Role of Artificial Intelligence in Data Protection for Digital Asset Systems: A Review of Recent Development

Mustafa Ababneh [1], Ayat Aljarrah [1]

[1] *Department of Robotics and Artificial Intelligence, Faculty of Science and Information Technology, Jadara University, Irbid, Jordan*

***Abstract* – AI integration in digital assets and data protection is revolutionizing asset management. Proper AI applications can enhance security, but regulation must balance innovation and misuse, requiring a thorough understanding of technology. Data protection safeguards sensitive data from loss, alteration, or corruption, ensuring compliance with legal and regulatory obligations. It involves business information procedures and data protection mechanisms, particularly in the financial industry. Restricting access to digital asset data is crucial. This paper systematically reviews the recent role of AI in data protection for digital asset systems. Recent studies have reported enhanced algorithms for data protection in digital assets, focusing on transactions, markets, surveillance, and infrastructure assets. Robust algorithms in the digital asset market improve data protection and address issues with traditional crowdfunding. Token financing is a new strategy aimed at solving these issues. However, startups often lack knowledge about risk when choosing new token financing options. In the future, AI may be able to predict potential threats or vulnerabilities to digital assets through data protection trends and patterns. This would allow proactive data protection measures rather than just reactive ones. It will enhance digital asset systems' functionality and accuracy.**

***Keywords* – Artificial intelligence, data protection, digital assets, DAM.**

DOI: 10.18421/TEM134-76
https://doi.org/10.18421/TEM134-76

Corresponding author: Mustafa Ababneh,
Department of Robotics and Artificial Intelligence, Faculty of Science and Information Technology, Jadara University, Irbid, Jordan
Email: mu.ababneh@jadara.edu.jo

Received: 10 May 2024.
Revised: 07 September 2024.
Accepted: 07 October 2024.
Published: 27 November 2024.

1. Introduction

AI remains a significant option for data protection in digital asset systems. According to IBM's Global Artificial Intelligence (AI) Adoption Index 2022, generative AI is one of Gartner's top strategic technology trends for 2022 [1]. The global AI adoption rate has increased to 35%, up four points from 2021. However, in 2023, the percentage of businesses and organizations using AI will remain constant at roughly 55% [2]. AI is incorporated into digital asset management (DAM) systems and made available to a large user via third-party plug-ins such as Amazon Image Recognition, Cloud Vision API, Tractable, and Google Vision. Large volumes of high-quality data are necessary for AI systems to identify patterns and generate precise predictions [3], [4]. Inaccurate results and false positives might emerge from poor-quality data [5]. The massive volumes of data collection and management required for successful AI-based systems are a challenge for many businesses and organizations [3].

Hackers or cyber-attackers are increasingly focusing on private and commercial data as the fintech industry develops into a digital asset payment system and the financial sector as a whole depends increasingly on digital systems [6], [7]. Large amounts of sensitive data are gathered and processed by financial institutions [8]. This data is then used, kept, and occasionally shared with other parties. Machine learning (ML) and AI approaches have been created to manage big and complicated financial data, with the goal of preventing data breaches in fintech and other financial organizations [9].

Data privacy is a key concern since applying AI to cybersecurity solutions necessitates gathering and analyzing vast amounts of data.

Businesses are now focusing on how to preserve and secure customer data by complying with applicable legislation, such as GDPR [10]. They also pay attention to information gathered that is not shared with outside parties or utilized for any illicit reasons. When AI technology ends up in the hands of malicious parties, like cybercriminals, the potential damage increases significantly. Important concerns include the possible abuse of AI technology in digital data systems, the need for strict data protection regulations, and the lack of comprehensive regulatory frameworks [11], [12].

This review aims to systematically highlight the recent role of AI in data protection in digital asset systems. This includes the protection of privacy and confidentiality. It also aims to further the discussion and investigation of AI's potential for mitigating security threats. The importance of this review includes providing information on the recent development of AI in data protection for DAM, which can help financial institutions and organizations secure ways to optimize, manage, and change digital assets. It can enhance DAM in every way, from workflow and automation procedures to metadata management and search and discovery optimization. It is also important to strike a balance between utilizing AI's advantages and making sure that robust security measures and ethical considerations are taken into account. Asset managers around the globe are still exploring various data protection solutions to support them in securing their digital asset management for financial, public, and customer usage. Compared to traditional asset management, digital assets are safer.

Contributions to this review include providing information on recent developments and the application of AI in data protection in digital asset systems. This is because AI technology can streamline the incorporation of assets by automating security, time-saving, and money-saving processes, including digital asset labeling, classification, and description. AI-based auto-tagging features in data protection solutions can provide security and save a great deal of time by applying relevant data to individual assets using image scanning and facial recognition. The review also contributes information on current AI features and functionality in data protection in digital asset systems, which can enhance their security efficiency, promote legal frameworks, and expedite the iterative process in digital asset systems.

2. Digital Assets

Digital assets represent all materials in a digital environment that have inherent or acquisition value [13]. The idea of an asset, which was first limited to the physical world but has since extended to the virtual world, is represented by digital assets. Generally, digital assets cover everything protected digitally that delivers value to individuals or organizations with legal ownership entities [14], [15]. These resources may consist of texts, images, videos, audios, documents, reports, websites, designs, and graphics that have digital ownership records and are under the direct control of their owners. The collection of digital assets might expand to include any newly developed digital file format. Digital assets provide audio-visual representations of goods and services, making it possible for people to interact with observers and an audience at any time and place via media and Internet networks [16]. In this context, legal protection for digital assets is concerned with the security and privacy risks that the environment presents [7], [17]. These include problems with data identity, privacy, systems, economy, governance, and social effects.

2.1. Digital Asset Issues Related to AI

Advances in AI technology, particularly deep learning, have made it possible for businesses to outperform traditional methods in digital asset management [9], [18]. However, rather than allowing the machine to learn on its own, existing AI technologies are only at the point where users may instruct the machine to perform specific tasks [3]. The majority of learning activities, such as digital assets, are only appropriate for closed, static environments because they lack robustness and interpretability and are unable to meet the demands of availability, robustness, interpretability, and adaptability in an environment that is open and dynamic.

A potential learning model that can monitor the performance of several ML techniques on a variety of learning tasks is meta-learning [19]. As a result of the continued demands of digital assets, meta-data is now capable of learning new tasks far more quickly than previously [20]. Meta-learning not only significantly increases the speed and quality of neural networks or ML pipeline construction [21], but it also enables the replacement of manually designed algorithms with innovative methods that are taught through data-driven methods. As a result, auto-machine learning through meta-learning will continue to be difficult in the coming years.

AI can enhance data protection for digital assets in a variety of ways, but there are drawbacks as well. The following are some of the difficulties that businesses must overcome when incorporating AI into a DAM system: data protection and security [7], algorithm bias and fairness [22], and accuracy of keywords in auto-tagging [23], users may need to use new processes and interfaces.

