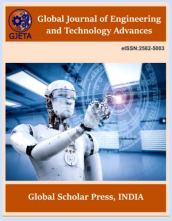
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(RESEARCH ARTICLE)

Check for updates

Big data and AI in employment: The dual challenge of workforce replacement and protecting customer privacy in biometric data usage

Idoko Peter Idoko [1,*], Monica Ajuma Igbede [2], Helena Nbéu Nkula Manuel [3], Tola Ojemai Adeoye [4], Francis Adejor Akpa [5] and Chukwunonso Ukaegbu [6]

[1] *Department of Electrical & Electronics Engineering, University of Ibadan, Ibadan, Nigeria.*
[2] *Department of Procurement, Clarissa Dynamic Links Ltd, Makurdi.*
[3] *College of Architecture Construction and Planning, Department of Architecture, The University of Texas at San Antonio, Texas, USA.*
[4] *C.T. Bauer College of Business, Department of Decision and Information Sciences, University of Houston, Texas, USA.*
[5] *Department of Public Health, Kogi State Ministry of Health, Lokoja, Kogi State, Nigeria.*
[6] *Production Department, Von Food and Farms Limited, Nimo, Anambra, Nigeria.*

Global Journal of Engineering and Technology Advances, 2024, 19(02), 089–106

Publication history: Received on 04 April 2024; revised on 12 May 2024; accepted on 14 May 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.19.2.0080

Abstract

The integration of Artificial Intelligence (AI) and Big Data is ushering in profound transformations across various industries, with biometric data usage standing out due to its deep implications for workforce dynamics and customer privacy. This review article critically examines the dual challenges presented by AI-driven automation and the extensive use of biometric data analytics, focusing on the resultant job displacement and escalating privacy concerns. Biometric technologies such as facial recognition, fingerprint identification, and voice analysis are increasingly deployed across sectors including finance, healthcare, and retail. These technologies aim to enhance security measures, improve user experience, and optimize operational efficiencies. However, they also bring to light substantial ethical dilemmas, particularly concerning the privacy of individuals and the security of the data being collected. The pervasive collection and analysis of biometric data can lead to invasive surveillance and profiling, exacerbating risks to personal privacy. Moreover, the use of AI in automating tasks that were traditionally performed by human workers is leading to significant shifts in employment structures. While AI can increase efficiency and reduce costs, it also raises the specter of widespread job displacement. This potential for automation-driven unemployment is especially pronounced in sectors that heavily utilize routine, repetitive tasks, posing critical socio-economic challenges. This article also explores the regulatory and technological frameworks currently in place, and those that are needed to address these challenges. The effectiveness of existing data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, and the California Consumer Privacy Act (CCPA) in the United States, is assessed in the context of AI and biometric data. We discuss the role of policy in shaping the ethical use of AI and protecting workers, along with the technological safeguards that could be implemented to secure biometric data and ensure privacy. By synthesizing insights from recent research, case studies, and expert analyses, this article provides a comprehensive overview of how AI and Big Data are reshaping the landscape of work and privacy. It critically discusses the need for a balanced approach that harnesses the benefits of technological advancements while safeguarding individual rights and employment security.

Keywords: Big Data; Artificial Intelligence; Workforce Replacement; Biometric Data Usage.

* Corresponding author: Idoko Peter Idoko.

1. Introduction

1.1. Brief overview of the integration of AI and Big Data

The integration of artificial intelligence (AI) and big data has revolutionized various sectors, including employment. This synergy allows organizations to harness vast amounts of data to derive valuable insights and make data-driven decisions (Awad et al. 2024). AI algorithms, powered by big data analytics, enable automation, predictive analysis, and personalized experiences, enhancing efficiency and competitiveness in the global market (Brynjolfsson & McAfee, 2014).

In their study, Idoko et al. (2024) emphasized the significance of renewable energy policies by conducting a comparative analysis between Nigeria and the USA. Although their focus was on energy policies, their findings underscore the broader implications of policy implementation and technological advancements on socio-economic dynamics. The integration of AI and big data in renewable energy initiatives exemplifies how innovative technologies shape workforce dynamics and regulatory frameworks.

The convergence of AI and big data fuels advancements in biometric technologies, driving their widespread adoption across industries (Awad et al. 2024). These technologies, ranging from facial recognition to fingerprint authentication, serve diverse purposes such as enhancing security measures, improving user experience, and optimizing operational efficiencies (Awad et al. 2024). However, alongside these benefits emerge ethical dilemmas and privacy concerns associated with pervasive biometric data collection and analysis (Awad et al. 2024). Hence, it becomes imperative to examine the dual challenges of workforce replacement and protecting customer privacy in biometric data usage within the context of AI and big data integration.

Table 1 Overview of the Integration of AI and Big Data in Various Sectors: Impacts, Applications, Studies, and Challenges

Aspect	Impact	Applications	Key Studies	Challenges
General Impact	Revolutionizes sectors including employment	Harnessing data for insights and decisions	Awad et al. (2024)	Balancing efficiency with ethical and privacy concerns
Technological Synergy	Enhances efficiency and global competitiveness	Automation, predictive analysis, personalized experiences	Brynjolfsson & McAfee (2014)	-
Renewable Energy Policies	Demonstrates socio-economic impacts of policy and technology	Renewable energy initiatives	Idoko et al. (2024)	Impact on workforce dynamics and regulatory frameworks
Biometric Technologies	Drives widespread adoption across industries	Security enhancements like facial recognition and fingerprint authentication	Awad et al. (2024)	Ethical dilemmas, privacy concerns, workforce replacement, customer privacy

Table 1 provides a structured summary of the integration of artificial intelligence (AI) and big data across various sectors. It highlights the general impact of this integration, such as revolutionizing industries and enhancing efficiency and global competitiveness, specifically in employment and technology-driven areas. Various applications are detailed, including the use of AI and big data for automation, predictive analysis, personalized experiences, and security enhancements like facial recognition and fingerprint authentication. Key studies like those by Awad et al. (2024), Brynjolfsson & McAfee (2014), and Idoko et al. (2024) underline the importance of data-driven decisions, the socio-economic impacts of renewable energy policies, and the broad implications for workforce dynamics and regulatory frameworks. The table also addresses challenges, noting ethical dilemmas and privacy concerns, particularly in the context of biometric technologies, emphasizing the need for a balance between technological advancements and ethical standards.

1.2. Importance of examining the dual challenges of workforce replacement and protecting customer privacy in biometric data usage

In the rapidly evolving landscape of technological innovation, the implementation of the Internet of Things (IoT) serves as a testament to the transformative power of interconnected devices (Idoko et al., 2024). However, alongside the proliferation of IoT devices comes the intricate balance between reaping the benefits of technological advancements and addressing the accompanying challenges, particularly concerning workforce displacement and safeguarding individual privacy, especially in the context of biometric data usage. The comparative analysis conducted by Idoko et al. (2024) between Ghana and the USA in IoT implementation sheds light on the multifaceted nature of technological integration and its impact on socio-economic dynamics. While IoT presents opportunities for improved efficiency, productivity, and connectivity, it also raises concerns regarding job displacement due to automation and the ethical use of personal data, including biometric information (Idoko et al., 2024).

Privacy concerns surrounding biometric data usage have garnered significant attention in recent years, with scholars emphasizing the need for robust safeguards to protect individuals' privacy rights (Kindt, 2013). Biometric data, including facial recognition and fingerprint scans, are increasingly utilized for authentication and identification purposes across various sectors. However, the collection, storage, and analysis of biometric data raise ethical and legal challenges, necessitating comprehensive regulatory frameworks and technological safeguards (Kindt, 2013). Furthermore, the advent of big data analytics and AI-driven automation amplifies the potential implications of workforce replacement, as routine and repetitive tasks become increasingly automated (Kühn, 2019). As highlighted by Acquisti and Gross (2006), the widespread adoption of digital technologies, such as social media platforms, has transformed notions of privacy and raised awareness regarding the protection of personal information. Similarly, the integration of biometric technologies into everyday applications underscores the importance of balancing technological advancements with privacy considerations to ensure ethical and responsible use of data (Acquisti & Gross, 2006). Therefore, examining the dual challenges of workforce replacement and protecting customer privacy in biometric data usage is paramount in navigating the complexities of the digital age while upholding individual rights and societal values.

1.3. Organization of the paper

The paper begins with an introduction providing a brief overview of the integration of artificial intelligence (AI) and big data, highlighting the importance of examining the dual challenges of workforce replacement and protecting customer privacy in biometric data usage. Following this, the paper delves into the age of AI-driven automation and its implications for employment dynamics, discussing the role of AI in automating tasks traditionally performed by human workers and the potential for job displacement, especially in sectors relying on routine and repetitive tasks. It then transitions into an exploration of biometric data usage, emphasizing its applications across industries and the ethical dilemmas and privacy concerns associated with pervasive biometric data collection and analysis. The subsequent section discusses ethical and regulatory frameworks, providing an overview of existing data protection laws and assessing their effectiveness in addressing challenges related to AI and biometric data. The paper then explores technological safeguards for biometric data privacy, discussing encryption, anonymization techniques, and data access controls, followed by case studies and expert analyses illustrating real-world implications of AI-driven automation and biometric data usage. Finally, the conclusion recaps key points discussed in the paper, emphasizes the importance of a balanced approach towards harnessing the benefits of AI and big data while safeguarding individual rights and employment security, and suggests future research directions and policy considerations.

