OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X

Vol. 2. No. 2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i2.298
Available : : https://jurnalhafasy.com/index.php/oikonomia

Digital Economic Revolution: The Role of Internet of Things (IoT) And Artificial Intelligence (AI) in Business Management and Accounting

Muhammad Umar A
Universitas Alkhairaat Palu, Indonesia

Received: January 13, 2025
Revised: January 28, 2025
Accepted: February 02, 2025
Published: February 07, 2025

Corresponding Author:
Author Name*: Muhammad Umar A
Email*: m.umar@unisapalu.ac.id

***Abstrak*:** *The digital economic revolution has changed the global business paradigm by integrating Internet of Things (IoT) and Artificial Intelligence (AI) technologies in company operations. IoT enables connectivity between devices that generate real-time data, while AI analyzes the data to improve decision-making. The implementation of these technologies improves operational efficiency, reduces human error, and accelerates business cycles. However, challenges such as data security, unequal access to technology, and the need to improve workforce competencies are still major obstacles. In accounting and business management, AI and IoT have accelerated the digitization of financial records, data analysis, and risk management. AI with machine learning algorithms can detect suspicious financial patterns and improve the accuracy of financial predictions, while IoT supports supply chain efficiency and asset management. However, the adoption of these technologies requires substantial financial investment as well as regulatory and company policy readiness. In addition, challenges in cybersecurity and digital skills gaps demand comprehensive mitigation strategies. Therefore, collaboration between companies, educational institutions and the public sector is crucial in ensuring the success of sustainable and ethical digital transformation. With the right strategy, companies can optimize AI and IoT to increase competitiveness in the digital era*

***Keywords* :** *Accounting; Artificial Intelligence; Business Management; Digital Economic Revolution; Internet Of Things*

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

INTRODUCTION

The digital economic revolution has become a key pillar in global business transformation, where technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) play a role in changing the operational paradigm of companies. This development is driven by the increasing need for efficiency, transparency, and automation in various aspects of business, including management and accounting. IoT enables connectivity between devices that generate real-time data, which is then processed by AI to improve the quality of decision making. According to a report by Norliani et al (2024), the adoption of digital technology can increase operational efficiency by 40%, reduce human error, and accelerate business cycles through process automation. However, on the other hand, this over-reliance on technology also poses challenges, such as data security, inequality in access to technology, and the need to improve workforce competencies in order to adapt to digital-based systems.

In the context of accounting and business management, AI and IoT have accelerated the digitization of financial recording systems, data analysis, and risk management. AI with machine learning algorithms can detect suspicious financial patterns, reduce the possibility of fraud, and improve the accuracy of company financial predictions. IoT, on the other hand, plays a role in improving supply chain efficiency and asset management by providing more accurate and transparent operational data. According to a report by Abdullah & Almaqtari (2024), companies that adopt AI and IoT in their business management and accounting systems experience a 30% increase in financial statement accuracy and a 25% reduction in operational costs. However, the adoption of these technologies requires not only large financial investments, but also regulatory readiness and company policies to ensure that technology integration remains in accordance with applicable ethical and legal standards.

The utilization of the Internet of Things (IoT) in the business world has opened up new opportunities in asset management and real-time operational monitoring. IoT enables the integration of sensors, smart devices, and cloud-based systems to collect and analyze large amounts of data (Prawiyogi & Anwar, 2023). In the context of business management, this technology provides greater visibility into a company's supply chain and operations, enabling optimization of resource use. For example, manufacturing companies can use IoT sensors to monitor machine conditions and identify potential malfunctions before they occur, which can reduce production downtime and improve operational efficiency. A study conducted by Pranata & Ichsan (2024) showed that companies that implemented IoT in their operations experienced increased efficiency while reducing maintenance costs. However, behind these benefits, IoT deployment also faces serious challenges, especially in terms of cybersecurity and data privacy. Attacks on IoT infrastructure can lead to sensitive information leakage, which risks destabilizing businesses and lowering customer trust.

In the world of accounting, IoT has a significant impact on the accuracy of transaction recording and stock management. Retail companies, for example, can adopt IoT-based systems to track the movement of goods in the warehouse, reducing the risk of errors in inventory recording. Data obtained from IoT sensors can be automatically connected to Enterprise Resource Planning (ERP) systems or cloud-based accounting software, enabling more transparent and accurate financial records. A research report by Panjaitan & Firdaus (2024) revealed that the use of IoT in accounting systems can reduce recording errors by 30% and speed up the company's internal audit process. However, the adoption of IoT in the accounting sector also raises dilemmas related to data protection and compliance with regulations, such as the General Data Protection Regulation (GDPR) in Europe or the Personal Data Protection Law (UU PDP) in Indonesia.

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

Therefore, companies looking to integrate IoT in their management and accounting systems need to ensure risk mitigation measures are in place, such as the implementation of data encryption, layered authentication systems, and compliance with global security standards.

The utilization of Artificial Intelligence (AI) in business and accounting has become a key factor in improving operational efficiency and decision-making accuracy. With machine learning algorithms and predictive analytics, AI can process large amounts of data to identify financial trends and predict potential business risks more accurately than traditional methods. In accounting systems, AI can automate transaction recording, perform financial reconciliation, and detect anomalies that could potentially indicate fraud. Damayanti's (2025) report shows that companies that adopt AI in the accounting process experience an increase in efficiency of up to 40% and a decrease in human error by 25%. However, although AI can improve the accuracy of financial statements, the reliability of AI models is highly dependent on the quality of the data used. If the inputted data has biases or imbalances, then AI may produce inaccurate outputs, which risks leading to wrong business decisions.