2.2. Digital Asset Issues Related to Data Protection Algorithms

Table 1 presents a summary of recent studies on digital assets and their reported algorithms for data protection. Some enhanced algorithms have been recently reported in the area of data protection in digital assets, with a focus on digital asset transactions, the digital asset market, surveillance, and infrastructure assets (Table 1). The enhanced Practical Byzantine Fault Tolerance Algorithm (PBFT) consensus algorithm study shows that system nodes must concur on the same transaction request at the same time when the PBFT algorithm delivers a consensus request in the blockchain network. But when more nodes join the blockchain network, it gets harder to address the fundamental problems of scalability and adaptability to large-scale network concerns by only improving the PBFT algorithm. As a result, the system becomes less reliable, has a linear increase in communication costs, and has a decrease in consensus efficiency. The problem in the [24] study was resolved by using the grouped multilayer PBFT consensus algorithm as a result of executing hierarchical multigroup consensus using the Grouped Multilayer Practical Byzantine Fault Tolerance Algorithm (GM-PBFT) approach. The performance of blockchain-based digital asset systems, such as consensus efficiency, communication complexity, and reliability, has become a limitation as market expectations have evolved focusing on the rather small body of research on the consensus process in scenarios involving the transfer of digital assets.

The use of robust algorithms in the digital asset market has also been reported to improve data protection.

In the realm of alternative finance, token financing is a relatively new strategy that aims to solve the errors and issues with conventional crowdfunding. On the other hand, token finance development is a broad and intricate process [25].

Previous research has mostly examined the worth of virtual currency [26], [27]. The majority of startup business owners lack substantial knowledge about the risks involved when it comes to assessing and choosing new token financing [28]. As a result, a model based on the MDM and BWM algorithms is presented by [25] (Table 1) to help businesses choose the best token-financing option. The best token-financing option was found by combining MDM, BWM, and startups as samples in the suggested model. Firstly, a collection of five conceptions, 17 criteria, and three token-financing options was gathered through literature research and expert opinions. Next, the weights assigned to each level were determined using the BWM. In order to determine the best token-financing option for entrepreneurs in the digital asset market, the weights that were acquired were finally ranked. This showed the efficiency of the algorithms for digital assets and their protection.

With applications of aerial vehicles (AV), electrical power providers have significantly increased the quality and efficiency of surveillance of overhead power lines and assessments of infrastructure assets throughout the past ten years [29]. They use helicopters equipped with external gimbals housing cameras to conduct routine visual inspections to assess the condition of their electrical lines. This allows them to identify any anomalies or abnormal circumstances. The current method of extensive aerial inspection involves skilled inspectors flying in helicopters and using cameras and binoculars to examine the lines while documenting the information in a logbook [30], [31]. These manual tasks are costly and prone to human error. [32] (Table 1) offer an alternative method based on AI technologies for digitally capturing power grid assets and identifying obvious irregularities in components.

Table 1. Summary of recent studies on digital assets and its reported algorithms for data protection

Study	Issue(s) addressed	Protection	Type of Algorithm	Algorithm	Environment of Application
[24]	High levels of communication complexity and inefficient consensus-building in the transaction of digital assets	Digital asset transactions	Grouped Multilayer Practical Byzantine Fault Tolerance (GM-PBFT) Algorithm	$P_m(t) =$ $\{\arg\max\{[\tau_\Pi(t).$ $[\Pi_\Pi], j \in J_m$ 0, otherwise	Blockchain networks
[25]	The data regarding the variables influencing startups' token financing.	Digital Assets Market	Best Worst Method (BWM) and modified Delphi method (MDM) Algorithm	$\lvert w_b\text{-} a_{bj} w_j \rvert \leq Z^L, for\ all\ j$ $\lvert w_j\text{-} a_{jw} w_w \rvert \leq Z^L, for\ all\ j$ $\sum_j w_j = 1$	Crowdfunding, Tokenization
[32]	Quality and efficiency of overhead power lines	Surveillance and infrastructure assets	Digital Asset Capturing (DAC)	CNNets	Image Recognition

2.3. Digital Asset Issues Related to Blockchain

Despite significant advancements in blockchain technology, there are still difficulties and unresolved problems when it comes to blockchain and data protection. The digital environment and its assets have high transaction volumes [28] can the current real-world non-fungible token (NFT) platforms handle them? Positioned on blockchains, NFTs are distinct cryptographic tokens. Digital properties such as real estate, cryptocurrencies, databases, computer software, and painting are assigned non-reproducible attributes via NFTs [19], [33]. But the NFT systems that are available now are only starting out. Improving NFT platforms' service quality and protections is a crucial area for research and engineering in order to satisfy the high-volume requirements of upcoming digital assets.

What guidelines does data protection in digital assets need for thriving blockchain-powered digital markets and businesses? From a policy standpoint, the digital blockchain-powered market may benefit from an amalgamation of decentralization and regulation [27]. One effective, decentralized, and promising standard that collaborates with like-minded people worldwide is the decentralized autonomous organization (DAO) [34]. Transparent smart contracts are used to carry out DAOs.

Is it possible to transfer the blockchain-powered application model from digital assets to the real world directly?

These days, there are many cryptocurrencies and initial coin offerings (ICOs) that have been associated with scams [35], such as fraudulent ICOs, the OneCoin Ponzi Scheme, giveaway scams, fake websites, and pump and dump schemes [36]. This has cast doubt on the position of data protection for digital assets in the digital environment. Furthermore, the current application models powered by blockchain are unable to satisfy the demanding level of data protection in digital assets in terms of low latency and high throughput performance. Thus, a high-performance and secure blockchain-powered model is required.

Does data protection in digital assets require new consensus techniques and blockchain platforms? Consensus mechanisms, including proof of work (PoW) and proof of stake (PoS), are the cornerstone of the blockchain [37]. On the other hand, there are a number of security flaws and significant hash calculation overhead with the current consensus methods. Therefore, it is anticipated that new consensus techniques and blockchain environments will emerge for digital assets.

2.4. Digital Asset Issues Related to Identity Theft, User Data, and Privacy Threats

Greater risks regarding identity theft can arise when a user's identity is stolen, compromising their digital asset security. Phishing, devices, and customer data can all provide hackers with access to personal information. Hackers will use this strategy to pretend to be authentic users in order to access digital services.

Digital asset creation and performance are prone to privacy-compromising data processing from individuals and their environment via leakage. Personal information of users may be violated via privacy compromise, which affects protection guidelines [38]. The availability of these data on digital assets can be accessed by attackers by deducing the privacy and preferences of their targets [39]. Concerns about privacy disclosure rise when users' personal data is stored on edge devices or cloud servers. Hackers can use DDoS assaults to completely compromise cloud storage or utilize differential attacks to obtain users' private information through commonly asked queries [40].