2. Biometric data usage in the age of AI

2.1. Explanation of biometric technologies and their applications across industries

Biometric data usage has witnessed significant advancements in the age of artificial intelligence (AI), particularly in the context of enhancing security measures, improving user experience, and optimizing operational efficiencies. Idoko et al. (2024) highlight the vital role of power electronics in California's renewable energy transformation, emphasizing the technological innovations driving sustainable power generation. Manso and El-Saadany (2012) provide a comprehensive review of recent advances in renewable energy integration, shedding light on the interdisciplinary nature of renewable energy technologies and their impact on power electronics. Within the realm of biometric data usage, Ge et al (2018) conduct a survey on big data in the Internet of Things (IoT), elucidating the role of biometric sensors and data analytics in IoT applications. Moreover, Colmenares-Quintero et al. (2021) review the application of big data in renewable energy, underscoring the potential of data-driven approaches in optimizing renewable energy systems. Thus, biometric data usage in the age of AI encompasses a multifaceted landscape of technological

advancements, spanning from renewable energy integration to IoT applications, underpinned by data-driven strategies and power electronics innovations.

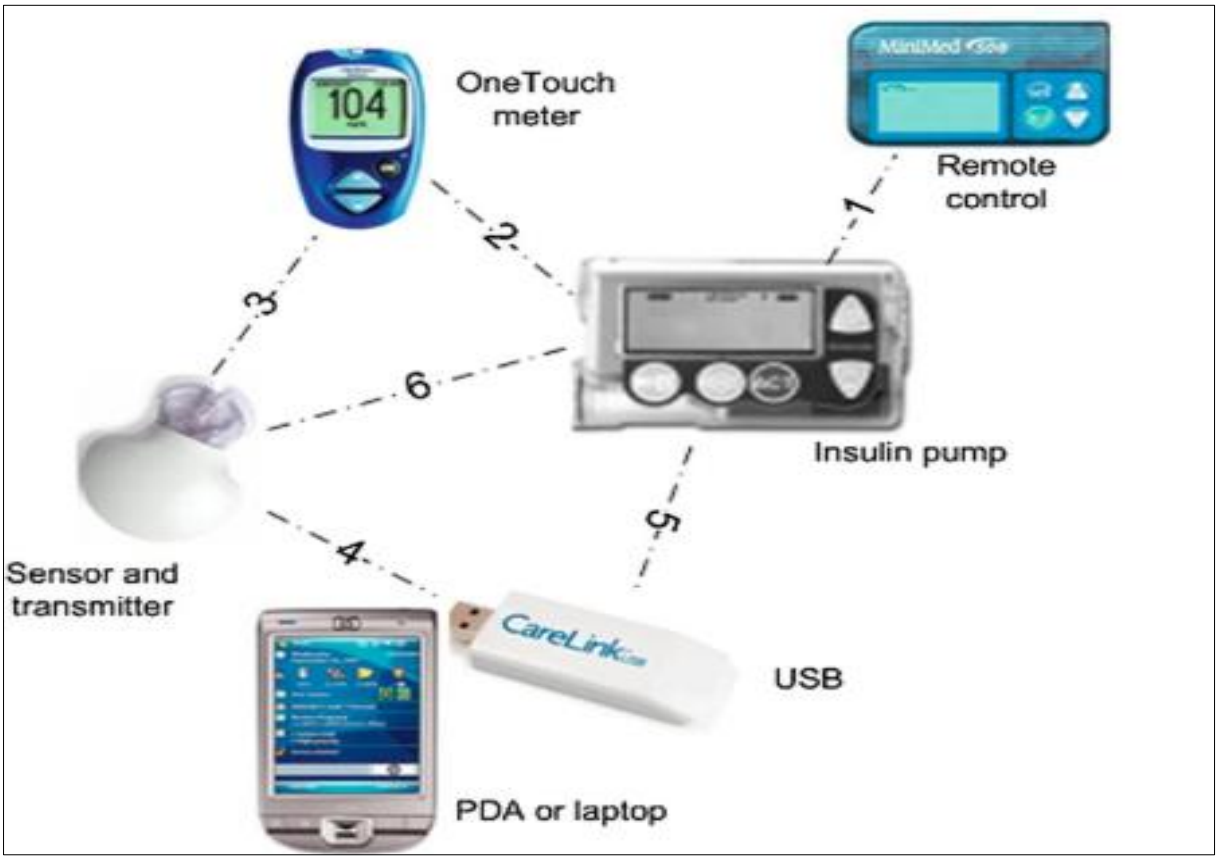


Figure 1 Biometric data application in health (Hei et al.2013)

Figure 1 illustrates a diabetes management system integrating several devices to monitor and control blood glucose levels using biometric data. It features a OneTouch meter for glucose measurement, an insulin pump for administering insulin, and a MiniMed device that acts as both a remote control and display unit. A sensor and transmitter worn on the body continuously monitor glucose levels and transmit this biometric data to other devices, including a PDA or laptop which allows for detailed data management and device configuration via USB. This interconnected setup enables an automated and precise approach to diabetes care, optimizing treatment through real-time data utilization.

Figure 2 illustrates two biometric systems: Identification and Verification. In the Identification System, a sensor captures biometric data, which is then processed to extract unique features. These features are compared against a database in a Biometric Matcher, resulting in an Output that identifies the individual. The Verification System starts similarly with a sensor capturing data when an ID is presented. It also extracts features and compares them against a database. However, its purpose is to either accept or reject the identity claim, as indicated by the final decision of "REJECT!!!" in the diagram.

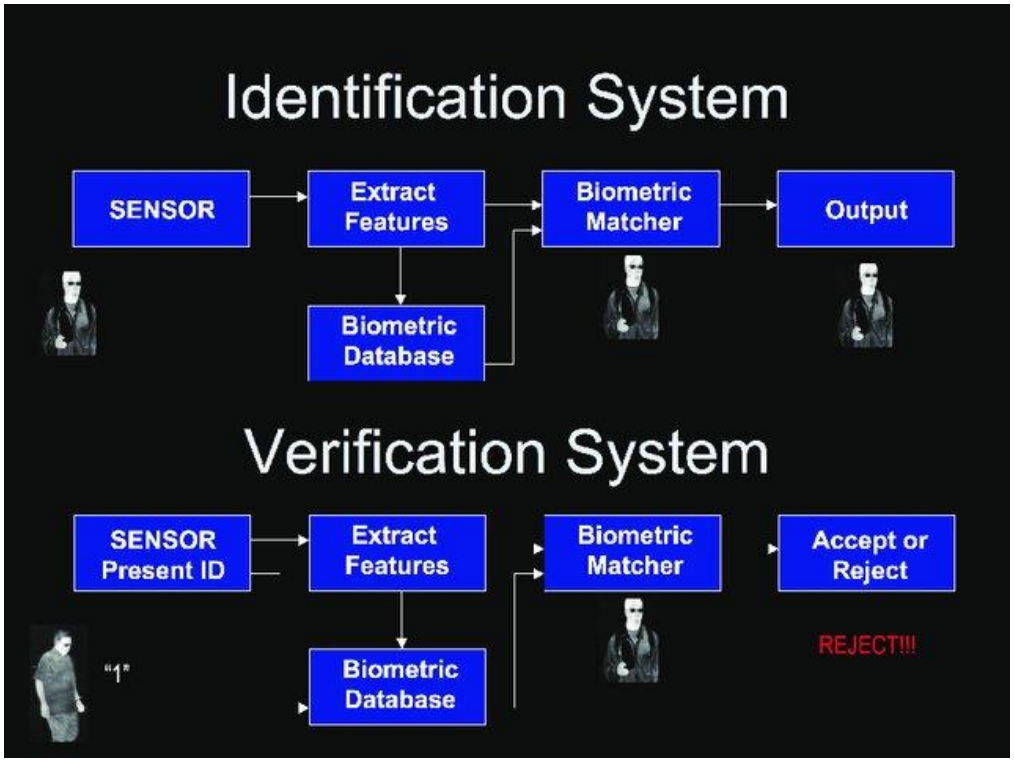


Figure 2 Biometric Identification and Verification Systems Flowchart (Byrd et al. 2009)

2.2. Emphasis on enhancing security measures, improving user experience, and operational efficiencies

In the age of artificial intelligence (AI) and biometric data usage, there is a significant emphasis on enhancing security measures, improving user experience, and optimizing operational efficiencies. Idoko et al. (2024) delve into the potential of Elon Musk's proposed quantum AI, providing a comprehensive analysis of its implications. Melzi et al (2022) discuss biometric authentication as a secure and privacy-enhancing approach, highlighting its role in bolstering security measures while ensuring user privacy. Within the context of the Internet of Things (IoT), Lien & Vhaduri (2023). survey the application of biometric recognition, elucidating its potential in enhancing security and user experience in IoT applications. Additionally, Meden et al (2021) conduct a survey on biometric data security and privacy, emphasizing the importance of safeguarding biometric information to maintain user trust and operational integrity. Thus, the integration of AI and biometric data usage facilitates the enhancement of security measures, the improvement of user experience, and the optimization of operational efficiencies across various domains, from quantum AI to IoT applications.

