly interconnected and intelligent systems.
Keywords: Cybersecurity, Audit Methodology, Emerging Technology, Artificial Intelligence, Machine Learning, Blockchain, Internet of Things, Digital Twin.

INTRODUCTION

The digital era is characterized by rapid technological evolution, fundamentally reshaping business processes and information systems. Emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, the Internet of Things (IoT), and Digital Twins (DTs) are transforming the cybersecurity landscape. These technologies not only enhance operational efficiency and decision-making through automation and real-time analytics but also introduce increasingly complex digital infrastructures prone to evolving cyber threats. As a result, the significance of cybersecurity audit methodologies is growing, as organizations strive to safeguard the integrity, confidentiality, and availability of their digital assets.

However, despite the increasing adoption of these technologies, traditional cybersecurity audit frameworks often fall short in addressing the dynamic and distributed nature of these new systems. Cook et al. (2009) argue that conventional auditing approaches, typically focused on predefined controls and historical compliance checks, lack the flexibility to capture real-time risk indicators and system behavior anomalies. Furthermore, the integration of operational technology (OT) with information technology (IT) further broadens the attack surface, creating vulnerabilities at the intersection of physical and digital systems. This convergence demands audit practices capable of monitoring hybrid systems with predictive and adaptive mechanisms.

Previous research has explored components of this evolving landscape, such as AI-driven threat detection (Singh et al., 2021) and blockchain-based audit trails (Zhou et al., 2020). These studies provide valuable insights into specific technologies but often do not assess their holistic impact on audit methodologies or compare cross-technology implications. There remains a gap in synthesizing these findings to inform the redesign of audit frameworks in a unified manner.

Therefore, this study aims to systematically review recent literature to examine how emerging technologies are reshaping cybersecurity audit methodologies. Specifically, it investigates the nature of new vulnerabilities introduced by these technologies and how audit practices must adapt. The central hypothesis of this study is that emerging technologies demand a shift from reactive, compliance-based audits to proactive, risk-based, and technologically integrated methodologies.

METHODS

This study employs a **systematic literature review** design to explore the evolving relationship between emerging technologies and cybersecurity audit methodologies. A structured approach was adopted to ensure comprehensive and unbiased coverage of existing research.

Step 1: Identification of Research Questions

The guiding questions for this review include:

- How do emerging technologies influence the cybersecurity audit process?
- What are the key vulnerabilities introduced by these technologies?
- How are audit methodologies evolving to address these changes?

Step 2: Database Selection and Search Strategy

Relevant academic databases such as IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar were searched using combinations of keywords, including "cybersecurity audit," "emerging technology," "AI audit," "blockchain security," and "IoT vulnerabilities." Boolean operators were used to refine the search scope.

Step 3: Inclusion and Exclusion Criteria

Articles were included if they were published between 2015 and 2024, peer-reviewed, and addressed at least one emerging technology in the context of cybersecurity audits. Articles focusing only on general cybersecurity practices without audit relevance were excluded.

Step 4: Data Extraction and Thematic Analysis

Selected articles were analyzed for key themes, such as types of audit frameworks, new risks and vulnerabilities, and proposed technological solutions for auditing. Thematic coding was applied to identify recurring patterns and gaps across studies.

Step 5: Synthesis and Reporting

Findings were synthesized and grouped based on technology type (e.g., AI, Blockchain, IoT, DTs). Each section highlights how the respective technology affects audit processes, referencing both risks and opportunities.

FINDINGS AND DISCUSSION

The review revealed several thematic insights on how emerging technologies are reshaping cybersecurity audit methodologies.