3. Digital Asset Systems

The digital asset, digital creation, digital currency, and digital market are the four components of the digital asset system, and their combined exploitation will cause traditional data protection to change. Figure 1 shows the relationship between digital asset systems based on the literature reviewed [5], [41], [42], [43], [44]. A digital asset possesses hidden features as a prerequisite for data protection in a digital environment. Three essential features of a digital asset are value, ownership rights and potential future advantages resulting from those rights, and digital storage [45], [46]. The architecture of digital asset systems is based on digital creation. The process of creation is comparable to that of material products.

Users can complete transactions and exchanges in the digital environment using digital currency (Figure 1). As a result of the high expense of the legal currency system, authorized currency is unable to meet the metaverse's expectations.

Furthermore, authorized money is exchanged for real money (such as gold and silver), which is the same as the digital money used in the digital system [41]. Single-currency such as USD, EUR, and GBP and a multi-currency coin including stablecoin, e-money, virtual currency, central bank digital currency, cryptocurrency, and in-game currency are supported by the digital asset systems [26], [27]. These digital currencies are protected by international policies.

However, digital currencies are still very prone to continued cyberattacks using different strategies, which shows continued digital assets and data protections are needed.

The basic digital environment where individuals can exchange assets for money is called the digital market (Figure 1). The developed metaverse market must be distinct from the current digital market in order to guarantee the protection of goods and legitimate trade carried out in the digital asset system. The primary focus of the [47] discussion is computational intelligence research, which uses ML and AI techniques to automatically identify, apply, and improve strategies for adaptive automated trading in financial markets. This shows disturbances and changes in traditional financial markets and services. The advent of digital assets has caused such disruptions to traditional financial services and global financial markets that several authorities now recognize digital assets as essential to the expansion of the evolving financial landscape [48]. As interest in this emerging global industry has grown, several governments have reached out to stakeholders in the digital asset market using a variety of strategies. According to data from Statista (Table 2), more and more nations are using cryptocurrencies as a payment method.

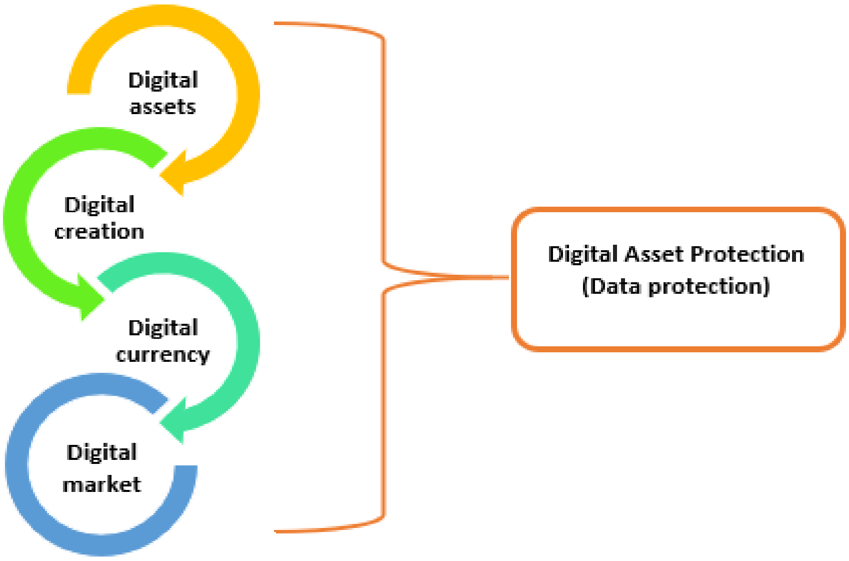

Figure 1. Shows relationship between digital asset systems based on literature.

Table 2. The percentage of participants who stated that, between 2019 and 2021, they either owned or utilized cryptocurrency across 25 nations and territories globally

Country	2019	2020	2021
	%	%	%
Nigeria	28	32	42
Thailand	23	18	31
Philippine	15	20	28
Viatnam	22	21	27
Turkey	20	16	25
Argentina	16	14	21
South Africa	16	18	21
Switzerland	10	11	16
Kenya	10	11	16
Malaysia	6	12	16
Brazil	16	11	15
Netherlands	9	10	15
Colombia	18	15	15
Czechia	10	9	15
India	7	9	14
Portugal	9	8	14
Spain	10	9	14
Chile	11	12	14
Pakistan	6	6	13
Ireland	8	10	13
United Arab Emirates	20	10	13
United States	6	6	13
Peru	15	16	13
Hong Kong	11	11	13
Greece	11	11	13

Based on Figure 1, the digital asset, digital creation, digital currency, and digital market can only function in an appropriate manner under robust and complete data protection for digital assets. The proactive approach to safeguarding digital assets, both financial and intellectual, is data protection [12]. As such, the Securities and Exchange Commission (SEC) oversees its regulation. Financial planning includes asset protection, which aids in securing assets from creditors. These techniques are intended to stop unauthorized use of property like images, videos, audio files, or software that has been granted a third-party license.

4. AI in DAM

Based AI is commonly understood to refer to "intelligent automation" [49] or "intelligent computer systems" [50]. In the past, AI was first used in 1956 to describe the process of making computer systems capable of simulating human brain activity and managing any broad cognitive function in any environment [51]. These AI-powered systems are typically divided into two categories: general AI and narrow AI [52]. Computer systems are capable of consciousness and are similar to humans in that they can generalize tasks [53].

Machine learning (ML) comprises the majority of modern AI, which describes statistical "tools" or techniques that enable computer systems to learn from data and experiences without explicit programming [9]. ML comes in three main classes: support learning, unsupervised learning, and supervised learning [54]. AI systems can examine enormous volumes of log data, spot trends, and swiftly identify anomalies or suspicious activity that might point to a possible cyberattack by utilizing ML algorithms [55], [56]. User digital spaces can become safer and more secure by using this capability to lessen breaches or unlawful access to digital assets. Organizations may respond to new threats more effectively by automating typical security operations with the help of AI-powered technologies. AI in asset management involves the application of modern technologies such as machine learning, natural language processing (NLP), cloud computing, and computer vision in the automation of processes like digital asset tagging, classification, and description [49].

An AI-powered DAM system may scan an image and tag it with relevant keywords by detecting the objects or faces it contains using a variety of different identification techniques [8]. Instead of taking weeks as it would have in the past, AI can now automatically tag thousands of digital items in a matter of hours.

AI-powered speech recognition technology can also be used to scan and automatically classify audio and video assets [57]. With the use of AI, computers can recognize and interpret speech patterns to categorize and, when necessary, translate words or entire phrases into text [58].