On the other hand, the application of AI in business management also presents ethical and regulatory challenges. AI-driven automation may replace work previously done by humans, creating concerns regarding labor reduction in the accounting and finance sectors. A study by Jha et al (2021) suggests that while AI can increase company productivity, around 15% of accounting and finance jobs are at risk of being disrupted in the next 5-10 years due to AI-based automation. Therefore, the role of humans is still needed in the strategic decision-making process, especially in interpreting data generated by AI. In addition, regulations related to accountability and transparency of AI systems are a major concern, especially in ensuring that the algorithms used are unbiased and auditable. Therefore, companies need to implement a human-in-the-loop approach, where AI serves as a tool for humans rather than a full replacement, to maintain a balance between technological efficiency and responsible business ethics.

One of the key challenges in the adoption of the Internet of Things (IoT) and Artificial Intelligence (AI) in business and accounting is data security and privacy. As more and more IoT devices are connected to corporate networks, the risk of cyberattacks and information leakage increases. AI that relies on large amounts of data is also vulnerable to exploitation if not properly protected. According to a report by Cybersecurity Ventures (2023), cyberattacks against IoT-based systems increased by 300% in the past five years, indicating that without a strong security strategy, companies could face huge losses, both financially and reputationally. In addition, non-uniform regulations related to data protection in various countries are also an obstacle for multinational companies in implementing AI and IoT optimally. Therefore, companies need to invest in cybersecurity, such as data encryption, layered authentication systems, and compliance with regulations such as GDPR in Europe or the PDP Law in Indonesia, to ensure that customer data and financial transactions remain secure.

In addition to security challenges, the readiness of human resources (HR) is also a key factor in the successful implementation of this technology. AI and IoT require a workforce that is not only tech-savvy, but also has the skills to analyze and interpret data generated by intelligent systems. Unfortunately, the digital skills gap is still a problem in many companies, especially in developing countries. A study from the World Economic Forum (2023) in Francisco & Linner (2023) states that only 30% of the global workforce has sufficient digital skills to work with AI and IoT-based systems, so companies must invest in training and reskilling employees in order to adapt to an increasingly digitized business ecosystem. Without adequate HR readiness, companies risk becoming dependent on technology vendors or

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

third parties, which can increase operational costs and reduce flexibility in data management. Therefore, the best strategy is to combine investment in technology with HR development so that the adoption of AI and IoT can be sustainable and have a positive impact on business in the long run.

METHOD

This research uses a qualitative approach with a case study method to explore the role of the Internet of Things (IoT) and Artificial Intelligence (AI) in business management and accounting. The study was conducted on three companies from the manufacturing, retail, and financial sectors that have adopted these technologies. Data was obtained through in-depth interviews with six respondents (two finance managers, two data analysts, and two operations managers), as well as direct observation of AI and IoT implementation. Secondary sources included industry reports and academic journals from research institutions such as McKinsey, Deloitte, and PwC.

Data analysis was conducted using thematic analysis methods, including data reduction, data presentation, and conclusion drawing, with a focus on operational efficiency, accounting automation, data security, and HR readiness. Data validity was maintained through source and method triangulation, by comparing the results of interviews, observations, and documentation studies. With this approach, the research is expected to provide in-depth insights into the impacts and challenges of AI and IoT implementation in business and accounting in the digital era.

RESULTS AND DISCUSSION

Digital Transformation in Business Management and Accounting: Optimization with AI and IoT

A. Automation and Efficiency in Accounting through AI

Automation and efficiency in accounting through artificial intelligence (AI) is a major transformation that changes the traditional way of recording and processing financial data. In today's digital age, many companies are turning to advanced technologies to increase productivity, reduce costs, and improve accuracy in financial reporting. AI, with the sophistication of machine learning algorithms and big data analysis, enables the automation of various accounting tasks, such as transaction recording, data reconciliation, and real-time financial report analysis. One of the most significant impacts of AI in accounting is its ability to reduce human error. Previously, recording financial transactions often required high precision and was prone to errors that could be fatal. With AI, this process becomes faster, more accurate, and more efficient, given the ability of AI systems to detect patterns and analyze data in greater depth than humans can in a short period of time. For example, research conducted by Sriningsih et al (2025) showed that companies that implemented AI technology in the audit process experienced a 40% increase in efficiency, with a significant reduction in administrative costs. This shows how AI is not just a tool, but a key element in modernizing accounting practices in many global companies.

Furthermore, the use of AI in financial statement analysis has a tremendous impact in terms of understanding a company's financial condition. AI allows financial

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

analysts to process and analyze large volumes of data at a speed unmatched by human capabilities. In a study conducted by Sunaryo et al (2024), it was found that the application of AI in financial analysis helps companies gain more accurate and faster insights into cash flow, earnings, and potential risks faced. This technology not only helps in detecting anomalies or recording errors, but also facilitates better financial forecasting or prediction. AI uses deep learning techniques and predictive algorithms to provide strategic recommendations that can improve a company's financial performance. For example, companies can use AI predictive models to plan future cash flows, identify potential revenue declines, or find new, more profitable investment opportunities, all based on historical data carefully analyzed by AI.