Table 1. Summary of Emerging Technologies and Their Impacts on Cybersecurity Audit

Technology	Audit Challenges	Opportunities for Audit Enhancement	Key Reference
AI & ML	Algorithmic bias, data poisoning	Predictive analytics, anomaly detection	Singh et al. (2021)
Blockchain	Immutable logs limit correction of audit errors	Tamper-proof audit trails	Zhou et al. (2020)
IoT	Device heterogeneity, scalability issues	Real-time monitoring	Patel et al. (2022)
Digital Twin	High data synchronization demands	Continuous auditing of system behaviors	Kim & Lee (2023)

Footnotes:
O = Challenge identified by multiple sources
X = Opportunity widely supported by literature

Penjelasan:

Based on Table 1, each technology brings specific challenges to the audit process. For example, in the use of AI, the main risks include algorithmic bias and manipulation of training data. However, AI also allows auditors to automatically detect anomalies through machine learning. In the case of Blockchain, its greatest strength, which is immutability, can actually become a hindrance when there are audit input errors that cannot be changed. Nevertheless, its ability to provide a transparent audit trail is very valuable for enhancing accountability.

This result shows that the traditional audit approach needs to evolve towards a more dynamic and adaptive technology-based system. Future audits should integrate real-time monitoring, predictive analytics, and risk-based evaluations to address the complexities of the modern digital ecosystem.

Cybersecurity Landscape in the Era of Emerging Technologies

The contemporary cybersecurity landscape is increasingly shaped by the integration of emerging technologies into critical infrastructures and operational environments. While these innovations—such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, the Internet of Things (IoT), and Digital Twins (DTs)—provide significant advancements in functionality, connectivity, and automation, they also introduce new and complex security threats. This section examines how each of these technologies transforms the cyber threat environment and challenges traditional audit mechanisms.

1.1. Artificial Intelligence (AI) and Machine Learning (ML)

Artificial intelligence (AI) and machine learning (ML) are now playing a crucial role in improving cybersecurity defenses by enabling automated and intelligent threat detection and response. These technologies are able to process large amounts of data in real-time, recognize complex attack patterns, and adapt to emerging threats. For example, deep learning models are increasingly being used to detect and classify cyber threats with greater accuracy and speed than traditional systems.

However, the use of AI by malicious actors in the cybercrime realm poses a heightened threat. Attackers are leveraging artificial intelligence (AI) to automate reconnaissance processes, perform vulnerability scans at scale, and create polymorphic malware that can evade common detection methods. Techniques such as data poisoning, in which training data is manipulated with malicious intent, and evasion attacks, which involve making minor alterations to inputs to confuse AI models, illustrate the vulnerabilities of contemporary AI-based security systems. These challenges necessitate not only the continual refinement of models, but also an augmented focus on enhancing interpretability, robustness, and the implementation of robust audit mechanisms to assess AI-driven decision-making processes.

1.2. Blockchain

The decentralized and tamper-resistant structure of blockchain has great potential to improve cybersecurity. With its ability to provide a clear and immutable audit trail, blockchain is an attractive option for secure data sharing, identity verification, and decentralized access management. In terms of auditing, this technology allows us to track changes in real time, verify data origin, and improve accountability.

However, blockchain is not completely immune to risk. Although the resilience or immunity of records is very useful for maintaining integrity, this can be a problem if incorrect or harmful data is entered, because that data cannot be changed or deleted. Additionally, centralized control in private or consortium blockchains can create vulnerabilities similar to those found in traditional systems. A 51% attack, where a single entity controls the majority of the network, also poses a serious threat. Other issues such as interoperability, regulatory

uncertainty, and scalability limitations further complicate the implementation of blockchain in the context of cybersecurity audits.

1.3. Internet of Things (IoT)

The widespread deployment of Internet of Things (IoT) devices has changed the way we collect data and connect systems, but it has also created a fragmented and highly vulnerable security environment. Many IoT devices are deployed with weak security settings, without adequate authentication, encrypted communications, or mechanisms to update firmware. As a result, these devices often become openings for cyberattacks.

Notable attacks, such as the Mirai botnet, illustrate the vulnerability of IoT devices to being weaponized for Distributed Denial of Service (DDoS) attacks. The proliferation of devices and platforms introduces a multifaceted landscape, complicating the implementation of uniform security policies and the standardization of audits. The IoT ecosystem provides a conducive environment for social engineering, physical tampering, and insider threats. These issues necessitate enhanced audit protocols that can scale across heterogeneous environments and identify hidden interdependencies among connected assets.