Data security or protection is given first priority within the DAM, and the system is commonly scalable and connects to AI-enabled infrastructure [59], [60]. Thus, choosing a solution with comprehensive analytics, reporting capabilities, and user-friendly interfaces is essential. It is crucial to specify the goals and scope of an AI-based digital asset and data protection system before application to make sure the AI tools are appropriate for the different classes of assets. Many studies have reported the application of AI in digital asset management, including data protection [5], [17], [38], [61], [62], [63]. These studies have reported applications that range from AI auto-tagging to image similarity search as well as speed, automation, and metadata management, as displayed in Figure 2. However, the AI is a two-edged blade. Cybercriminals, hackers, or malevolent threat actors may take advantage of it. They have the ability to use advanced AI algorithms to find weaknesses, plan devious phishing attacks, or even automate the creation and spread of malware [5], [53], [56].

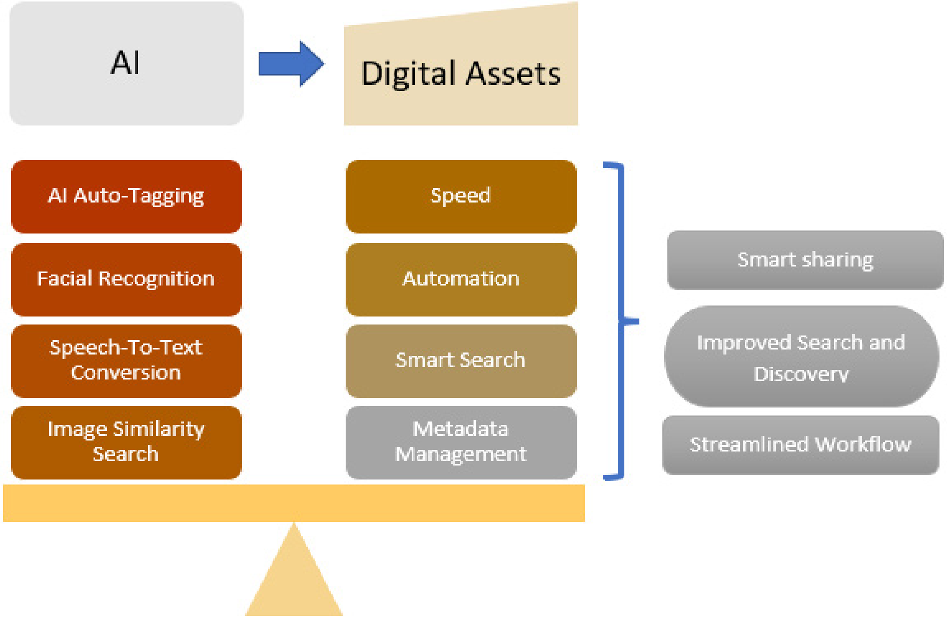

Figure 2. Application of AI in DAM and protection based on literature. Source: Current study's contribution

In a more recent DAM, systems that make use of AI can cut down on a lot of these tasks' time [8] [64]. AI has the potential to reduce employee time spent on unimportant tasks by a staggering 40 percent [60]. In fact, AI has the potential to give businesses the ability to swiftly sort, search, filter, and arrange the enormous volume of content stored in their DAM system (Figure 2).

4.1. Related Studies

Table 3 presents recent studies on the application and integration of AI into digital assets. These studies focus on digital assets that are AI-based, using a variety of methods and addressing different issues. The studies examine digital assets that cut across many nations and have significant contributions to financial systems. [10] evaluate how SPChain may be used to protect privacy [6] and comply with GDPR.

Rare digital RCURRENCY consequently appeared, as seen in buy/hold/sell assets that are limited by predetermined values [43].

AI and art can now be combined to make rapid advancements in computer vision. This may show the nature of decentralization and security features of cryptocurrencies, and tokenization of assets presents exciting opportunities for this innovative approach in AI [6]. Banking and financial sectors democratize the digital asset market, which is currently exclusive to collectors with the means and connections to secure digital currency and blockchain following digital creation. It is becoming more and more blockchain-related. Integration of AI technology into digital assets has revolutionized the digital assets industry with many applications in a variety of domains (Table 3), such as industry 4.0 [65] and FlexiChain 3.0 [66] in real estate, industry 4.0 in finance [67], and FinTech in banking [68] and finance [6].

Table 3. Recent studies on application and integration of AI in Digital assets

Study	Country	Domain	Issue(s) addressed	Type of Assets	Target Tech	Model
[66]	USA	Real estate	Challenges with massive volume of data that vehicles produce, a fast communication and secure channels are necessary	Digital assets	FlexiChain 3.0	AI-based
[7]	Indonesia	Law	Protection of digital assets and personal data	Digital assets	Metaverse	AI-based
[65]	Germany	Real estate	The anticipation of CO2 on smart cities' emissions are high	Digital assets	Industry 4.0	AI-based
[10]	Taiwan	Management	Lack of diversity in the smart contracts and comprehensive GDPR analysis	Digital assets	SPChain	AI-based
[43]	Netherlands	Trading	The buy/hold/sell assets are limited by the predetermined values.	Digital assets	RCURRENCY	AI-based
[68]	Indonesia	Banking	Lack of adequate laws and regulations protection of digital assets in Islamic financing	Digital assets	Fintech	AI-based
[67]	South Africa	Banking	The issues of information asymmetry, chatbots for customer service and helpdesk support, fraud detection, and cybersecurity.	Digital finances	Industry 4.0 in finance	AI-based
[6]	Romania	Financing	The uncertainty around the underlying value persists as this native asset class matures.	Digital assets	FinTech	AI-based

Source: Current study's contribution

5. AI in Public Data in Relation to Digital Assets

The usage of AI technology fueled by the digital data revolution has a noticeable impact on our daily lives and on public sector organizations and services. The question surrounding the use of AI to "conquer" the world of public data simultaneously in a data-driven digital economy is not only whether using AI in digital assets is justified, but rather how using AI technologies can protect the use of data in a more effective manner.

The EU stated in its AI White Book and 2018 AI strategy that a specific "European approach" is required to properly take advantage of the benefits that AI presents and overcome the accompanying challenges.

This European approach encompasses, among other things, the "anthropocentrism" of AI, the necessity of building "trust" in technology, and fundamental rights and values, such as the protection of privacy and human dignity [69]. This is corroborated by the fact that a number of EU member states consider the availability of trustworthy data to be strategically significant for the broad and safe application of AI to digital assets [70].

6. Smart Blockchain in Digital Assets

Blockchain technology offers a decentralized foundation for creating reliable information storage platforms in AI-enabled systems.

It is possible to securely control the authority, ownership, content, and fingerprinting of data in digital assets using methods like smart contracts via recording and protecting the propagation transactions based on such an AI-enabled system [38], [65]. On these platforms, data can produce associated digital assets that trace and record ownership, authority, and other rights to use information [49]. This allows data management in decentralized blockchain systems. However, there are still a lot of research problems that need to be resolved in order to safeguard digital assets, and such decentralized systems have vulnerabilities. Data integrity and privacy protection are just two of the many technological issues that must be resolved when creating digital assets for financial data. Many digital asset systems have been developed based on different architectural designs and protocols for blockchain-based DAM with the support of AI [10], [61]. However, the security of digital assets and the usability of decentralized data protection are at risk without effective measures to prevent data loss.