However, while AI brings efficiency and automation, challenges in its application cannot be ignored. One of them is the need to ensure the integrity and security of the data used in AI systems. Financial data processed by AI must be highly protected, given the potential risk of data leakage that could damage the company's reputation and jeopardize the financial security of their clients. In this regard, research by Lestari et al (2024) revealed that one of the biggest challenges in implementing AI in the accounting sector is the issue of cybersecurity. Data security is very important, considering that the information processed is very sensitive and prone to being the target of attacks from outside parties. Therefore, companies must ensure that the technology used in managing AI-based financial data is equipped with an adequate protection system, including data encryption and a transparent audit trail.

In addition, the adoption of AI in accounting also requires changes in organizational structure and human resource (HR) skills. According to a study by Judijanto (2024), although AI can automate many accounting tasks, companies still need a workforce that has the ability to understand and manage this technology effectively. This creates a need for continuous training and digital skills development among accounting professionals, so that they can function well in an environment that is increasingly dominated by technology. AI is not about completely replacing human work, but rather a collaboration between humans and machines, where accounting professionals still play an important role in data interpretation and strategic decision-making.

Based on a number of studies and experiments that have been conducted, it can be concluded that the application of AI in accounting provides many benefits, including reduced costs, improved accuracy, and significant time savings. For example, a study by Raihan (2024) found that companies that adopted AI-based automation experienced improvements in operational efficiency and customer satisfaction due to a reduction in the time required for administrative processes. AI also enables companies to more quickly respond to changes in market conditions by providing more precise and faster insights into their financial state. While challenges related to data security and changes in HR skills need to be addressed, the benefits derived from the automation and efficiency offered by AI make it a worthwhile investment for companies looking to remain competitive in an increasingly digitized global market.

Overall, it can be said that the implementation of AI in accounting brings about a profound paradigm shift. Not only does AI offer automation solutions for administrative tasks, but it also introduces

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

new possibilities in financial analysis and strategic planning. With the support of existing research, this technology is proven to bring tremendous efficiency improvements, but it still requires serious attention to security aspects and HR readiness to utilize the full potential of AI in the future.

B. The Role of IoT in Optimizing Operational and Supply Chain Management

The role of the Internet of Things (IoT) in optimizing operational and supply chain management has become one of the key factors driving digital transformation in various industries. IoT, which connects physical devices through sensors and communication devices, enables real-time monitoring and management of assets and production processes (Prawiyogi & Anwar, 2023; Trista, 2022). Thus, this technology not only improves operational efficiency, but also reduces costs and improves accuracy in data-driven decision-making. One of the key benefits of IoT in operations management is its ability to provide highly accurate and up-to-date data, which is essential in strategic planning and decision-making. In the context of the supply chain, IoT enables the monitoring and management of goods inventory with a higher degree of accuracy, thereby reducing the recording errors that often occur in traditional systems that rely on manual input. Research conducted by Oktavia (2023) shows that the application of IoT-based sensor technology in warehouses can reduce the error rate in inventory by up to 30%. This technology also enables more efficient management of the distribution of goods by minimizing delivery delays and maximizing delivery routes through the analysis of data obtained from IoT systems. Through the real-time data collected, companies can make adjustments in a short period of time to production and delivery planning. This is especially relevant in the manufacturing sector, where an efficient supply chain is a key factor in maintaining smooth production and delivery of goods to customers.

In addition, IoT enables proactive monitoring of the operational condition of machines and equipment through sensors attached to critical assets. With real-time data on the condition of assets, companies can carry out preventive maintenance that reduces the likelihood of damage or failure that can stop operations. Research by Priyatna (2024) revealed that by utilizing IoT for machine condition monitoring, companies can reduce downtime by up to 20% and improve production efficiency. By minimizing downtime, companies can not only save on maintenance costs, but also increase their throughput and competitiveness in an increasingly competitive market.

The utilization of IoT in supply chain management is not only limited to the physical monitoring of goods, but also includes the collection of data from various points in the value chain. In a study conducted by Respati & Sukmadewi (2024), the application of IoT technology in supply chain management systems can reduce the delivery time of goods by up to 15%, because companies can access real-time data on transportation and logistics conditions. This information allows supply chain managers to adjust delivery routes or schedules according to field conditions, such as congestion or bad weather, ultimately reducing delays and improving customer satisfaction. In addition, IoT also enables smarter, data-driven decision-making. With big data analysis generated from IoT devices, companies can conduct predictive analysis to forecast product demand, identify market trends, and plan

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

production and delivery more effectively. This can improve planning accuracy and reduce the risk of understocking, which can adversely affect a company's profitability.

However, while the implementation of IoT brings many benefits, there are also challenges to be aware of. One of the main challenges is related to data security and privacy. IoT collects large amounts of data that can include sensitive information related to company and customer operations. Therefore, IoT deployments must be accompanied by a robust cybersecurity strategy to protect data from potential cyber threats. Research by Faizal et al. (2023) revealed that although many companies have adopted IoT in their operations, they are often exposed to the risk of data leakage due to a lack of adequate security systems. Therefore, it is important for companies to integrate encryption technologies, strong authentication, and surveillance of connected IoT devices to ensure that the collected data remains secure.

Overall, the role of IoT in operational and supply chain management is growing and becoming increasingly important in improving operational efficiency and accuracy. This technology has been proven to make a significant contribution to improving company performance, reducing costs, and making data-driven decision-making easier. Nonetheless, its implementation requires special attention related to data security and privacy issues. With the right approach, IoT can be a key enabler in creating a more efficient, responsive, and integrated supply chain, ultimately providing a sustainable competitive advantage for companies.