1.4. Digital Twins (DTs)

Digital Twins, which serve as real-time virtual representations of physical systems, are at the heart of Industry 4.0. They provide tremendous capabilities in predictive analytics and system optimization. However, because they have two sides—digital and physical—this also poses serious security challenges in both domains.

Digital Twins (DTs) face several significant risks. A primary concern is data integrity attacks, where tampering with incoming or outgoing data can cripple the system. There are also surveillance attacks, where adversaries gather information about a DT's structure to launch more targeted disruptions. Beyond these, new threats are emerging, such as simulation-based exploitation, where attackers model system responses to pinpoint vulnerabilities. Other dangers like malware injection, intellectual property theft, and operational sabotage can occur at various stages of a DT's lifecycle. To combat these challenges, a thorough security audit is essential. This audit needs to cover both the cyber and physical aspects of the digital twin system to guarantee data authenticity, real-time system validation, and secure decommissioning processes.

IMPACT ON CYBERSECURITY AUDIT METHODOLOGY

The rapid growth of new technologies, along with the unique cyber threats they bring, calls for a major shift in how we approach cybersecurity audits. Traditional methods often aren’t enough to keep up with the complexity and constantly changing nature of systems like AI, machine learning, blockchain, IoT, and digital twins.

Challenges for Traditional Audit Methodologies

As technology evolves, especially with the rise of AI, IoT, and digital twin systems, the limitations of traditional cybersecurity audits are becoming more apparent.

- Lack of Standardization: One of the biggest issues is the absence of clear and widely accepted standards. In fast-moving areas like IoT and digital twins, security frameworks are either still being developed or vary too much across platforms. This makes it hard for auditors to assess these systems using a consistent set of rules, leading to gaps or inconsistencies in evaluations.
- Complexity and Opacity: When it comes to auditing AI or machine learning systems especially deep learning things get a bit tricky. These models can be incredibly detailed and, at times, difficult to follow. Honestly, even developers don’t always know exactly why the model made a certain decision. That makes it pretty hard for auditors to step in and say whether the system is doing what it should. If you can’t clearly see what’s happening inside, then checking for problems like bias or security risks becomes guesswork, which obviously isn’t ideal.

- Data Volume and Velocity: Let's face it systems like IoT and digital twins produce a lot of data, and they do it really fast. It's honestly way too much for anyone to go through manually. Traditional audit methods just weren't built for that kind of speed or scale. Unless you have tools that can keep up smart ones that can spot problems automatically you're probably going to miss something important.
- Dynamic Threat Landscape: To be honest, one of the hardest things with all these new technologies is just how fast the threats keep changing. Like, you think you've patched one thing, and the next week there's some new zero day vulnerability nobody saw coming. The usual audits those that happen maybe once a quarter or so can't really keep up with that. By the time they run, the threat landscape might already be different. It's kind of like chasing something that's always two steps ahead.
- Interoperability and Heterogeneity: IoT and digital twin systems are made up of all kinds of devices, software, and communication methods, often from different vendors. This mix creates a complex environment where everything doesn't always "speak the same language." Trying to assess security across such a varied setup isn't easy. Making sure all the parts work together safely is one of the bigger challenges auditors face.
- Trust and Liability: In systems like blockchain or federated learning, where many different parties are involved, building trust between everyone isn't always straightforward. If something goes wrong like a data breach or tampering it's often unclear who should be held responsible. Figuring out how to manage these issues makes the auditing process much more complicated.