7. Data Protection and Data Privacy

Data protection is the process of protecting sensitive data from loss, alteration, or corruption while also having a backup plan in place in case a breach occurs, and the data becomes inoperable or inaccessible [71]. Data protection ensures that information is not tampered with, is only available for approved reasons, and complies with all applicable legal and regulatory obligations. When needed, protected data ought to be accessible and useful for the intended purpose. The procedures and tools utilized to safeguard and preserve data can be viewed as business information procedures and data protection mechanisms that work together to accomplish the main objective of maintaining the continuous availability and immutability of vital business data, particularly in the financial industry [43], [72].

Restricting access to digital asset data and systems is a crucial first step in protecting them from theft or loss. The proactive approach to wholesomeness safeguarding the intellectual and financial digital asset data is still challenging currently [73]. Nonetheless, a number of instruments and approaches, such as an offshore and domestic asset protection trust, can provide a high degree of security for cryptocurrencies and other digital assets [74], [75], [76]. Digital assets belonging to a firm may contain sensitive and private data.

Data protection is essentially a technical issue of what data privacy dictates in relation to digital assets concerning the securing of data against unauthorized access. The most recent technical approaches to data protection are AI-enabled systems that provide holistic protection against unauthorized access [7]. AI has the ability to discover, classify, and secure sensitive personal data. It is possible to train ML models to recognize data that contains sensitive content or personally identifying information [65]. Once located, this data can be secured using a variety of techniques, including encryption. AI systems can also be trained to spot unusual or suspicious behavior directed toward any digital assets, which may indicate that an individual's privacy has been violated [49], [77]. Figure 3 displays the recent two-edged application of AI in data protection. The two-edge effect shows that AI has both positive and negative effects on digital asset applications in terms of data usage and management that affect the data protections in return. AI systems learn from vast amounts of data. However, a small bias in this data could lead to an amplified effect. The complexities of the construction of ML algorithms are not always fully understood, and there is always a chance that during the development stage, inherent bias will be introduced [78]. As a result, there is no adequate transparency. Consequently, the most important barriers to the general adoption of AI are the lack of clarity surrounding the creation of algorithms and the caliber of the data utilized for training [79]. For example, if a user starts downloading large amounts of private data, the digital AI-enabled system might recognize this as possibly violating the rule. The system might then take one of two actions in response: it could stop the action or alert the system administrators to a possible breach [80], [81], [82].

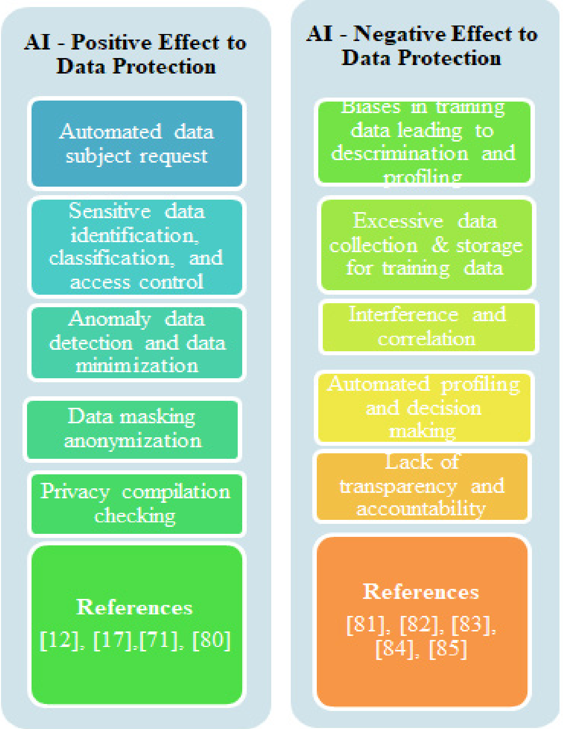
AI - Positive Effect to Data Protection
Automated data subject request
Sensitive data identification, classification, and access control
Anomaly data detection and data minimization
Data masking anonymization
Privacy compilation checking
References
[12], [17],[71], [80]
AI - Negative Effect to Data Protection
Biases in training data leading to descrimination and profiling
Excessive data collection & storage for training data
Interference and correlation
Automated profiling and decision making
Lack of transparency and accountability
References
[81], [82], [83], [84], [85]

Figure 3. Recent two edge effect application of AI in data protection. Source: Current study's contribution

Recently, there have been many concerns regarding the status of data privacy, particularly financial data and its usage in AI-enabled DAM systems. These concerns are displayed in Figure 4. These worries are related to the possibility that huge language models will use private information for training. Inadvertently providing too much personal information in a query is a possibility, albeit is not guaranteed. This information could be utilized to further train the model. Furthermore, AI-enabled digital asset systems utilized by governments possess the ability to capture face information, which permits automated profiling that may result in biased usage. It can be difficult to comprehend how these AI systems handle, store, and govern data [49]. Regulations are not keeping up with the rapid advancement of AI, which could have negative effects on people and their digital assets.

Conversely, data protection under AI-enabled digital assets is one of the most recently considered paradoxes of privacy and personalization. The term "privacy paradox" refers to a phenomenon that involves users' behavior online and characterizes the differences between users' attitudes and actions. Despite their open concern for privacy, users take virtually little action to safeguard their personal information [86], [87]. The privacy calculus is arguably the most persuasive theory that explains the privacy paradox, among others. Users use a risk-benefit analysis to determine whether to reveal personal information, with the benefits always outweighing the hazards [88]. This is caused by context reliance, absent level-headedness, lack of awareness, uncertainty, and flexibility of preferences [89].

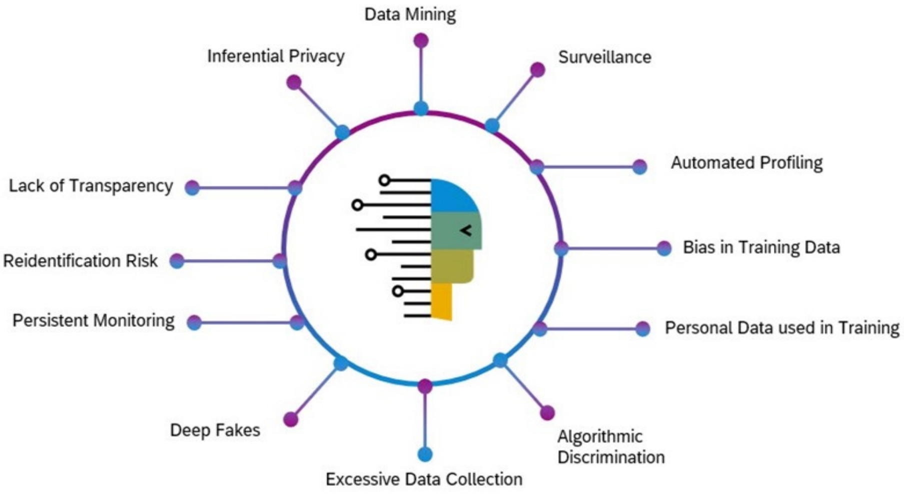

Figure 4. Concerns of AI applications in digital data privacy. Source: Current study's contribution

8. Challenges of AI Regulations on Digital Assets

Although AI applications for digital assets are still in their infancy, a wide range of businesses are now adopting them. The speed at which AI-enabled digital asset protection is adopted by businesses is developing, which makes it challenging for regulators to fully understand its ramifications and to pass legislation that quickly enough tackles emerging problems [85]. Regulators everywhere are keeping a careful eye on how technology is developing and being used in asset management, all the while being rational about how technology, particularly AI and ML, may enhance regulatory functions [83], [84].