C. Barriers to AI and IoT Implementation: Cost, Regulation, and Technology Dependency

The implementation of Artificial Intelligence (AI) and Internet of Things (IoT) technologies has revolutionized various industrial sectors, providing great opportunities in improving efficiency and innovation. However, despite its great potential, the process of adopting this technology is not separated from various challenges, most of which come from the aspects of cost, regulation, and dependence on technology vendors. One of the biggest obstacles in the implementation of AI and IoT is the cost of procurement and implementation. Companies must invest significant resources to purchase IoT hardware, develop and implement AI algorithms, and ensure integration with existing systems. Research conducted by Achadiyah. (2019) mentioned that the high cost in the early stages of implementation is one of the reasons why many companies, especially MSMEs, are reluctant to adopt this technology. IoT devices require expensive sensors and infrastructure, while effective AI development requires technical expertise as well as adequate investment in data training and machine learning. In addition, integrating new systems with existing infrastructure also requires significant costs, which can burden many companies with limited budgets.

In addition, regulations that are not yet fully clear are also a significant obstacle to the adoption of AI and IoT. The collection and processing of data generated by IoT devices must comply with strict personal data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. Without a clear regulatory framework, companies can face difficulties in managing and securing

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

data, putting them at risk of privacy violations. Research by Syahfitri et al (2025) highlights that these immature regulations often hinder innovation and slow down the adoption of AI and IoT technologies. On the other hand, the application of AI technology also raises complex ethical issues, such as non-transparent decisions and algorithmic bias. In this case, the company needs to have a clear policy to ensure that the use of this technology is carried out in a fair way and does not harm any party. Nasman et al (2024) in their research suggest the need for stricter ethical guidelines to regulate the use of AI to prioritize fairness, transparency, and accountability in every process carried out.

In addition to cost and regulatory challenges, reliance on technology vendors is also one of the main obstacles affecting companies' flexibility in adopting AI and IoT technologies. Many companies are stuck in reliance on solution providers that bring together their IoT devices and AI platforms in a single package, which often limits the options and ability to innovate further. Abos (2019) states that this reliance on one vendor can cause interoperability issues between devices, as well as increase the risk of vendor lock-in, where it is difficult for companies to switch to other technology providers without incurring high costs or operational losses. This can be very detrimental in the long run, especially if the technology provided by the vendor is no longer evolving according to the company's needs. The research of Erwin et al. (2023) also shows that interoperability and flexibility in choosing vendors are essential to prevent companies from getting caught up in situations where they only rely on one specific technology.

In overcoming these barriers, companies need to develop a mature and evidence-based strategy. One approach that can be done is to adopt technology gradually. Instead of directly investing large funds to implement AI and IoT across the board, companies can start with smaller pilot projects, measure the results and impact obtained, and then develop them as progress and learning from the initial project are achieved. This approach has been shown to be effective in mitigating the risks associated with high costs, as revealed in the Adha study (2020), which showed that companies that start with small-scale implementations are more likely to succeed in the technology transition than those that immediately adopt technology on a large scale without mature readiness. In addition, companies also need to develop internal policies that support compliance with applicable regulations, as well as create a risk management system to deal with potential issues related to ethics and data security.

To reduce reliance on a single vendor, companies can choose a solution provider that enables cross-platform integration and ensures interoperability between systems. This not only increases flexibility in the long run, but also allows companies to adjust and update their technology according to changing market needs and technological developments. Firdaus & Kuswinamo (2024) revealed that companies that choose open platform-based solutions tend to have an advantage in terms of flexibility and adaptability to technological changes.

Thus, despite the significant barriers to AI and IoT adoption, through the right approach and a deep understanding of these challenges, companies can mitigate these risks and reap the long-term benefits of these technologies.

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

Challenges and Risks of AI and IoT Implementation in Business: Data Security and HR Readiness

A. Data Security Risks in IoT and AI Systems

Data security in IoT (Internet of Things) and AI (Artificial Intelligence) systems has become one of the most pressing issues in this digital era, as the number of devices connected to the internet increases. IoT, which allows physical devices to communicate with each other over a network, provides convenience in managing data in real-time, but also opens up many loopholes for larger security threats. Research by Cybersecurity Ventures (2023) reveals that attacks on IoT-based systems have increased by 300% in the last five years, reflecting an increase in threats to sensitive data and information stored and exchanged between devices. The security of data contained in IoT devices and AI ecosystems has become more critical due to its nature, which often contains personal data and critical data that is highly vulnerable to leakage or manipulation. In this context, more and more IoT devices are operating without adequate security protocols, increasing the number of weak points that can be exploited by irresponsible parties. In addition, devices that are constantly connected to a central system have a huge risk of cyberattacks, where unauthorized access to personal data or company information can occur at any time.

In response to this threat, many data security experts and practitioners have proposed the need to implement data encryption and layered authentication systems as an effective solution to maintain data integrity and confidentiality. End-to-end encryption is becoming a key strategy for protecting data in transit, especially among interconnected IoT devices. By encrypting data, even if it is successfully accessed by unauthorized parties, it remains unreadable without a valid decryption key. Research conducted by Kurniati (2024) on security architecture for IoT, emphasizes that encryption is one of the fundamental security layers in IoT-based systems. A layered authentication system is also needed, which not only relies on simple passwords but incorporates stronger identification methods, such as biometrics and authentication tokens. This multi-factor authentication can ensure that only legitimate users and devices have access to sensitive information, preventing potential data leaks or manipulation.