Evolution of Audit Methodologies

In order to tackle these challenges, cybersecurity audit methodologies need to adapt by integrating innovative approaches and tools:

- AI/ML-Driven Audit Tools: Auditors need to leverage AI and ML capabilities to enhance their own audit processes. This involves leveraging AI for the automation of log analysis, detecting anomalies in network traffic, employing predictive analytics to uncover emerging threats, and utilizing advanced vulnerability scanning techniques across extensive datasets. AI has the potential to greatly minimize false positives while enhancing both the speed and precision of threat detection.
- Instead of relying only on periodic audits, there's a growing need to shift toward continuous and more adaptive audit approaches. This means building in real-time monitoring and assessment tools that can keep up with fast-changing systems. For example, audit functions can be embedded directly into CI/CD pipelines during software development, allowing checks to happen as code is released. In some cases, pulling data directly from IoT devices or even digital twins might help, especially when trying to figure out what's going on inside the system at a certain point in time. But of course, things don't stay the same for long, threats change, sometimes unpredictably so it really wouldn't make sense to keep the audit parameters static. They should be able to change too, or at least be reviewed regularly, otherwise they'll fall behind and miss critical issues.
- Attacks such as data poisoning or the injection of false information are becoming a real concern, especially when large amounts of data are being processed automatically. Because of that, audits should not only look at how data is used but also where it came from and whether it has been changed along the way. Making sure that data is accurate and understanding where it comes from is becoming more important in audit practices. Rather than focusing only on the final results, it is also necessary to consider how the data was collected, transferred, and processed. Some researchers have begun exploring the use of blockchain as a possible solution. This technology can help maintain records that are difficult to modify and may provide a clearer view of how the data has been handled over time.

- In many cases, just looking for known patterns or threats is no longer enough. Auditors need to start paying more attention to how systems behave in real situations. That includes trying to understand what is considered normal activity, whether it is from an AI model, a connected device, or a digital twin. Once that normal behavior is understood, it becomes easier to notice when something unusual happens. If a system starts acting differently without a clear reason, that could be a sign that something is going wrong and should probably be checked.
- Sometimes, with AI or machine learning systems, it is just not clear why they make certain choices. For people doing audits, this can be a real issue because it's hard to explain what the system is doing or why. That's where some methods called explainable AI come in. They are meant to help make those decisions a bit easier to follow. If you can understand how the system came to a decision, then it is also easier to tell if something seems off or if there might be mistakes in how the model works.
- Simulation and Digital Twin-Based Audits: Using digital twins for cybersecurity audits gives auditors a safe space to test things out—like simulating cyberattacks or checking how well a system can handle a threat—without putting the real system at risk. This kind of setup, often called a "cyber range," lets teams run penetration tests, try out their incident response plans, and see how effective their security measures really are, all in a realistic but completely controlled environment.
- Interdisciplinary Skills and Collaboration: These days, auditors can't just stick to traditional IT knowledge. With tech like AI, blockchain, and industrial control systems becoming more common, they really need to pick up new skills to keep up. But even with that, no one can handle it all alone. That's why working closely with data scientists, AI engineers, and people who know the specific field inside-out has become super important. Without that kind of teamwork, it's tough to build audit strategies that actually make sense in real-world situations.

CONCLUSION

The rise of new technologies has changed the way we think about cybersecurity. While tools like AI, machine learning, blockchain, IoT, and digital twins offer major improvements in efficiency, they also introduce more complex and unpredictable risks. Based on recent studies, it's clear that traditional cybersecurity audits are no longer enough. These technologies handle vast and often sensitive data, operate through intricate processes, and are exposed to threats that keep changing over time. What makes things more challenging is the absence of consistent standards to guide how security should be managed. Given these factors, it's no longer practical to rely on traditional audit methods cybersecurity practices must evolve to keep pace with the systems they're meant to protect.

Audit methods are definitely shifting lately, and there's growing awareness that AI and machine learning might actually be quite useful for spotting and making sense of cybersecurity threats. But adopting these tools isn't just a matter of plugging in new software it's also about changing how audits are done overall. So, audits might need to be more flexible maybe even ongoing, depending on the situation. Even so, we shouldn't lose sight of the basics. It's important to double-check that the data we're using is solid and that we actually know where it came from. Another issue is that a lot of AI models are pretty hard to interpret they don't always show how they arrive at their conclusions. That's where Explainable AI, or XAI, comes in. It helps people actually understand the logic behind what the system is doing, especially when the process is hidden or complex. Then there's Digital Twin tech, which offers a safe way to run simulations and test systems for weaknesses basically letting us experiment without breaking anything real. All of this, though, depends on people working together. It's not just about auditors it takes cooperation between them, tech developers, and people who really

know the subject matter, because without that kind of teamwork, dealing with all this digital complexity would be way harder.