The EU put up its first AI Act proposal in April 2021 after seeing the need for regulation of AI [69]. A uniform legal and regulatory framework for AI is what this plan aims to achieve [90].

A risk-based framework for AI regulation with four tiers is outlined in the AI Act that the European Commission has suggested [91]. AI systems that are regarded as posing an "acceptable risk" to the user's safety and rights are prohibited by the Act. Systems classified as "high risk," like those in essential infrastructure, will have stringent pre-market criteria (Figure 5). "Limited Risk" systems, such as chatbots, must explicitly notify users when they are engaging with AI, unless the situation clearly indicates otherwise (Figure 5). The majority of AI systems that pose "minimal risk" are also left to market forces; the draft law has a passive stance in this regard (Figure 5). But as AI regulation develops further, this paradigm might see revisions or adjustments.

Other challenges include difficulty and complexity in striking a balance between encouraging innovation and digital asset data protection from possible abuse.

Public engagement in regulatory discussions is difficult since there are no widely accepted standards or definitions pertaining to AI in digital assets, and non-experts frequently find it difficult to comprehend the consequences of AI systems. Last but not least, ethical issues such as protecting data privacy, openness, and justice add even more complexities to AI dominance.

9. Future Trends

With an eye toward the future, the application of AI in data protection in digital asset systems will continue to provide the dependable features and functionalities that consumers rely on. Yet, developments in AI will change DAM solutions. AI systems are becoming more powerful and dependable because of advancements in computer vision and natural language processing, which make it possible to automate more and more features related to DAM.

Future developments in AI in DAM to watch out for include improved creation and administration of metadata; AI-analytics-driven protection; AI image creation; AI prediction in DAM virtual assistants; enhanced classification and tagging; AI-driven customized content suggestions; and AI generation for project descriptions. The quality, functionality, and accuracy of DAM solutions will all be enhanced by these technical developments, increasing asset protection robustness and efficiency. AI technology will be widely used in the future to identify trends and abnormalities that could point to a cyber threat. Organizations may be able to identify and address risks faster and more precisely using this than with human assistance. This can entail removing the impacted systems from service, stopping specific activities, or even starting defenses against the attack's origin.

10. Conclusion

The advancement of AI integration into digital asset and data protection is an inexorable revolution, constrained only by our imagination. It remains a crucial component of many asset management tasks. AI keeps changing data protection and privacy environments. How AI is employed will determine the state of data protection in the future. AI can assist users in building a more secure and safe digital environment if it is properly applied. AI's dualism and double-edged characteristics emphasize the necessity of a framework of laws and rules that is constantly changing in digital assets. Regulations in the future will need to change and adapt in order to keep up with the rapid advancements in AI.

The challenge is striking a careful balance between encouraging innovation and safeguarding against misuse. A thorough grasp of the technology and its possible effects is necessary for regulation, as is a proactive approach to foreseeing and resolving ethical conundrums and security issues.

References:

[1]. Watson, I.B.M. (2022). *Global AI Adoption Index 2021*. IBM Media Relations, IBM (NYSE: IBM).

[2]. Kandepu, R. (2023). IBM FileNet P8: Evolving Traditional ECM Workflows with AI and Intelligent Automation. International Journal of Innovative Analyses and Emerging Technology, *3*(9), 23-30.

[3]. Ozdamli, F., Ababneh, M., Karagozlu, D., & Aljarrah, A. (2022). Development and Testing of Performance Scale Application as an Effective Electronic Tool to Enhance Students' Academic Achievements. *Electronics*, *11*(23), 4023.

[4]. Liang, W., Tadesse, G.A., Ho, D., Fei-Fei, L., Zaharia, M., Zhang, C. & Zou, J. (2022). Advances, challenges and opportunities in creating data for trustworthy AI. *Nature Machine Intelligence*, *4*(8), 669-677.

[5]. Wang, X. (2022). Digital Intellectual Property Protection System Based on Artificial Intelligence Algorithm. In *Proceedings of the 2022 4th International Conference on Software Engineering and Development*, 71-74.

[6]. Popescu, A.D. (2020). Financial technology (FinTech) as a driver for financial digital assets. *Ovidius University Annals, Economic Sciences Series*, *20*(2), 1055-1059.

[7]. Irianto, K.N. (2023). Digital Asset and Personal Data Protection in the Metaverse: Analyzing the Implementation of Indonesian Laws in Addressing Challenges in the Virtual Era. *Indonesian Law Journal*, *16*(2), 137-159.

[8]. Huddart, K. (2022). Artificial intelligence powered digital asset management: Current state and future potential. *Journal of Digital Media Management*, *11*(1), 6-17.

[9]. Novick, B., Mayston, D., Marcus, S., Barry, R., Fox, G., Betts, B., Pasquali, S. & Eisenmann, K. (2019). Artificial intelligence and machine learning in asset management. *Blackrock. Oct.*

[10]. Lee, W.S., John, A., Hsu, H.C. & Hsiung, A. (2022). Spchain: A smart and private blockchain-enabled framework for combining GDPR-compliant digital assets management with ai models. *IEEE Access*, *10*, 130424-130443.

[11]. Hoofnagle, C.J., Van Der Sloot, B. and Borgesius, F. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

[12]. Labadie, C. & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16-44.

[13]. Toygar, A., Rohm Jr, C.E. & Zhu, J. (2013). A new asset type: digital assets. *Journal of International Technology and Information Management*, *22*(4), 7.

[14]. Chimakurthi, V.N.S.S. (2020). Digital Asset Management: A Lowdown on Intricacies of Digital Rights and Permissions. *Global Disclosure of Economics and Business*, *9*(2), 129-140.

[15]. Busari, S.A., Suleiman, H. & Zakariyah, H. (2023). Ownership transfer of digital assets in Islamic wealth management: A juristic analysis. *Journal of Emerging Economies & Islamic Research*, *11*(3).

[16]. Steen, A., Graves, C., D'Alessandro, S. & Shi, H.X. (2023). Managing digital assets on death and disability: An examination of the determinants of digital asset planning literacy. *Australian Journal of Management*, 03128962231157005.