On the other hand, while encryption and authentication can provide strong protection, they are not a perfect solution, given the increasingly sophisticated threats in the digital world. Therefore, it is important to keep security policies updated by implementing regular software updates and ensuring that the IoT devices used do not have vulnerabilities, such as easy-to-guess default passwords or software loopholes that have not been fixed. Research by Neshenko et al. (2019) revealed that most IoT devices available in the market do not come with automatic security updates, thus adding to their vulnerability to attacks. In this case, strict security policies and continuous network monitoring are key to detecting threats early before they cause greater damage. Therefore, companies and organizations need to invest not only in security devices but also in sophisticated monitoring systems to detect suspicious activity in their IoT networks.

Furthermore, the existence of AI in the IoT ecosystem also adds a layer of complexity to this security problem. AI can help detect and analyze cyber threats more quickly and accurately, using machine

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

learning techniques to analyze data traffic patterns and detect anomalies that could indicate potential attacks. However, AI itself is not immune to attacks, such as adversarial attacks aimed at corrupting algorithms or providing incorrect inputs to mislead AI decisions. Research by Meneghello et al. (2019) shows that machine learning algorithms used in AI can be affected by adversarial attacks, where data injected into AI systems can lead to incorrect or inaccurate decisions. This creates new challenges in maintaining the reliability and integrity of systems that rely on AI for security. Therefore, in addition to strengthening defenses against attacks on IoT devices and networks, steps must also be taken to protect and secure the AI system itself, so as not to become a point of weakness in the larger system.

In the face of these challenges, companies and organizations are expected to focus not only on technical measures, but also on stricter regulatory policies in managing and protecting data obtained from IoT devices. Clear and systematic cybersecurity policies are indispensable to create a safer environment for IoT and AI development and adoption. Human resources must also be provided with adequate training related to possible security threats and how to mitigate them. Collaboration between the public and private sectors in creating better security policies and standards will provide a clear direction for companies in ensuring their IoT and AI systems are secure and reliable. As explained by Makhdoom et al. (2018), the importance of collaboration between the technology sector and regulators to create security standards that can be followed globally, as threats to IoT and AI systems are cross-border and require comprehensive solutions.

Overall, data security issues in IoT and AI systems require a holistic approach, which includes the development of stronger encryption and authentication technologies, as well as the use of AI in detecting threats more effectively. Ongoing research and development, along with stricter policies and collaboration between relevant sectors, will be crucial to ensure that potential attacks on IoT devices can be minimized, and the resulting data remains well protected.

B. Human Resource Readiness in Facing Digital Transformation

The readiness of human resources (HR) in facing digital transformation is a very crucial challenge in the context of implementing new technology, especially in the industrial world which is increasingly influenced by advanced technology such as Artificial Intelligence (AI) and the Internet of Things (IoT). While AI and IoT offer significant opportunities to improve efficiency and innovation in business operations, the reality is that many companies face difficulties in optimizing the potential of these technologies due to the skills gap among the workforce. Recent data shows that only about 30% of the global workforce has sufficient digital skills to work with this technology, which means that most employees are not yet ready to face the challenges brought by digital transformation (World Economic Forum, 2020). Another study conducted by Laelawati (2024) also highlighted that the lack of digital skills is one of the biggest barriers to the adoption of advanced technologies in the industrial sector.

For this reason, it is important for companies to not only invest in the latest hardware and software, but also prioritize efforts to improve their HR competencies

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

through training and reskilling. This employee reskilling focuses on developing new skills required in the digital world, which will allow the workforce to adapt to technological changes. In this context, training that includes skills in data analysis, AI-based system management, and an understanding of IoT applications is essential. As AI and IoT evolve, companies need to prepare human resources who are not only able to operate these technologies but can also leverage them to generate better business insights. Data analysis, for example, is an increasingly needed skill, because IoT technology generates a huge volume of data that needs to be analyzed to add value to business processes (Fauziyyah, 2022). Through training that focuses on data collection, cleaning, analysis, and interpretation, employees can improve their ability to identify patterns and trends that will aid in faster and more accurate decision-making.

In addition, understanding AI-based system management is also one of the important aspects in human resource readiness to face digital transformation. According to a report from Raza & Komala (2020), AI is predicted to affect almost every aspect of a company's operations, from manufacturing to customer service. With the increasing use of AI technology, employees need to understand how to manage and optimize AI-based systems in their day-to-day operations, such as the application of machine learning in product demand prediction or supply chain management. Research conducted by Ramdhan & Aripin (2024) shows that companies that are able to utilize AI to improve their operational efficiency will have an advantage in the global market. Therefore, training in the use of AI-based tools should be integrated in HR development programs so that employees can understand the algorithms and intelligent systems used in various business applications.

Meanwhile, IoT technology is key in connecting various physical devices to collect and share data in real-time. A deep understanding of IoT infrastructure and how these devices work is also important for the workforce. Without adequate understanding, the use of IoT in business processes will be hampered and unable to optimize the potential of this technology. Research by Rahmawati & Subardjo (2023) shows that companies that adopt IoT well can monitor and control industrial processes more efficiently, which can ultimately result in significant cost savings and improve customer satisfaction. Therefore, the development of IoT-related technical skills, such as device and network management, as well as IoT data analysis, is essential to ensure that HR can work with these technologies effectively.