2.3. Introduction of ethical dilemmas and privacy concerns associated with pervasive biometric data collection and analysis

In the context of AI and biometric data usage, there is an introduction of ethical dilemmas and privacy concerns associated with pervasive biometric data collection and analysis. Ijiga et al. (2024) explore generative music models, voice cloning, and voice transfer for creative expression, highlighting the intersection of AI and creative endeavors. Kaur et al (2023) provide a comprehensive review of recent advances in biometric encryption, emphasizing the importance of protecting biometric data to safeguard user privacy and prevent unauthorized access. Delac & Grgic (2004) survey recent approaches and algorithms in biometric recognition systems, discussing the implications of biometric data usage for security and privacy. Moreover, Rui & Yan (2018) review security and privacy issues in voice biometrics, underscoring the need for robust safeguards to protect individuals' biometric information from potential misuse. Thus, while AI and biometric technologies offer innovative solutions for various applications, ethical considerations and privacy concerns surrounding biometric data collection and analysis remain paramount in ensuring responsible and secure deployment of these technologies.

Figure 3 explores ethical dilemmas and privacy concerns related to the use of biometric data. At the center of the diagram, the main topic is highlighted, with subtopics branching out to detail various aspects of the issue. On the left, there is a focus on the protection of biometric information, emphasizing the importance of safeguards against potential misuse and pervasive data collection, and the need for robust measures to ensure privacy. On the right, future considerations and technological advancements are mapped out from 2004 to 2024, highlighting key developments like

AI and biometric data usage, issues in voice biometrics, and advances in biometric encryption. Notably, the timeline progresses towards emerging technologies such as voice cloning and generative music models. The diagram underscores the evolving landscape of biometric technology and the pressing need to address the ethical and privacy challenges that accompany its growth.

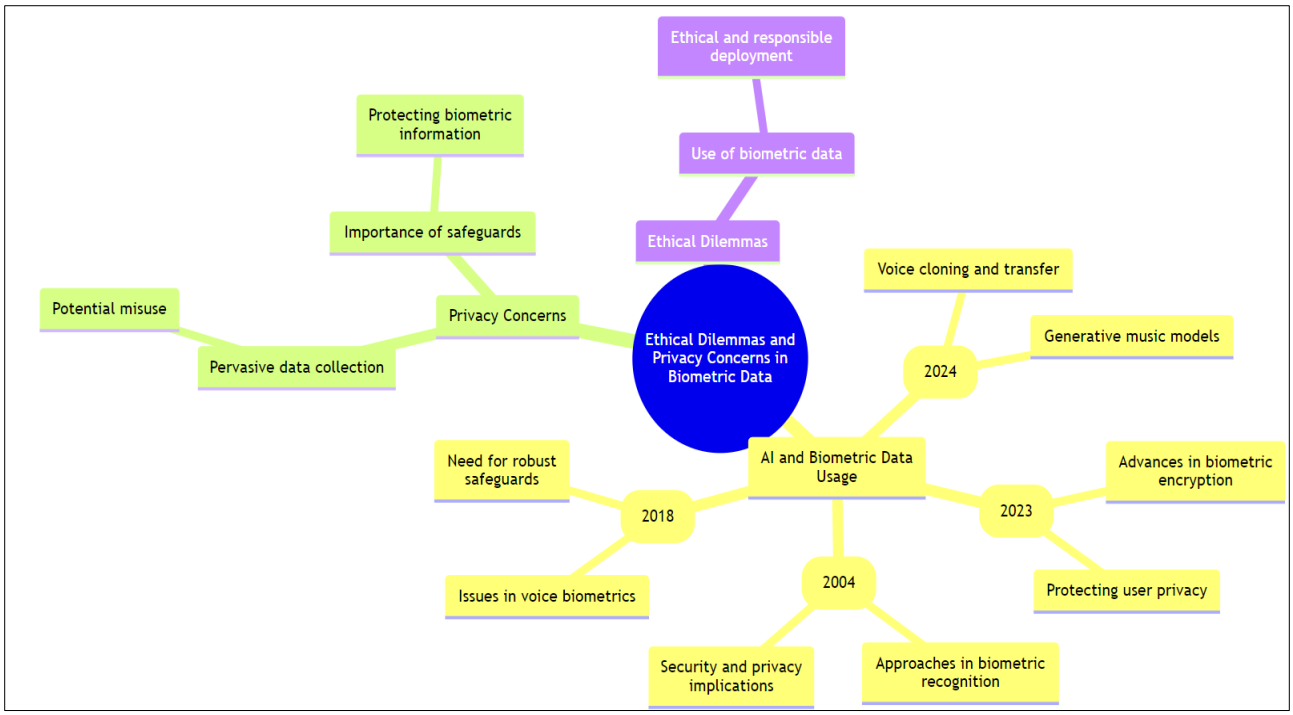


Figure 3 Navigating Ethical Dilemmas and Privacy Concerns in Biometric Data Usage

3. AI-driven automation and employment dynamics.

3.1. Discussion on the role of AI in automating tasks traditionally performed by human workers

In the context of technological innovations, the role of artificial intelligence (AI) in automating tasks traditionally performed by human workers is a subject of considerable discussion. Ijiga et al. (2024) explore technological innovations in mitigating winter health challenges in New York City, showcasing the transformative potential of AI-driven solutions in addressing public health concerns. Brynjolfsson and McAfee (2014) delve into the implications of the second machine age, highlighting the unprecedented advancements in AI and automation that reshape the nature of work and productivity. Leopold et al. (2018) discusses the future of jobs, emphasizing the impact of AI and automation on employment dynamics and the need for reskilling and upskilling initiatives to adapt to the evolving labor market. Additionally, Acemoglu and Restrepo (2018) examine the relationship between AI, automation, and work, elucidating the implications of technological advancements for labor markets, income distribution, and economic growth. Thus, the discussion on the role of AI in automating tasks traditionally performed by human workers encompasses a multifaceted examination of its impact on industries, employment patterns, and societal well-being.

Table 2 provides a concise summary of key research findings regarding the role of artificial intelligence (AI) in automating tasks traditionally performed by human workers. It encompasses insights from various authors and studies spanning different years. Ijiga et al. (2024) highlight the transformative potential of AI-driven solutions in addressing public health challenges, particularly in winter health issues in New York City. Brynjolfsson and McAfee (2014) emphasize the significant advancements in work and productivity brought about by AI and automation, shaping the nature of employment. Leopold et al. (2018) discuss the substantial impact of AI and automation on employment dynamics, emphasizing the necessity for reskilling and upskilling initiatives to adapt to the evolving labor market. Finally, Acemoglu and Restrepo (2018) delve into the broader implications of AI and automation on labor markets, income distribution, and economic growth, highlighting the need for structural adaptations to address these changes. Overall, the table presents a comprehensive overview of the multifaceted discussion surrounding AI's impact on industries, employment patterns, and societal well-being.

Table 2 Exploring the Impact of AI and Automation: Insights from Recent Studies

Author(s)	Year	Focus Area	Key Findings	Implications
Ijiga et al.	2024	Technological innovations in public health	AI-driven solutions are effective in mitigating winter health challenges in New York City.	Transformative potential for public health.
Brynjolfsson & McAfee	2014	The second machine age	AI and automation bring unprecedented advancements in work and productivity.	Reshaping of work nature and productivity.
Leopold et al.	2018	Future of jobs	AI and automation significantly impact employment dynamics; reskilling and upskilling are essential.	Need for adaptive labor initiatives.
Acemoglu & Restrepo	2018	AI, automation, and work	Examines how AI and automation influence labor markets, income distribution, and economic growth.	Implications for economic structures and income distribution.

3.2. Examination of the potential for job displacement, especially in sectors relying on routine and repetitive tasks

An examination of the potential for job displacement, especially in sectors relying on routine and repetitive tasks, is critical in understanding the impact of technological advancements on employment dynamics. Ijiga et al. (2024) address ethical considerations in implementing generative AI for healthcare supply chain optimization, shedding light on the transformative potential of AI-driven solutions in healthcare logistics. Frey and Osborne (2017) conduct a comprehensive analysis of the future of employment, assessing the susceptibility of jobs to computerization and highlighting the risks of job displacement, particularly in occupations characterized by routine and predictable tasks. Ford (2015) discusses the rise of automation and its implications for mass unemployment, emphasizing the need for societal adaptation to mitigate the adverse effects on labor markets. Manyika et al. (2017) explore the future of work, discussing the implications of automation and AI on jobs, skills, and wages, and proposing strategies to navigate the evolving labor landscape. Thus, the examination of job displacement in sectors reliant on routine and repetitive tasks provides valuable insights into the potential disruptions caused by technological advancements and underscores the importance of proactive measures to address workforce transitions and mitigate socio-economic challenges.