[17]. Timan, T. & Mann, Z. (2021). Data protection in the era of artificial intelligence: trends, existing solutions and recommendations for privacy-preserving technologies. In *The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem,* 153-175. Cham: Springer International Publishing.

[18]. Al-Okaily, M., Al-Majali, D., & Al-Okaily, A. (2023). Blockchain technology and its applications in digital accounting systems: insights from Jordanian context. *Journal of Financial Reporting and Accounting*.

[19]. Wang, Q., Li, R., Wang, Q. & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*.

[20]. Tukra, S., Lidströmer, N. & Ashrafian, H. (2020). Meta Learning and the AI Learning Process. *Artificial Intelligence in Medicine*, 1-15.

[21]. Daglarli, E. (2021). Explainable artificial intelligence (xai) approaches and deep meta-learning models for cyber-physical systems. In *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*, 42-67. IGI Global.

[22]. Sun, W., Nasraoui, O. & Shafto, P. (2020). Evolution and impact of bias in human and machine learning algorithm interaction. *Plos one*, *15*(8), e0235502.

[23]. Salminen, J., Yoganathan, V., Corporan, J., Jansen, B.J. & Jung, S.G. (2019). Machine learning approach to auto-tagging online content for content marketing efficiency: A comparative analysis between methods and content type. *Journal of Business Research*, *101*, 203-217.

[24]. Liu, J., Feng, W., Huang, M., Feng, S. & Zhang, Y. (2023). Grouped Multilayer Practical Byzantine Fault Tolerance Algorithm: A Practical Byzantine Fault Tolerance Consensus Algorithm Optimized for Digital Asset Trading Scenarios. *Sensors*, *23*(21), 8903.

[25]. Chou, C.H. & Lin, C.Y. (2022). Combining the MDM and BWM Algorithm to Determine the Optimal Crowdfunding Tokenization Solution for Digital Assets Market Startups. *Systems*, *10*(4), 87.

[26]. Nandhini, N. S., & Arumugam, P. (2023). Digital currency banking using block chain technology. *World Journal of Advanced Engineering Technology and Sciences*, *8*(1), 53-61.

[27]. Mokhinur, K., Dilshodbek, A., Khodjaev, S. & Amira, S. (2023). The Regulation and Differences between Cryptocurrency, Stablecoin, Central Bank Digital Currency, E-Money, Virtual Currency, and In-Game Currency. *Stablecoin, Central Bank Digital Currency, E-Money, Virtual Currency, and In-Game Currency.*

[28]. Schwiderowski, J., Pedersen, A.B., Jensen, J.K. & Beck, R. (2023). Value creation and capture in decentralized finance markets: Non-fungible tokens as a class of digital assets. *Electronic Markets*, *33*(1), 45.

[29]. Altenhain, C. (2023). Networked security in the colonial present: Mapping infrastructures of digital surveillance and control in São Paulo. *Security Dialogue*, *54*(1), 21-38.

[30]. Walko, C. and Maibach, M.J., (2021). Flying a helicopter with the HoloLens as head-mounted display. *Optical Engineering*, *60*(10), 103103-103103.

[31]. Dobija, K., (2023). Countering Unmanned Aerial Systems (UAS) in Military Operations. *Safety & Defense*, *9*(1), 74-82.

[32]. Valigi, E., Bolognesi, M. and Ciancarelli, F., (2019). Digital asset capturing (dac): an image recognition based algorithm supporting collection and analysis of overhead power grid assets. 25st International Conference on Electricity Distribution Madrid, 3-6 June 2019, Paper 1595.

[33]. Fairfield, J.A., (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal*, *97*, 1261.

[34]. Riaza, B. and Gnabo, J.Y., (2023). Decentralized autonomous organizations (DAOs): catalysts for enhanced market efficiency. *Finance Research Letters*, *58*, 104445.

[35]. Liebau, D. and Scheuffel, , (2019). Cryptocurrencies & initial coin offerings: are they scams?—An empirical study. *The Journal of The British Blockchain Association*, 2, 1–7.

[36]. Kutera, M., (2022). Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management and Innovation*, *18*(4), 45-77.

[37]. Wu, M., ZHU, G. and Wu, S., (2020). Improved consensus mechanism of blockchain based on proof-of-work and proof-of-stake. *Journal of Computer Applications*, *40*(8), 2274.

[38]. Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, , Nauman, A. and Kim, S.W., (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE access*, *8*, 24746-24772.

[39]. Kutschera, S., (2023). Incidental data: observation of privacy compromising data on social media platforms. *International Cybersecurity Law Review*, *4*(1), 91-114.

[40]. Teichmann, F.M.J., Sergi, B.S. and Wittmann, C., (2023). The compliance implications of a cyberattack: a distributed denial of service (DDoS) attack explored. *International Cybersecurity Law Review*, 1-8.

[41]. Treacher, M., (2018). The role of digital assets in global payments. *Journal of Payments Strategy & Systems*, *12*(1), 9-12.

[42]. Li, J., Lan, M., Tang, Y., Chen, S., Wang, F.Y. and Wei, W., (2020). A blockchain-based educational digital assets management system. *IFAC-PapersOnLine*, *53*(5), 47-52.

[43]. Hu, Y.J., van Gurp, R., Somai, A., Kooijman, H. and Rellermeyer, J.S., (2021). RCURRENCY: Live Digital Asset Trading Using a Recurrent Neural Network-based Forecasting System. *arXiv preprint arXiv:2106.06972*.

[44]. Al-Okaily, M., Alkayed, H., & Al-Okaily, A. (2024). Does XBRL adoption increase financial information transparency in digital disclosure environment? Insights from emerging markets. *International Journal of Information Management Data Insights*, *4*(1), 100228.

[45]. Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A. and Favenza, A., (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, 100142.

[46]. Trequattrini, R., Lardo, A., Cuozzo, B. and Manfredi, S., (2022). Intangible assets management and digital transformation: evidence from intellectual property rights-intensive industries. *Meditari Accountancy Research*, *30*(4), 989-1006.

[47]. Goodell, J.W., Kumar, S., Lim, W.M. and Pattnaik, D., (2021). Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. *Journal of Behavioral and Experimental Finance*, *32*, 100577.

[48]. Agarwal, J.D., Agarwal, M., Agarwal, A. and Agarwal, Y., (2021). Economics of cryptocurrencies: Artificial intelligence, blockchain, and digital currency. In *Information for Efficient Decision Making: Big Data, Blockchain and Relevance*, 331-430.

[49]. Sarker, I.H., (2022). Ai-based modeling: Techniques, applications and research issues towards automation, intelligent and smart systems. *SN Computer Science*, *3*(2), 158.

[50]. Arani, L.A., Hosseini, A., Asadi, F., Masoud, S.A. and Nazemi, E., (2018). Intelligent computer systems for multiple sclerosis diagnosis: a systematic review of reasoning techniques and methods. *Acta Informatica Medica*, *26*(4), 258.