However, in addition to technical skills, soft skills such as communication, teamwork, and adaptability must also be considered. In a study by Mohammed & Ozdamli (2024), 63% of company leaders revealed that soft skills, especially the ability to adapt quickly to technological changes, are one of the determining factors for the success of digital transformation. In an ever-changing digital age, the ability to collaborate in cross-functional teams and adapt to new tools and systems is a skill that cannot be ignored. Therefore, training in interpersonal and managerial skills needs to be part of the reskilling program to ensure that the workforce is not only technically competent, but also capable of working in an increasingly dynamic and connected environment.

In response to these challenges, companies must take proactive steps in preparing their workforce to face the digital age. One step that can be taken is to develop a project-based training program that

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

allows employees to learn practically about the application of AI and IoT technology in a real business context. Partnerships with educational institutions can also be a solution to create a human resource pipeline that is ready to face new technologies. Through this collaboration, companies can ensure that the recruited workforce has skills relevant to the needs of the industry. Mentoring and coaching programs that involve senior employees with experience in digital technology can also accelerate the transfer of knowledge and skills. With this comprehensive approach, companies can not only reduce the skills gap but also ensure that digital transformation can be carried out successfully and sustainably.

Overall, the readiness of HR in the face of digital transformation is an important factor that will determine whether companies can harness the full potential of AI and IoT technologies. Without the right investment in skills development, companies risk losing a competitive advantage in an increasingly digital market. Therefore, companies must take strategic steps in improving the digital skills of their human resources through training, reskilling, and soft skills development, as well as establishing partnerships that support the development of quality human resources.

C. The Need for Strict Data Security Policies and Regulations

The application of technologies such as artificial intelligence (AI) and the Internet of Things (IoT) in various industry sectors brings great challenges, especially in terms of data protection and privacy. In the midst of these rapid advances in technology, the need for strict data security policies and clear regulations has become increasingly urgent. Data security is not only a technical issue, but also related to legal and ethical aspects, which must be regulated in relevant policies and regulations. Many scientific studies and previous studies have highlighted the importance of implementing adequate policies in maintaining the privacy and security of users' personal data. For example, research by Tabayyana & Purwhanata (2024) shows that clear and transparent privacy policies can increase consumer trust in technology companies, which in turn supports wider adoption of AI and IoT technologies. However, despite the awareness of the importance of these policies, the main challenge faced is the implementation of effective regulation, especially in a highly dynamic global market.

Companies using AI and IoT technologies must ensure that they comply with applicable data security regulations in various jurisdictions. In Europe, the General Data Protection Regulation (GDPR) has set high standards in the management of personal data and ensures that individuals' privacy rights are protected across the board. The GDPR not only limits how data can be collected and processed, but it also establishes an obligation for companies to report data leaks within a short period of time. In addition, in Indonesia, the Personal Data Protection Law (PDP Law) which was recently passed in 2022 serves to strengthen personal data protection at the domestic level. Despite these regulations, major challenges remain, especially when it comes to consistent implementation around the world. A number of studies by Arafat & Wirasto (2024) identified gaps in the implementation of the GDPR outside Europe, where global companies still face difficulties in meeting these regulatory standards in countries with weaker regulations. Therefore, it is important for companies to make policy adaptations that not only focus on compliance with local

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

regulations, but are also able to meet more stringent global standards.

One of the critical aspects of data security policies is transparency and accountability in the management of personal data. Research by Alayiddrus & Rizqi. (2023) shows that companies that are open about personal data management policies tend to gain higher trust from consumers. This underscores the importance for companies to not only meet regulatory obligations, but also actively educate their customers on how their data is used and protected. The implementation of this policy is also in line with the views of academics such as Sain & Bahri (2024) who argue that the protection of personal data must be based on the principle of high transparency, which requires companies to give users more control over their data. Thus, more proactive measures in security policies can reduce the risk of data leaks and increase consumer loyalty and trust in the company.

However, it is undeniable that while policies and regulations can help reduce the risk of data leaks, incorrect implementation or negligence in implementing policies can be fatal. Research by Pool et al (2024) on data leaks shows that information leaks often occur due to a lack of compliance with internal security procedures, such as adequate encryption and access controls. Therefore, strict policies must be supported by proper technical implementation, including strong encryption technology, multi-factor authentication, and continuous monitoring of the systems used. Additionally, companies should always be ready to work closely with regulators to ensure that the policies implemented not only meet the legality aspects, but also protect the ethical interests of stakeholders.

Cooperation between the private sector and regulators is also crucial in dealing with these challenges. In many cases, this collaboration helps shape policies that are more holistic and relevant to the latest technological developments. For example, the European Union Agency for Cybersecurity (ENISA) has developed guidelines on how companies can meet GDPR obligations in the context of AI and IoT, which provides practical direction for companies to implement more secure systems. Collaboration between companies and regulators is also important to ensure that the technology used is not only effective in terms of functionality, but also does not violate the basic rights of individuals, such as privacy and freedom.

Overall, strict data security policies and regulations play a crucial role in ensuring the safe, ethical, and trustworthy implementation of AI and IoT technologies. In this digital era, where personal data has become extremely valuable, data protection must be a top priority for all stakeholders, be it companies, regulators, or consumers themselves. With policies that are transparent, accountable, and compliant with global standards, companies can mitigate the risk of data leaks, build customer trust, and ensure that the use of technology is carried out responsibly and sustainably.