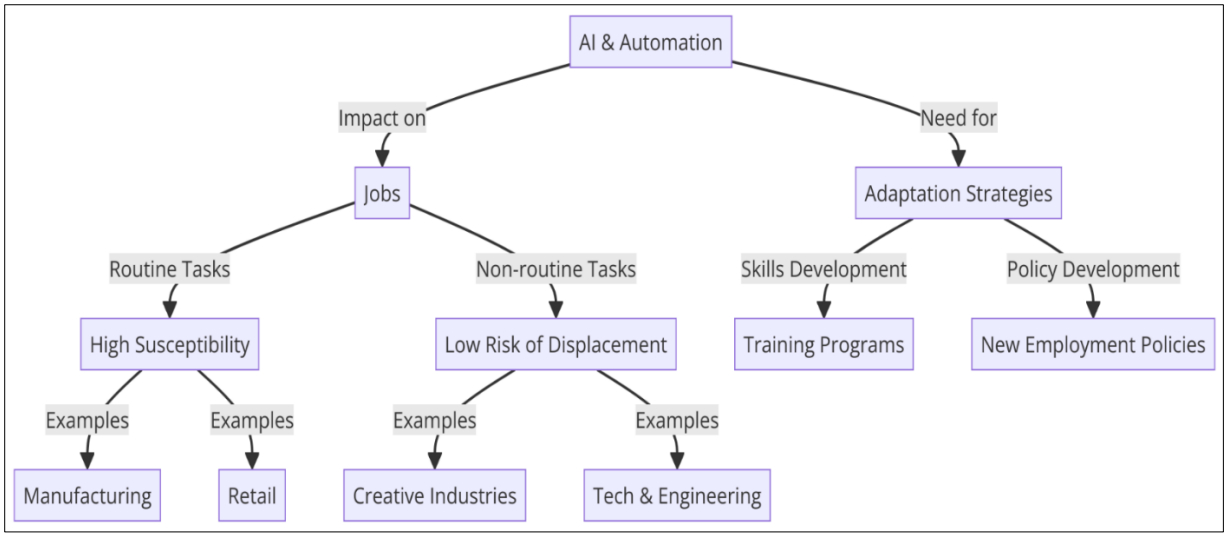


Figure 4 Impact of AI and Automation on Job Displacement

Figure 4 visually represents the impact of AI and automation on job displacement across different sectors, focusing on routine and non-routine tasks. It delineates the heightened susceptibility of jobs involving routine tasks, such as in

manufacturing and retail, to automation. Conversely, jobs involving non-routine tasks, like those in creative industries and tech engineering, show a lower risk of displacement. The diagram also explores necessary adaptation strategies, highlighting the need for skills development through training programs and the creation of new employment policies to mitigate the effects of job displacement. This organized layout helps in understanding the interconnections between AI advancements and their varied impacts on different job sectors.

3.3. Highlighting socio-economic challenges posed by automation-driven unemployment

Highlighting socio-economic challenges posed by automation-driven unemployment is essential for understanding the broader implications of technological advancements on society. Ijiga et al. (2024) delve into ethical considerations in implementing generative AI for healthcare supply chain optimization, underscoring the need to address potential socio-economic ramifications of AI-driven solutions. Brynjolfsson and McAfee (2014) discuss the second machine age, emphasizing the transformative impact of technology on work, progress, and prosperity, while also acknowledging the challenges posed by automation-driven unemployment. Stahl et al (2022) examines the regulatory and ethical implications of artificial intelligence, stressing the importance of ensuring ethical standards and protecting fundamental rights in the development and deployment of AI technologies. Additionally, Tarisayi (2024) provides a toolkit for empowering AI leadership through trust and responsibility, highlighting the importance of ethical governance frameworks to mitigate socio-economic challenges and foster responsible AI innovation. Thus, highlighting socio-economic challenges posed by automation-driven unemployment serves as a catalyst for informed policy interventions and ethical considerations to ensure inclusive and sustainable societal progress amidst technological disruptions.

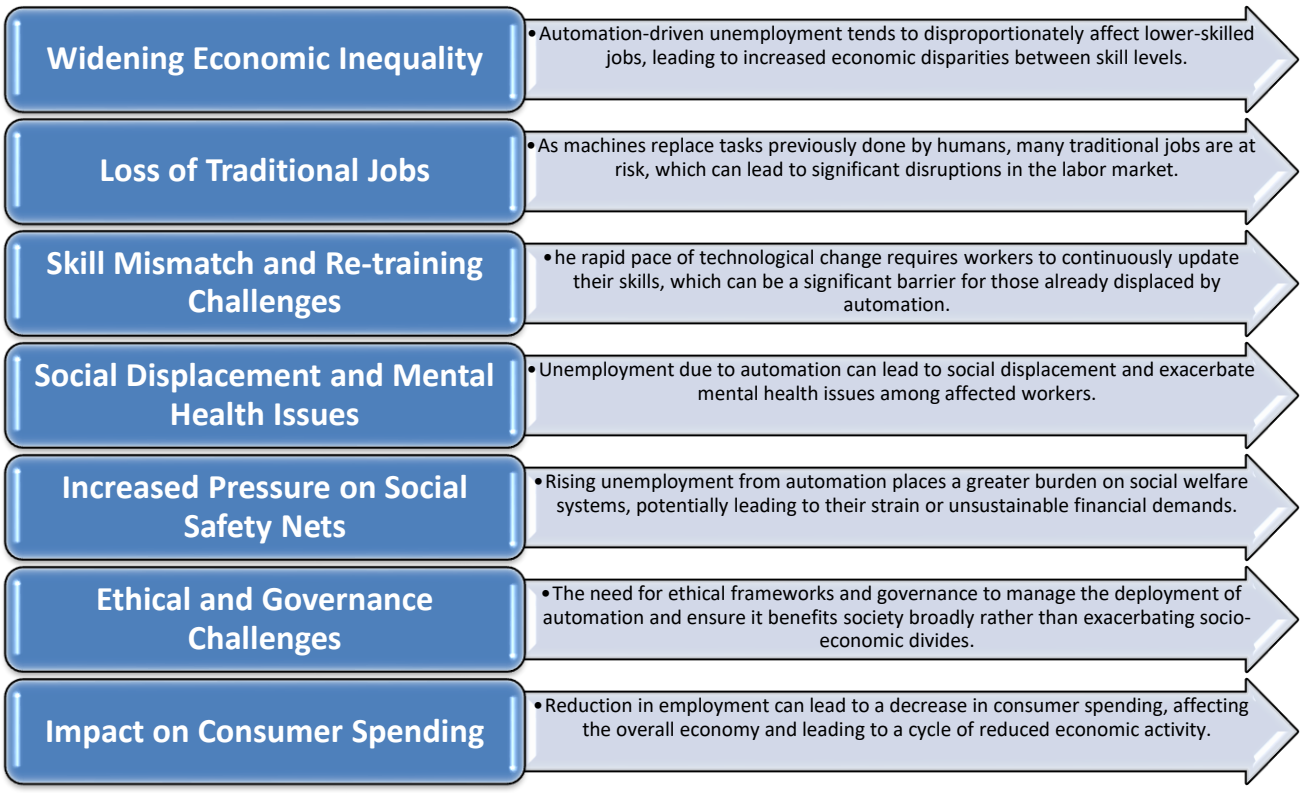


Figure 5 Socio-Economic Challenges of Automation-Driven Unemployment

Figure 5 outlines the socio-economic challenges posed by automation-driven unemployment. It highlights several key areas impacted by the increasing use of automation and technology in the workplace: Widening Economic Inequality, due to automation disproportionately affecting lower-skilled jobs; Loss of Traditional Jobs, as machines replace tasks previously done by humans; Skill Mismatch and Re-training Challenges, necessitating continual skill updates; Social Displacement and Mental Health Issues, as unemployment from automation leads to social and psychological stress; Increased Pressure on Social Safety Nets, straining welfare systems due to rising unemployment; Ethical and Governance Challenges, requiring robust frameworks to ensure equitable technology deployment; and Impact on Consumer Spending, reducing overall economic activity due to lower employment. Each point in the diagram emphasizes the need for thoughtful policy and ethical considerations to mitigate these challenges.

4. Ethical and regulatory frameworks

4.1. Overview of existing data protection laws, including GDPR and CCPA

An overview of existing data protection laws, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), is essential for understanding the regulatory landscape governing AI and data usage. Ijiga et al. (2024) delve into ethical considerations in implementing generative AI for healthcare supply chain optimization, highlighting the importance of adhering to data protection regulations in AI-driven solutions. Stahl et al (2022) examines the regulatory framework surrounding artificial intelligence, focusing on the GDPR's role in ensuring ethical standards and protecting individuals' privacy rights in AI applications. Ufert (2020) discusses the impact of the GDPR on AI, emphasizing the privacy considerations and challenges posed by the regulation's stringent data protection requirements. Thus, an overview of existing data protection laws, including the GDPR and CCPA, provides insights into the evolving regulatory landscape shaping AI development and deployment, with a focus on safeguarding individuals' privacy and data rights.