For future work, research should focus on:

- The development of standardized and comprehensive audit frameworks designed specifically to address the distinctive security requirements of integrated IT/OT environments - including AI, ML, Blockchain, IoT, and Digital Twins - represents a critical need in modern cybersecurity practice.
- Creating open-source, real-world datasets for emerging technology vulnerabilities and attacks to facilitate the development and benchmarking of new audit tools and methodologies.
- Exploring the ethical implications of AI-driven audits, particularly concerning privacy, algorithmic bias, and the accountability of automated security decisions.
- Investigating the integration of quantum-safe cryptography into audit practices to prepare for future threats posed by quantum computing.
- Designing mechanisms for real-time, automated policy enforcement and compliance checking within highly dynamic IoT and Digital Twin environments, moving towards "security by design" rather than reactive measures.

This literature review points out that standard cybersecurity audit methodologies are insufficient for tackling the intricate and dynamic features of systems involving AI, ML, Blockchain, IoT, Digital Twins and ohters in the digital future.

DAFTAR PUSTAKA

Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in fintech. *Iraqi Journal for Computer Science and Mathematics*, *5*(3). https://doi.org/10.52866/ijcsm.2024.05.03.004

Canonico, R., & Sperlì, G. (2023). Industrial cyber-physical systems protection: A methodological review. *Computers & Security*, *135*, 103531. https://doi.org/10.1016/j.cose.2023.103531

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access*, *9*, 7152–7169. https://doi.org/10.1109/access.2020.3048839

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*, *57*(8). https://doi.org/10.1007/s10462-024-10805-3

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys*, *54*(11s), 1–35. https://doi.org/10.1145/3510410

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, *170*, 108036. https://doi.org/10.1016/j.compbiomed.2024.108036

Qawasmeh, S. A.-D., AlQahtani, A. A. S., & Khan, M. K. (2025). Navigating cybersecurity training: A comprehensive review. *Computers and Electrical Engineering*, *123*, 110097. https://doi.org/10.1016/j.compeleceng.2025.110097

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., & Santos, O. (2021). Artificial intelligence and the internet of things in industry 4.0. *CCF Transactions on Pervasive Computing and Interaction*, *3*(3), 329–338. https://doi.org/10.1007/s42486-021-00057-3

Ramos-Cruz, B., Andreu-Perez, J., & Martínez, L. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. *Neurocomputing*, *581*, 127427. https://doi.org/10.1016/j.neucom.2024.127427

Ribas Monteiro, L. F., Rodrigues, Y. R., & Zambroni de Souza, A. C. (2023). Cybersecurity in cyber–physical power systems. *Energies*, *16*(12), 4556. https://doi.org/10.3390/en16124556

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00957-y

Sedar, R., Kalalas, C., Vazquez-Gallego, F., Alonso, L., & Alonso-Zarate, J. (2023). A comprehensive survey of V2X cybersecurity mechanisms and future research paths. *IEEE Open Journal of the Communications Society*, *4*, 325–391. https://doi.org/10.1109/ojcoms.2023.3239115

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies*, *13*(10), 2509. https://doi.org/10.3390/en13102509

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. (2023). *Iraqi Journal for Computer Science and Mathematics*, 87–101. https://doi.org/10.52866/ijcsm.2023.01.01.008

Umer, M. A., Belay, E. G., & Gouveia, L. B. (2024). Fortifying Industry 4.0: Internet of things security in cloud manufacturing through artificial intelligence and provenance blockchain—a thematic literature review. *Sci*, *6*(3), 51. https://doi.org/10.3390/sci6030051

Pethő, Z., Török, Á., & Szalay, Z. (2021). A survey of new orientations in the field of vehicular cybersecurity, applying artificial intelligence based methods. *Transactions on Emerging Telecommunications Technologies*, *32*(10). https://doi.org/10.1002/ett.4325