CONCLUSIONS

Transformasi digital dalam manajemen bisnis dan akuntansi berkembang pesat dengan penerapan kecerdasan buatan (AI) dan Internet of Things (IoT), yang meningkatkan efisiensi dan otomatisasi operasional. Di bidang akuntansi, AI mengotomatiskan pencatatan transaksi, rekonsiliasi data, dan analisis laporan keuangan secara real-time, sehingga mengurangi kesalahan manusia dan juga biaya administrasi. Studi menunjukkan bahwa perusahaan yang menerapkan AI dalam audit mengalami peningkatan efisiensi sebesar 40%. AI juga membantu analis keuangan memproses data besar dengan kecepatan tinggi, memberikan wawasan yang akurat tentang arus kas dan risiko bisnis. Meskipun memiliki

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

banyak manfaat, penerapan AI menghadapi tantangan keamanan data, sehingga perusahaan harus mengadopsi sistem enkripsi dan keamanan yang kuat. Selain itu, IoT mengoptimalkan operasi dan manajemen rantai pasokan melalui pemantauan aset secara real-time, sehingga mengurangi kesalahan pencatatan hingga 30%. Teknologi IoT juga mendukung distribusi barang yang lebih efisien dan pemeliharaan prediktif, sehingga mengurangi waktu henti produksi hingga 20%. Namun, adopsi AI dan IoT menghadapi kendala biaya yang tinggi, regulasi yang tidak jelas, dan ketergantungan pada vendor teknologi. Regulasi yang ketat seperti GDPR menjadi tantangan tersendiri bagi perusahaan dalam mengelola data IoT. Selain itu, perusahaan harus memastikan tenaga kerja yang siap untuk digitalisasi dengan pelatihan keterampilan teknologi. Dengan strategi yang tepat, AI dan IoT dapat menjadi pendorong utama transformasi digital, meningkatkan efisiensi operasional, dan memberikan keunggulan kompetitif bagi perusahaan di era digital.

REFERENCES

Abdullah, A. A. H., & Almaqtari, F. A. (2024). The impact of artificial intelligence and Industry 4.0 on transforming accounting and auditing practices. Journal of Open Innovation: Technology, Market, and Complexity, 10(1), 100218.

Abos, P. (2024). Vendor Lock-In and Interoperability: Importance of interoperability among cloud services.

Achadiyah, B. N. (2019). Otomatisasi pencatatan akuntansi pada UMKM. Jurnal Akuntansi Multiparadigma, 10(1), 188-206.

Adha, L. A. (2020). Digitalisasi industri dan pengaruhnya terhadap ketenagakerjaan dan hubungan kerja di Indonesia. Jurnal Kompilasi Hukum, 5(2), 267-298.

Alayiddrus, A. S., & Rizqi, R. M. (2023). Pengaruh Kemampuan Dan Integritas Dalam Meningkatkan Minat Pembelian. Jurnal Ekonomi Bisnis, Manajemen dan Akuntansi (JEBMA), 3(3), 844-854.

Arafat, M., & Wirasto, A. T. E. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia. Equality: Journal of Law and Justice, 1(2), 220-241.

Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: surviving online threats. Journal of Business Strategy, 44(1), 3-12.

Damayanti, V. (2025). STRATEGI PEMASARAN BERKELANJUTAN UNTUK MENINGKATKAN DAYA SAING PT. SUN POWER CERAMICS DI ERA DIGITAL: PENDEKATAN INOVATIF DAN PRAKTIS. Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA), 9(1), 18-45.

Erwin, E., Pasaribu, A. W., Novel, N. J. A., Thaha, A. R., Adhicandra, I., Suardi, C., ... & Syafaat, M. (2023). Transformasi Digital. PT. Sonpedia Publishing Indonesia.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini. Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam, 5(2), 87-100.

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

Fauziyyah, N. (2022). Efek digitalisasi terhadap akuntansi manajemen. Jurnal akuntansi keuangan dan bisnis, 15(1), 381-390.

Firdaus, M. A. A., & Kuswinarno, M. (2024). Strategi inovatif dalam pengembangan sumber daya manusia dalam meningkatkan daya saing perusahaan di era digital. Jurnal Media Akademik (JMA), 2(11).

Francisco, M., & Linnér, B. O. (2023). AI and the governance of sustainable development. An idea analysis of the European Union, the United Nations, and the World Economic Forum. Environmental Science & Policy, 150, 103590.

Jha, N., Prashar, D., & Nagpal, A. (2021). Combining artificial intelligence with robotic process automation—an intelligent automation approach. Deep learning and big data for intelligent transportation: enabling technologies and future trends, 245-264.

Judijanto, L., Al-Amin, A. A., & Nurhakim, L. (2024). Implementasi Teknologi Artificial Intelligence dan Machine Learning dalam Praktik Akuntansi dan Audit: Sebuah Revolusi atau Evolusi. COSMOS: Jurnal Ilmu Pendidikan, Ekonomi dan Teknologi, 1(6), 470-483.

Kurniati, S., Kom, M., Saptadi, I. N. T. S., Kom, S., Pardosi, V. B. A., Kom, S., ... & Ilham, S. T. (2024). Internet of Thing. CV Rey Media Grafika.

Laelawati, K. (2024). Membangun Budaya Inovasi Melalui Digital Leadership: Tantangan Dan Peluang Dalam Manajemen Sumber Daya Manusia. Jurnal Mirai Management, 9(1), 1144-1152.

Lestari, N., Jafar, R. F., Febriyanti, N., Saleh, N., Rahmadani, I., & Arsal, M. (2024). Penerapan Kecerdasan Buatan Dalam Akutansi Keuangan: Tantangan Dan Peluang. IJMA (Indonesian Journal of Management and Accounting), 5(2), 279-284.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 6(5), 8182-8201.