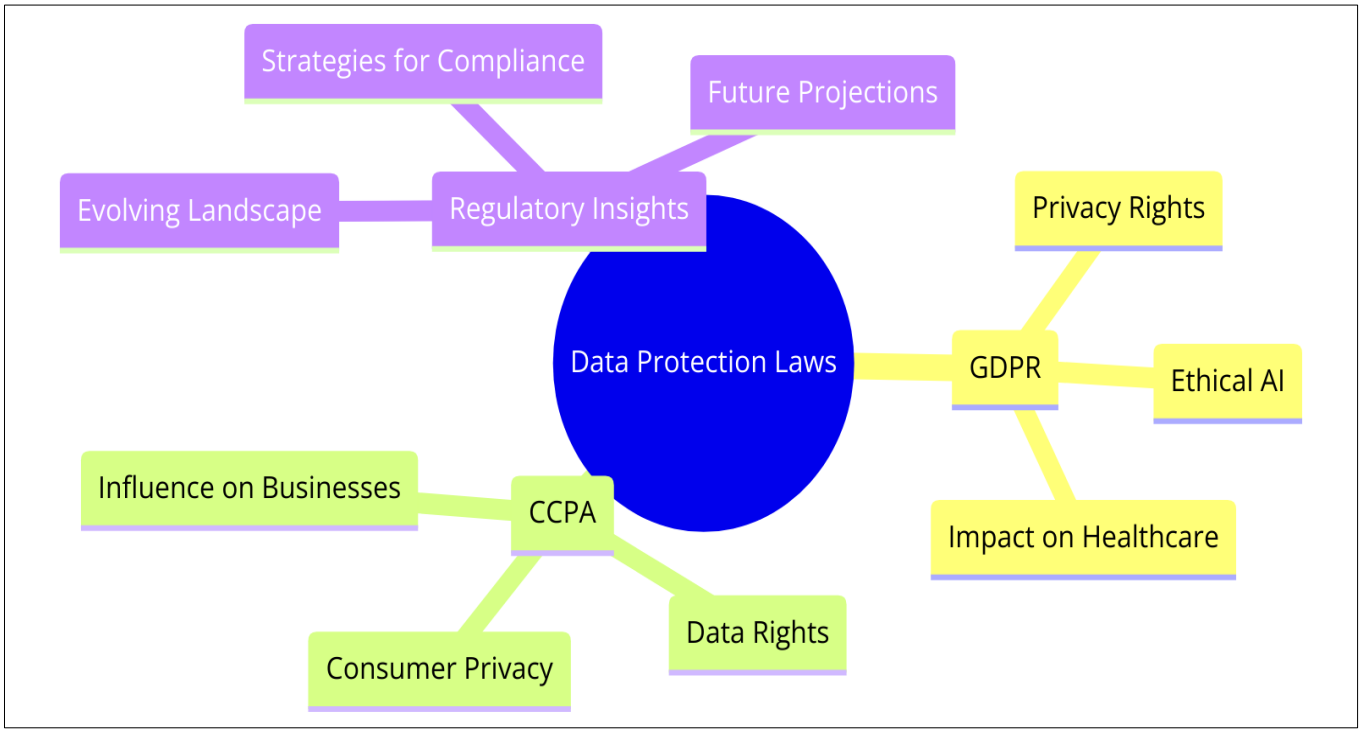


Figure 6 Overview of Data Protection Laws: GDPR and CCPA

Figure 6 provides a structured overview of the major data protection laws, specifically the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). It highlights the key aspects of GDPR, such as privacy rights, ethical AI considerations, and its impact on healthcare sectors, alongside the CCPA's focus on consumer privacy, data rights, and its influence on business practices. Additionally, the diagram outlines broader regulatory insights, discussing the evolving landscape of data protection, strategies for compliance, and future projections, offering a comprehensive view of how these laws shape the handling and protection of data in various domains.

4.2. Assessment of their effectiveness in addressing challenges related to AI and biometric data

An assessment of the effectiveness of existing data protection laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), in addressing challenges related to AI and biometric data usage is crucial for ensuring ethical and responsible use of technology. Ijiga et al. (2024) explore ethical considerations in implementing generative AI for healthcare supply chain optimization, emphasizing the need for regulatory frameworks to mitigate potential risks associated with AI-driven solutions. Stahl et al (2022) examines the regulatory landscape surrounding artificial intelligence and its ethical implications, assessing the role of the GDPR in safeguarding individuals' privacy rights in AI applications. Townsend & Wallace (2017) provide ethical guidelines for using social media data in research, highlighting the importance of ethical considerations and data protection measures in utilizing sensitive data sources for scientific inquiry. Thus, an assessment of the effectiveness of existing data protection laws in addressing

challenges related to AI and biometric data usage underscores the need for robust regulatory frameworks to uphold ethical standards and protect individuals' rights in the digital age.

Table 3 Effectiveness of Data Protection Laws in Addressing AI and Biometric Data Challenges

Author(s)	Year	Regulatory Focus	Key Considerations	Effectiveness Assessment
Ijiga et al.	2024	Generative AI in healthcare	Need for regulatory frameworks to mitigate risks	Stresses importance of regulations but lacks specific assessment
Stahl et al.	2022	AI regulations, GDPR	Privacy rights in AI applications	Highlights GDPR's role but suggests need for further adaptation
Townsend & Wallace	2017	Ethical use of social media data	Ethical guidelines and data protection	Calls for strong ethical considerations, effectiveness unclear

Table 3 summarizes the discussions from various studies regarding how well current regulations address the complexities of AI and biometric data, indicating a general consensus on the necessity for enhanced or adapted regulatory measures to meet the specific challenges posed by new technologies.

4.3. Discussion on the need for updated regulations and policies to ensure ethical use of AI and protect workers' rights

A discussion on the need for updated regulations and policies to ensure the ethical use of artificial intelligence (AI) and protect workers' rights is imperative for addressing emerging ethical challenges in the digital age. Ijiga et al. (2024) explore ethical considerations in implementing generative AI for healthcare supply chain optimization, highlighting the necessity for regulatory frameworks to guide AI deployment responsibly across different countries. Stahl et al (2022) examines the regulatory landscape surrounding AI and its ethical implications, emphasizing the importance of updated regulations to address emerging ethical concerns and protect individuals' rights in AI applications. Mittelstadt and Floridi (2016) discuss the ethics of big data in biomedical contexts, underscoring the need for ethical frameworks to govern data usage and protect individuals' privacy and autonomy in healthcare settings. Thus, a discussion on the need for updated regulations and policies serves as a call to action for policymakers to prioritize ethical considerations and enact measures to safeguard workers' rights and ensure responsible AI deployment in the digital era.

Table 4 Urgent Need for Updated Regulations to Ensure Ethical AI Use and Worker Protection

Author(s)	Year	Proposed Solutions	Key Points	Call to Action
Ijiga et al.	2024	Develop international regulatory frameworks	Necessity for regulatory frameworks across countries	Advocate for responsible AI deployment guidelines
Stahl et al.	2022	Update and adapt existing regulations	Importance of updated regulations for emerging concerns	Emphasize updating regulations to protect rights
Mittelstadt and Floridi	2016	Establish ethical guidelines specific to healthcare	Need for ethical frameworks to protect privacy and autonomy	Urge creation of ethical guidelines in healthcare

Table 4 summarizes the perspectives and recommendations of various researchers on the need for updated regulations and policies to ensure the ethical use of AI and protect workers' rights. Ijiga et al. (2024) advocate for the development of international regulatory frameworks specifically tailored to the deployment of generative AI in healthcare, emphasizing the need for responsible guidelines. Stahl et al. (2022) focus on the necessity to update and adapt existing regulations to better address the new ethical challenges that arise with AI advancements, ensuring that individuals' rights are safeguarded. Mittelstadt and Floridi (2016) call for the establishment of specific ethical guidelines in healthcare to manage big data use, aiming to protect individuals' privacy and autonomy. Collectively, these discussions urge policymakers to prioritize ethical considerations and create robust measures to ensure responsible AI deployment across various sectors.

5. Technological safeguards for biometric data privacy

5.1. Exploration of technological solutions to secure biometric data and ensure privacy

Exploring technological solutions to secure biometric data and ensure privacy is essential in mitigating the risks associated with data breaches and unauthorized access. Ijiga et al. (2024) discuss ethical considerations in implementing generative AI for healthcare supply chain optimization, highlighting the importance of robust data security measures to protect sensitive healthcare information. Chen and Chiu (2018) address data security and privacy protection issues in cloud computing, emphasizing the need for encryption, access controls, and authentication mechanisms to safeguard data stored in the cloud. Durneva et al. (2020) conduct a systematic review on blockchain technology in the healthcare sector, exploring its applications in securing electronic health records and ensuring data integrity and privacy. Thus, the exploration of technological solutions such as encryption, blockchain, and secure cloud computing offers promising avenues to enhance the security and privacy of biometric data in various domains, including healthcare supply chains.

Figure 7 visualizes various technological strategies to enhance the security and privacy of biometric data. Central to the diagram are three main technological solutions: Encryption, Blockchain, and Secure Cloud Computing. Each branch details specific applications such as cloud data encryption, end-to-end encryption, securing electronic health records, ensuring data integrity, and implementing robust encryption, authentication, and access controls within cloud environments. This arrangement highlights how these technologies can safeguard sensitive information against unauthorized access and breaches, particularly in healthcare and related sectors.

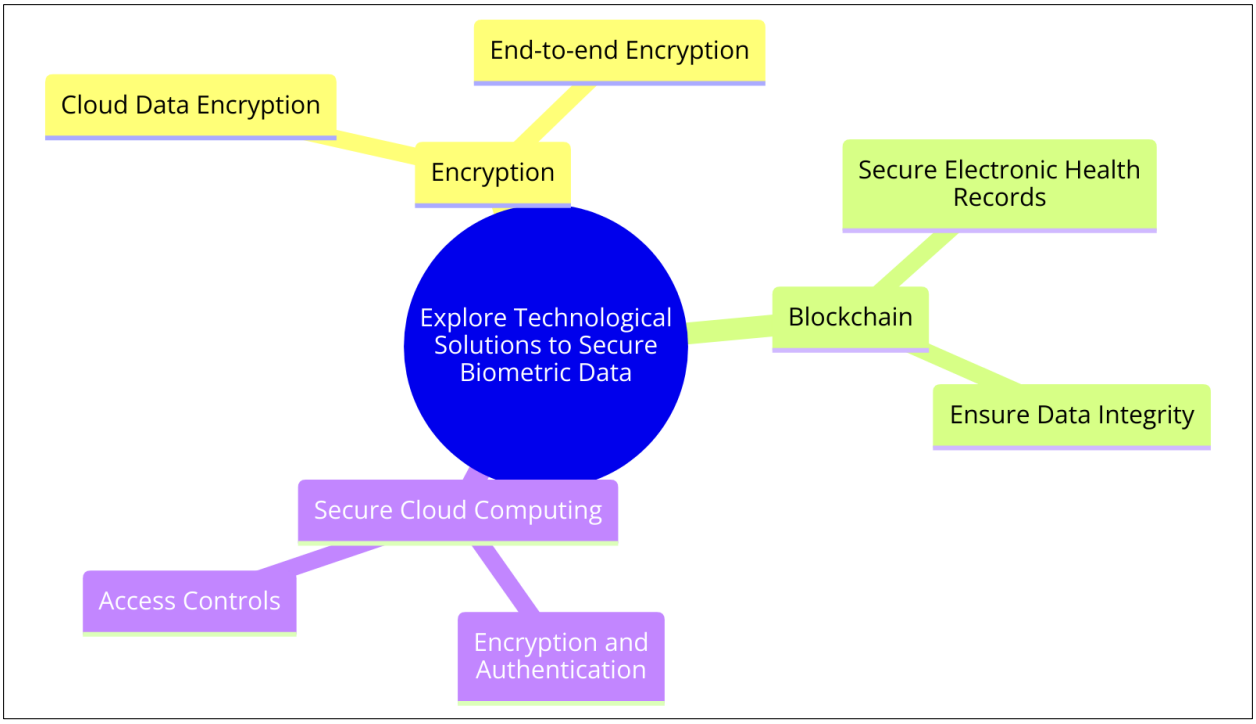


Figure 7 Exploring Technological Solutions for Biometric Data Security

5.2. Discussion on encryption, anonymization techniques, and data access controls

A discussion on encryption, anonymization techniques, and data access controls is crucial for enhancing the security and privacy of biometric data in various applications. Ijiga et al. (2024) explore ethical considerations in implementing generative AI for healthcare supply chain optimization, highlighting the importance of encryption and access controls to protect sensitive healthcare information. Rathore, Ahmad, Paul, and Wan (2016) discuss real-time medical emergency response systems, emphasizing the role of encryption and anonymization techniques in ensuring the privacy and security of health data transmitted over the Internet of Things (IoT). Yew et al. (2020) review IoT-based real-time smart health monitoring systems, underscoring the significance of data access controls in maintaining the confidentiality and integrity of patient health data. Thus, the discussion on encryption, anonymization techniques, and

data access controls provides valuable insights into the technological measures employed to safeguard biometric data and ensure privacy and security in healthcare and other domains.

Table 5 Technological Measures for Enhancing Privacy and Security in Healthcare Applications

Source	Year	Application	Focus	Key Points
Ijiga et al.	2024	Healthcare supply chain optimization	Generative AI	Highlights the importance of encryption and access controls to protect sensitive healthcare information.
Rathore et al.	2016	Emergency response systems	Medical IoT	Discusses the role of encryption and anonymization techniques in securing health data transmitted over IoT.
Yew et al.	2020	Health monitoring systems	Smart IoT Health Monitoring	Reviews the significance of data access controls in maintaining confidentiality and integrity of patient health data.

Table 5 summarizes key research findings on the implementation of encryption, anonymization techniques, and data access controls in healthcare-related technologies. It outlines the contributions of various studies: Ijiga et al. (2024) focus on generative AI for optimizing healthcare supply chains, emphasizing the necessity of encryption and access controls. Rathore et al. (2016) discuss the application of these technologies in real-time medical emergency response systems, particularly through IoT, stressing the importance of both encryption and anonymization for data security. Lastly, Yew et al. (2020) explore smart health monitoring systems, underlining the critical role of data access controls in safeguarding patient data integrity and confidentiality. Together, these studies highlight evolving strategies to bolster data protection across different facets of healthcare technology.

5.3. Evaluation of the effectiveness and feasibility of implementing these safeguards

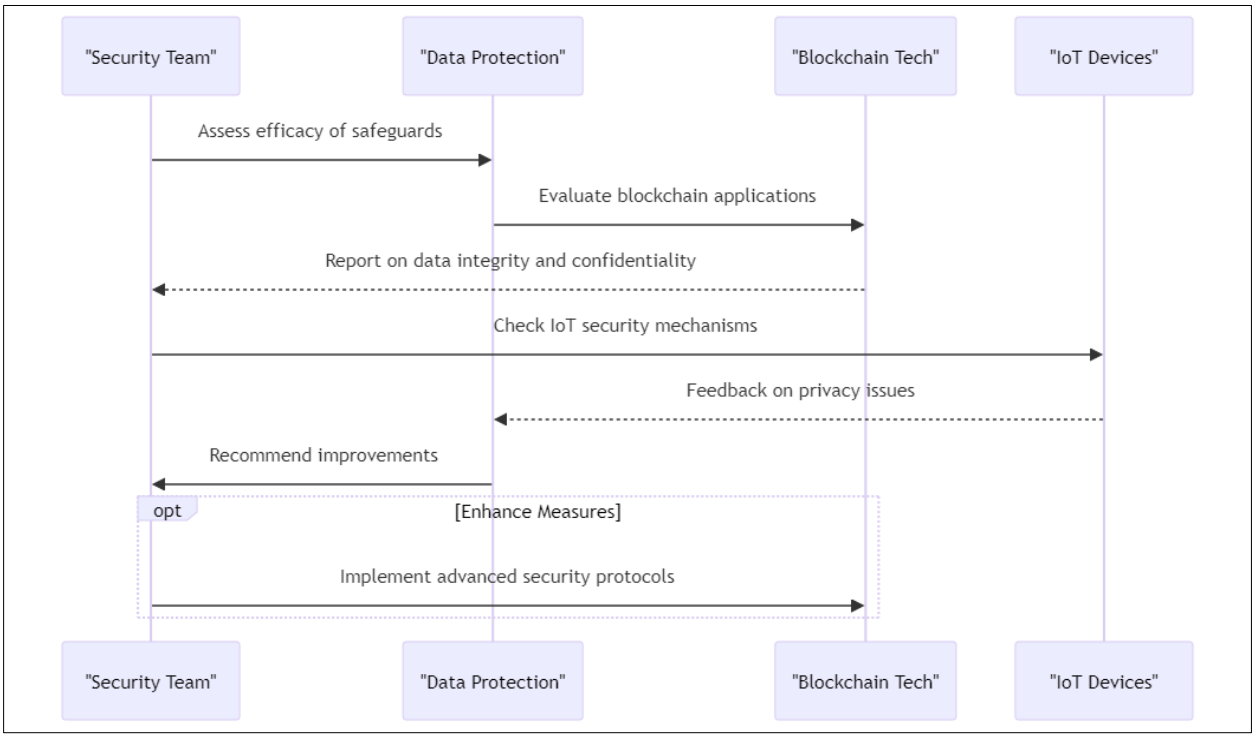


Figure 8 Evaluation of Technological Safeguards for Data Security

The evaluation of the effectiveness and feasibility of implementing technological safeguards is essential for ensuring the security and privacy of biometric data in various applications. Ijiga et al. (2024) discuss ethical considerations in implementing generative AI for healthcare supply chain optimization, emphasizing the need to assess the efficacy of technological safeguards in protecting sensitive healthcare information. Alphand, Berthier, Kovačević, Bocquet, and

Olivier (2017) examine security and privacy issues in the Internet of Things (IoT), highlighting the importance of evaluating the effectiveness of security mechanisms in IoT devices and networks to mitigate potential threats to data privacy. Wang, Zhang, and Yu (2019) propose blockchain-enabled data sharing with privacy preservation in vehicular edge computing and networks, underscoring the feasibility of leveraging blockchain technology to ensure data integrity and confidentiality while enabling secure data sharing. Thus, the evaluation of technological safeguards such as encryption, access controls, and blockchain offers insights into their effectiveness and feasibility in protecting biometric data and ensuring privacy and security in various domains, including healthcare and IoT.