Mohammed, F. S., & Ozdamli, F. (2024). A Systematic Literature Review of Soft Skills in Information Technology Education. Behavioral Sciences, 14(10), 894.

Nasman, N., Astuti, P., & Perwitasari, D. (2024). ETIKA DAN PERTANGGUNGJAWABAN PENGGUNAAN ARTIFICIAL INTELENGENCE DI INDONESIA. Jurnal Hukum Lex Generalis, 5(10).

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

Surveys & Tutorials, 21(3), 2702-2733.

Norliani, N., Sari, M. N., Safarudin, M. S., Jaya, R., Baharuddin, B., & Nugraha, A. R. (2024). Transformasi digital dan dampaknya pada organisasi: Tinjauan terhadap implementasi teknologi informatika. Jurnal Review Pendidikan dan Pengajaran (JRPP), 7(3), 10779-10787.

Oktavia, S. (2023). Peran Teknologi Dalam Meningkatkan Efisiensi Operasional Perusahaan Logistik. Central Publisher, 1(9), 1049-1056.

Panjaitan, S. P., & Firdaus, R. (2024). PERAN SISTEM INFORMASI AKUNTANSI DALAM MENGOPTIMALKAN EFISIENSI OPERASIONAL PERUSAHAAN. Jurnal Intelek Insan Cendikia, 1(9), 5691-5696.

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: a scoping review. International Journal of Information Management, 74, 102719.

Pranata, W. A., & Ichsan, I. N. (2024). Menggali Peluang Pasar dan Keuntungan Ekonomi dari Penerapan Industrial IoT. Innovative: Journal Of Social Science Research, 4(6), 1628-1638.

Prawiyogi, A. G., & Anwar, A. S. (2023). Perkembangan Internet of Things (IoT) pada Sektor Energi: Sistematik Literatur Review. Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 1(2), 187-197.

Priyatna, N. M. (2024). Transformasi Digital: Efisiensi dan Inovasi dalam Manajemen Operasional. Economic Reviews Journal, 3(3), 2653-2662.

Rahmawati, M. I., & Subardjo, A. (2023). Internet Of Things (Iot) Dan Blockchain Dalam Perspektif Akuntansi. Jurnal Akuntansi dan Keuangan (JAK), 28(1), 28-36.

Raihan, M., Nasution, M. L. I., & Daulay, A. N. (2024). Analisis Dampak Perkembangan Teknologi AI Dalam Meningkatkan Efisiensi Operasional Bank Syariah (Studi Kasus Bank Sumut Kantor Cabang Syariah Medan Ringroad). Jesya (Jurnal Ekonomi Dan Ekonomi Syariah), 7(2), 2049-2062.

Ramdhan, H., & Aripin, S. (2024). Strategi digital untuk bisnis: Pendekatan praktis dan implementasi di industri 4.0. ADI Bisnis Digital Interdisiplin Jurnal, 5(1), 34-40.

Raza, E., & Komala, A. L. (2020). Manfaat dan Dampak Digitalisasi Logistik di Era Industri 4.0. Jurnal Logistik Indonesia, 4(1), 49-63.

Respati, D. R., & Sukmadewi, R. (2024). Adaptasi Internet of Things (IoT) dalam Manajemen Distribusi dan Gudang: Rantai Pasokan Pada PT. X. JIIP-Jurnal Ilmiah Ilmu Pendidikan, 7(2), 1712-1719.

Sain, M., & Bahri, S. (2024). Ekonomi Islam sebagai Landasan Fundamental dalam Praktik Bisnis Online Era Digital. El-kahfi| Journal of Islamic Economics, 5(02), 203-218.

OIKONOMIA Journal of Management Economics and Accounting
E-ISSN : 3047-602X
Vol. 2. No.2, January 2025
E-ISSN : 3047-602X
DOI : https://doi.org/10.61942/oikonomia.v2i1.298
Available : https://jurnalhafasy.com/index.php/oikonomia

Sriningsih, E., Syam, N. A., & Mustamin, I. (2025). Pengaruh Digitalisasi Akuntansi terhadap Efisiensi dan Pengurangan Biaya pada Perusahaan Wirausaha UMKM di Kota Makassar. Jurnal Penelitian Multidisiplin Ilmu, 3(5), 2959-2968.

Sunaryo, D., Hamdan, A. A., & Cecilia Winata, D. D. A. (2024). Prediksi tren risiko keuangan perusahaan berdasarkan model machine learning (ARIMA): Tinjauan literatur. Jurnal Akuntansi Manajemen, 3(2), 78-94.

Syahfitri, N. C., Al Fiqih, M. E. K., Putri, C., & Hasibuan, A. (2025). STRATEGI TECNO PRENEURSHIP DALAM MENINGKATKAN INOVASI DAN DAYA SAING INDUSTRI. VARIABLE RESEARCH JOURNAL, 2(01), 146-153.

Tabayyana, Q. F., & Purwhanata, N. R. M. R. (2024). Pengaruh Pelanggaran Etika dalam Perkembangan Teknologi Informasi terhadap Kerahasiaan Data Pribadi. Jurnal Riset Ekonomi Syariah, 145-152.

Trista, R. T. (2022). Peran Internet Of Things (IoT) Dalam Industri 4.0. Jurnal Sains dan Teknologi Widyaloka (JSTekWid), 1(2), 235-241.