Figure 8 summarizes the process of evaluating the effectiveness and feasibility of technological safeguards for biometric data security. It starts with the security team assessing the efficacy of current safeguards, followed by evaluations involving blockchain technology for data integrity and IoT device security mechanisms. Feedback on privacy issues from IoT devices is incorporated into data protection strategies. Recommendations for improvements are then relayed back to the security team. Optional enhancements include the implementation of advanced security protocols, illustrating a dynamic approach to enhancing data protection across technologies.

6. Case studies and expert analyses

6.1. Presentation of case studies illustrating real-world implications of AI-driven automation and biometric data usage

The presentation of case studies illustrating real-world implications of AI-driven automation and biometric data usage provides valuable insights into the practical applications and ethical considerations of these technologies. Ijiga et al. (2024) discuss ethical considerations in implementing generative AI for healthcare supply chain optimization, presenting case studies across India, the United Kingdom, and the United States to demonstrate the diverse challenges and opportunities in deploying AI solutions in healthcare logistics. Davenport and Ronanki (2018) explore artificial intelligence for the real world, presenting case studies of organizations leveraging AI to enhance operational efficiency, customer service, and decision-making processes, thereby showcasing the tangible benefits and potential pitfalls of AI adoption in business contexts.

Table 5 Real-World Case Studies and Ethical Implications of AI-Driven Automation and Biometric Data Usage

Source	Year	Application	Focus	Key Insights
Ijiga et al.	2024	Healthcare supply chain	Generative AI	Discusses ethical considerations and presents case studies from India, UK, and USA illustrating challenges and opportunities in healthcare logistics.
Davenport and Ronanki	2018	Business operations	AI in the Real World	Explores AI applications in business, highlighting operational efficiency and decision-making through case studies.
Tandon et al.	2020	Healthcare systems	Blockchain Technology	Conducts a review on blockchain in healthcare, detailing improvements in data security, interoperability, and patient care via case studies.
Brey	2019	Various domains	AI and Robotics Ethics	Addresses ethical issues of AI and robotics, examining societal impacts through diverse case studies.

Tandon et al (2020) conduct a systematic literature review on blockchain in healthcare, synthesizing frameworks, architectures, and case studies to illustrate the applications of blockchain technology in improving data security, interoperability, and patient care in healthcare systems. Additionally, Brey (2019) addresses the ethical aspects of artificial intelligence and robotics, presenting case studies to examine the ethical dilemmas and societal impacts arising from the deployment of AI and robotic technologies in various domains. Thus, the presentation of case studies offers a nuanced understanding of the real-world implications of AI-driven automation and biometric data usage, informing ethical decision-making and policy development in the adoption of these technologies. Table 5 provides an organized overview of various studies that explore the practical applications and ethical considerations of artificial intelligence and biometric data across different sectors. Ijiga et al. (2024) focus on the healthcare supply chain, examining generative AI's ethical considerations through case studies in India, the UK, and the USA, highlighting the diverse challenges and opportunities in healthcare logistics. Davenport and Ronanki (2018) delve into AI applications in business operations,

showcasing how organizations leverage AI to improve operational efficiency and decision-making, with real-world case studies that illustrate both benefits and potential pitfalls. Tandon et al. (2020) review blockchain technology in healthcare, emphasizing its role in enhancing data security, interoperability, and patient care through specific case studies. Lastly, Brey (2019) discusses the ethical issues of AI and robotics across various domains, providing case studies that explore the ethical dilemmas and societal impacts of these technologies. This collection of case studies offers valuable insights into the real-world implications and ethical landscapes of AI-driven technologies, aiding ethical decision-making and policy development.

6.2. Incorporation of expert analyses providing insights into the challenges and opportunities presented by these technologies

Incorporating expert analyses providing insights into the challenges and opportunities presented by AI-driven automation and biometric data usage enriches the discourse on the ethical implications and societal impacts of these technologies. Ijiga et al. (2024) explore ethical considerations in implementing generative AI for healthcare supply chain optimization, offering expert analyses on the ethical dilemmas and regulatory challenges associated with AI deployment in healthcare logistics across different countries. Ford (2015) discusses the rise of automation and its implications for mass unemployment, providing expert analysis on the socio-economic challenges posed by AI-driven automation in various industries. Mahalakshmi et al (2022) examines artificial intelligence and machine learning in financial services, presenting expert insights on the opportunities and risks of AI adoption in transforming financial markets and services. Additionally, Yang, Liu, Chen, and Tong (2018) introduce federated machine learning, providing expert analysis on the concept and applications of distributed machine learning techniques in addressing privacy and scalability concerns in AI systems. Thus, the incorporation of expert analyses enhances understanding of the multifaceted challenges and opportunities associated with AI-driven automation and biometric data usage, informing strategic decision-making and ethical considerations in the adoption and regulation of these technologies.

Table 6 Insights into AI-Driven Automation and Biometric Data Usage: Challenges and Opportunities

Source	Year	Application	Focus	Expert Insights
Ijiga et al.	2024	Healthcare logistics	Healthcare supply chain	Explores ethical dilemmas and regulatory challenges in AI deployment in healthcare logistics across different countries.
Ford	2015	Various industries	Automation and employment	Discusses the socio-economic challenges of mass unemployment due to AI-driven automation in various industries.
Mahalakshmi et al	2022	Financial markets and services	Financial services	Presents opportunities and risks of AI in transforming financial markets and services.
Yang, Liu, Chen, and Tong	2018	Distributed AI systems	Federated machine learning	Provides analysis on privacy and scalability concerns in distributed machine learning techniques.

The table 6 consolidates expert analyses from diverse studies, illustrating the multifaceted implications of artificial intelligence in various sectors. Ijiga et al. (2024) delve into ethical dilemmas and regulatory challenges associated with deploying generative AI in healthcare logistics, across multiple countries. Ford (2015) addresses the socio-economic impacts of automation, particularly the risk of mass unemployment in various industries due to AI-driven technologies. Mahalakshmi et al. (2022) explore the transformational potential and inherent risks of AI in financial markets and services, providing a nuanced view of its effects on the sector. Lastly, Yang, Liu, Chen, and Tong (2018) discuss federated machine learning, focusing on how distributed AI techniques can tackle privacy and scalability issues. This table presents a holistic view of how AI technologies are reshaping economic, ethical, and operational landscapes across different domains.

7. Conclusion

7.1. Recapitulation of key points discussed in the review paper

In recapitulating the key points discussed in this review paper, it is evident that the integration of artificial intelligence (AI) and big data presents both opportunities and challenges, particularly in the realms of workforce displacement and

the protection of customer privacy in biometric data usage. The examination of biometric data usage highlighted its applications across various industries, emphasizing its role in enhancing security measures, improving user experience, and operational efficiencies, while also raising ethical dilemmas and privacy concerns. The discussion on AI-driven automation underscored its potential for job displacement, especially in sectors reliant on routine and repetitive tasks, necessitating proactive measures to address socio-economic challenges. Moreover, the review of ethical and regulatory frameworks emphasized the importance of updated regulations and policies to ensure the ethical use of AI and protect workers' rights, with a focus on data protection laws such as the GDPR and CCPA. Furthermore, the exploration of technological safeguards revealed promising avenues to secure biometric data and ensure privacy, including encryption, anonymization techniques, and data access controls. The presentation of case studies and expert analyses provided valuable insights into the real-world implications of AI-driven automation and biometric data usage, informing ethical decision-making and policy development. In conclusion, a balanced approach towards harnessing the benefits of AI and big data while safeguarding individual rights and employment security is paramount, necessitating ongoing research, stakeholder collaboration, and regulatory vigilance to navigate the evolving landscape of technology and society.

7.2. Emphasis on the importance of a balanced approach towards harnessing the benefits of AI and Big Data while safeguarding individual rights and employment security

The discussions presented in this review paper underscore the critical importance of adopting a balanced approach towards the integration of artificial intelligence (AI) and big data. While these technologies offer immense potential to revolutionize industries and improve societal outcomes, it is essential to prioritize ethical considerations and mitigate potential risks to individual rights and employment security. The dual challenges of workforce displacement and protecting customer privacy in biometric data usage necessitate proactive measures to address socio-economic disparities and safeguard personal data. Moreover, the ethical and regulatory frameworks governing AI and data usage must evolve to keep pace with technological advancements, ensuring that ethical standards are upheld, and individuals' rights are protected. Technological safeguards such as encryption and data access controls offer promising solutions to enhance data security and privacy, but their effectiveness must be continuously evaluated and updated. Furthermore, the insights gleaned from case studies and expert analyses highlight the real-world implications of AI-driven automation and biometric data usage, informing strategic decision-making and policy development. In moving forward, collaboration among stakeholders, including policymakers, industry leaders, and ethicists, is paramount to foster responsible innovation and ensure inclusive and sustainable societal progress. By striking a balance between technological advancement and ethical considerations, we can harness the benefits of AI and big data while safeguarding individual rights and employment security, paving the way for a more equitable and prosperous future.

7.3. Suggestions for future research directions and policy considerations

Building upon the insights gleaned from the discussions presented in this review paper, several suggestions for future research directions and policy considerations emerge. Firstly, there is a need for continued research to explore the socio-economic impacts of AI-driven automation, particularly in vulnerable sectors facing job displacement. Understanding the nuanced dynamics of workforce transition and identifying effective strategies for reskilling and upskilling will be crucial for mitigating adverse effects and fostering inclusive growth.

Secondly, research efforts should focus on advancing technological solutions for enhancing data security and privacy, especially in the context of biometric data usage. Continued innovation in encryption, anonymization techniques, and decentralized data architectures will be essential to address evolving threats and ensure individuals' rights are protected in an increasingly digitized world.

Moreover, policymakers must prioritize the development of updated regulatory frameworks to govern AI and big data usage effectively. This includes enhancing existing data protection laws, such as the GDPR and CCPA, to address emerging challenges and promote responsible AI deployment. Additionally, regulatory bodies should collaborate with industry stakeholders and civil society to develop ethical guidelines and best practices for AI development and deployment.

Furthermore, interdisciplinary collaboration between experts from fields such as ethics, law, technology, and social sciences is essential to inform evidence-based policymaking and ethical decision-making in the realm of AI and big data. By fostering dialogue and knowledge exchange among diverse stakeholders, policymakers can develop holistic approaches that balance technological innovation with ethical considerations and societal impacts.

Lastly, there is a need for ongoing monitoring and evaluation of AI applications and data usage practices to ensure compliance with regulatory standards and ethical norms. This requires robust mechanisms for auditing and

accountability, as well as transparent communication between organizations and the public regarding data practices and potential risks.

Future research and policy efforts should prioritize addressing the socio-economic impacts of AI-driven automation, advancing technological safeguards for data security and privacy, updating regulatory frameworks to ensure ethical AI deployment, promoting interdisciplinary collaboration, and fostering transparency and accountability in AI governance. By addressing these priorities, we can navigate the complex challenges and opportunities presented by AI and big data while advancing towards a more ethical, inclusive, and sustainable future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Acemoglu, D., & Restrepo, P. (2018). Artificial Intelligence, Automation, and Work. NBER Working Paper, (24196).

[2] Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Privacy Enhancing Technologies (pp. 36-58). Springer.

[3] Alphand, O., Berthier, R., Kovačević, A., Bocquet, M., & Olivier, C. (2017). Security and privacy in the Internet of Things: Current status and open issues. IEEE Access, 5, 19293-19326.

[4] Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 82, 103748.

[5] Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.

[6] Chen, H., & Chiu, C. (2018). Data security and privacy protection issues in cloud computing. International Journal of Information Management, 48, 193-202.

[7] Colmenares-Quintero, R. F., Quiroga-Parra, D. J., Rojas, N., Stansfield, K. E., & Colmenares-Quintero, J. C. (2021). Big Data analytics in Smart Grids for renewable energy networks: Systematic review of information and communication technology tools. Cogent Engineering, 8(1), 1935410.

[8] Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. Harvard Business Review, 96(1), 108-116.

[9] Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine (pp. 184-193). IEEE.

[10] Durneva, P., Cousins, K., & Chen, M. (2020). The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review. Journal of medical Internet research, 22(7), e18619.

[11] Ford, M. (2015). Rise of the Robots: Technology and the Threat of Mass Unemployment. Basic Books.

[12] Ge, M., Bangui, H., & Buhnova, B. (2018). Big data for internet of things: a survey. Future generation computer systems, 87, 601-614.

[13] Hei, X., Du, X., Hei, X., & Du, X. (2013). Conclusion and Future Directions. Security for Wireless Implantable Medical Devices, 37-41.

[14] Idoko, I. P., Ijiga, O. M., Agbo, D. O., Abutu, E. P., Ezebuka, C. I., & Umama, E. E. (2024). Comparative analysis of Internet of Things (IOT) implementation: A case study of Ghana and the USA-vision, architectural elements, and future directions. World Journal of Advanced Engineering Technology and Sciences, 11(1), 180-199.

[15] Idoko, I. P., Ijiga, O. M., Akoh, O., Agbo, D. O., Ugbane, S. I., & Umama, E. E. (2024). Empowering sustainable power generation: The vital role of power electronics in California's renewable energy transformation. World Journal of Advanced Engineering Technology and Sciences, 11(1), 274-293.

[16] Idoko, I. P., Ijiga, A. C., Peace, A. E., Agbo, D. O., Harry, K. D., Ezebuka, C. I., & Ukatu, I. E. (2024). Technological innovations in mitigating winter health challenges in New York City, USA. International Journal of Science and Research Archive, 11(1), 535-551.

[17] Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Ugbane, S. I., Akoh, O., & Odeyemi, M. O. (2024). Exploring the potential of Elon Musk's proposed quantum AI: A comprehensive analysis and implications. Global Journal of Engineering and Technology Advances, 18(3), 048-065.

[18] Idoko, I. P., Ijiga, O. M., Kimberly, D. H., Chijioke, C. E., Ukatu, I. E., & Abutu, P. E. (2024). Renewable energy policies: A comparative analysis of Nigeria and the USA. World Journal of Advanced Research and Reviews, 21(01), 888-913.

[19] Ijiga, A. C., Peace, A. E., Idoko, I. P., Agbo, D. O., Harry, K. D., Ezebuka, C. I., & Ukatu, I. E. (2024). Ethical considerations in implementing generative AI for healthcare supply chain optimization: A cross-country analysis across India, the United Kingdom, and the United States of America. International Journal of Biological and Pharmaceutical Sciences Archive, 7(01), 048-063.

[20] Ijiga, O. M., Idoko, I. P., Enyejo, L. A., Akoh, O., & Ileanaju, S. (2024). Harmonizing the voices of AI: Exploring generative music models, voice cloning, and voice transfer for creative expression.

[21] Kindt, E. J. (2013). Privacy and data protection issues of biometric applications. In A Comparative Legal Analysis (Vol. 12). Springer.

[22] Kühn, S. (2019). 1 Global employment and social trends. World Employment and Social Outlook, 2019(1), 5-24.

[23] Kaur, P., Kumar, N., & Singh, M. (2023). Biometric cryptosystems: a comprehensive survey. Multimedia Tools and Applications, 82(11), 16635-16690.

[24] Leopold, T. A., Ratcheva, V., & Zahidi, S. (2018, September). The future of jobs report 2018. In World Economic Forum (Vol. 2).

[25] Lien, C. W., & Vhaduri, S. (2023). Challenges and opportunities of biometric user authentication in the age of iot: A survey. ACM Computing Surveys, 56(1), 1-37.

[26] Mahalakshmi, V., Kulkarni, N., Kumar, K. P., Kumar, K. S., Sree, D. N., & Durga, S. (2022). The role of implementing artificial intelligence and machine learning technologies in the financial services industry for creating competitive intelligence. Materials Today: Proceedings, 56, 2252-2255.

[27] Manso, L. J., & El-Saadany, E. F. (2012). Recent advances in renewable energy integration: A review. IEEE Journal of Emerging and Selected Topics in Power Electronics, 1(3), 139-152.

[28] Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., ... & Sanghvi, S. (2017). Jobs lost, jobs gained: Workforce transitions in a time of automation. McKinsey Global Institute, 150(1), 1-148.

[29] Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., & Ko, R. (2017). Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages. McKinsey Global Institute.

[30] Meden, B., Rot, P., Terhörst, P., Damer, N., Kuijper, A., Scheirer, W. J., ... & Štruc, V. (2021). Privacy–enhancing face biometrics: A comprehensive survey. IEEE Transactions on Information Forensics and Security, 16, 4147-4183.

[31] Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., & Busch, C. (2022). An overview of privacy-enhancing technologies in biometric recognition. arXiv preprint arXiv:2206.10465.

[32] Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: Current and foreseeable issues in biomedical contexts. Science and Engineering Ethics, 22(2), 303-341.

[33] Rathore, M. M., Ahmad, A., Paul, A., & Wan, J. (2016). Real-time medical emergency response system: Exploiting IoT and big data for public health. IEEE Communications Magazine, 54(9), 121-127.

[34] Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE access, 7, 5994-6009.

[35] Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values. Computer Law & Security Review, 45, 105661.

[36] Tandon, A., Dhir, A., Islam, A. N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290.

[37] Tarisayi, K. S. (2024, March). Strategic leadership for responsible artificial intelligence adoption in higher education. In CTE Workshop Proceedings (Vol. 11, pp. 4-14).

[38] Townsend, L., & Wallace, C. (2017). The ethics of using social media data in research: A new framework. In The ethics of online research (pp. 189-207). Emerald Publishing Limited.

[39] Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI?. European Papers-A Journal on Law and Integration, 2020(2), 1087-1097.

[40] Wang, S., Zhang, Y., & Yu, F. R. (2019). Blockchain-enabled data sharing with privacy preservation in vehicular edge computing and networks. IEEE Network, 33(6), 94-100.

[41] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2018). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.

[42] Yew, H. T., Ng, M. F., Ping, S. Z., Chung, S. K., Chekima, A., & Dargham, J. A. (2020, February). Iot based real-time remote patient monitoring system. In 2020 16th IEEE international colloquium on signal processing & its applications (CSPA) (pp. 176-179). IEEE.