[51]. Buchanan, B.G., (2005). A (very) brief history of artificial intelligence. *Ai Magazine*, *26*(4), 53-53.

[52]. Gautam, K., (2022). Artificial Intelligence, from Narrow to Broad to Artificial Consciousness: Some Issues and Concerns. *Liberal Stud.*, *7*, 87.

[53]. De Stefano, V., (2019). Negotiating the Algorithm": Automation, Artificial Intelligence, and Labor Protection. *Com Lab. L. & Pol'y J.*, *41*, 15.

[54]. Sharma, R., Sharma, K. and Khanna, A., (2020). Study of Supervised Learning and Unsupervised Learning. *International Journal for Research in Applied Science and Engineering Technology*, *8*(6), 588-593.

[55]. Mauri, L. and Damiani, E., (2021). Estimating degradation of machine learning data assets. *ACM Journal of Data and Information Quality (JDIQ)*, *14*(2), 1-15.

[56]. Özalp, A.N. and Albayrak, Z., (2022). Detecting Cyber Attacks with High-Frequency Features using Machine Learning Algorithms. *Acta Polytechnica Hungarica*, *19*(7), 213-233.

[57]. Elghaish, F., Chauhan, J.K., Matarneh, S., Rahimian, F. and Hosseini, M.R., (2022). Artificial intelligence-based voice assistant for BIM data management. *Automation in Construction*, *140*, 104320.

[58]. Capote-Leiva, J., Villota-Rivillas, M. and Muñoz-Ordóñez, J., (2022). Access Control System based on Voice and Facial Recognition Using Artificial Intelligence. *International Journal on Advanced Science, Engineering and Information Technology*, *12*(6), 2342-2348.

[59]. Ababneh, M., & Aljarrah, A. (2024). Cybersecurity: Malware Multi-Attack Detector on Android-Based Devices Using Deep Learning Methods. *Journal of Theoretical and Applied Information Technology*, *102*(1).

[60]. Schmitt, M., (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*, 100520.

[61]. Fradera, F., (2018). Conference Report on 'Digital Revolution: Data Protection, Artificial Intelligence, Smart Products, BlockchainTechnology and Virtual Currencies. Challenges for Law in Practice'. *European Review of Private Law*, *26*(5).

[62]. Al-Shabandar, R., Lightbody, G., Browne, F., Liu, J., Wang, H. and Zheng, H., (2019). The application of artificial intelligence in financial compliance management. In *Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing*, 1-6.

[63]. Nekit, K.H., (2023). Legal nature of a smart-contract and issues of its application in the field of digital assets. *Economics and Law*, (1 (68)), 53-61.

[64]. Yousaf, I., Youssef, M. and Goodell, J.W., (2023). Tail connectedness between artificial intelligence tokens, artificial intelligence ETFs, and traditional asset classes. *Journal of International Financial Markets, Institutions and Money*, 101929.

[65]. Weber-Lewerenz, B.C. and Traverso, M., (2023). Navigating Applied Artificial Intelligence (AI) in the Digital Era: How Smart Buildings and Smart Cities Become the Key to Sustainability. In *Artificial Intelligence and Applications*, 230-243.

[66]. Alkhodair, A., Mohanty, S. and Kougianos, E., (2023). FlexiChain 3.0: distributed ledger technology-based intelligent transportation for vehicular digital asset exchange in smart cities. *Sensors*, *23*(8), 4114.

[67]. Mhlanga, D., (2020). Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies*, *8*(3), 45.

[68]. Rahman, Y.M., Bachro, R.S., Djukardi, E.H. and Sudjana, U., 2021. Digital Asset/Property Legal protection in Sharia Banking Financing and its Role in Indonesian Economic Development. *International Journal of Criminal Justice Sciences*, *16*(2).

[69]. Mazsu, D., (2022). White Book and Strategy: AI Regulation Initiations in the European Union and Hungary. *Pro Futuro*, 119.

[70]. Najem, R., Amr, M.F., Bahnasse, A. and Talea, M., (2022). Artificial Intelligence for Digital Finance, Axes and Techniques. *Procedia Computer Science*, *203*, 633-638.

[71]. Ali, H. and Kasowaki, L., (2024). *Data Protection in the Digital Age: Safeguarding Information Assets* (No. 11743). EasyChair.

[72]. Birch, K., Cochrane, D.T. and Ward, C., (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society*, *8*(1), 20539517211017308.

[73]. Serrano, W., (2023). Smart or Intelligent Assets or Infrastructure: Technology with a Purpose. *Buildings*, *13*(1), 131.

[74]. Miric, M., Boudreau, K.J. and Jeppesen, L.B., (2019). Protecting their digital assets: The use of formal & informal appropriability strategies by App developers. *Research Policy*, *48*(8), 103738.

[75]. Jie, W. S., Tubishat, M., Alrashdan, M. T., & Ahmed, M. Z. (2023). Analytic Fraud Detection. In *2023 International Conference on Integrated Intelligence and Communication Systems,* 1-5. IEEE.

[76]. Watters, C., (2023). Digital Gold or Digital Security? Unravelling the Legal Fabric of Decentralised Digital Assets. *Commodities*, *2*(4), 355-366.

[77]. Alzboon, M. S., Bader, A. F., Abuashour, A., Alqaraleh, M. K., Zaqaibeh, B., & Al-Batah, M. (2023). The Two Sides of AI in Cybersecurity: Opportunities and Challenges. In *2023 International Conference on Intelligent Computing and Next Generation Networks,* 1-9. IEEE.

[78]. Ntoutsi, E., Fafalios, , Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.E., Ruggieri, S., Turini, F., Papadopoulos, S., Krasanakis, E. and Kompatsiaris, I., (2020). Bias in data‐driven artificial intelligence systems—An introductory survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(3), e1356.

[79]. Akter, S., McCarthy, G., Sajib, S., Michael, K., Dwivedi, Y.K., D'Ambra, J. and Shen, K.N., (2021). Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management*, *60*, 102387.

[80]. Ishii, K., (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. *AI & society*, *34*, 509-533.

[81]. Oostveen, M., (2018). Protecting individuals against the negative impact of big data: Potential and limitations of the privacy and data protection law approach. Kluwer Law International BV.

[82]. Mazurek, G. and Małagocka, K., (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.

[83]. Cheng, X., Su, L., Luo, X., Benitez, J. and Cai, S., (2022). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *31*(3), 339-363.

[84]. Marengo, F., (2023). The challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of artificial intelligence. *Information and Modeling*, *63*(21), 25-36.

[85]. Mühlhoff, R., (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data & Society*, *10*(1), 20539517231166886.

[86]. Blümel, J.H., Zaki, M. and Bohné, T., (2024). Personal touch in digital customer service: a conceptual framework of relational personalization for conversational AI. *Journal of Service Theory and Practice*, *34*(1), 33-65.

[87]. Khaksar, S.M.S., Shahmehr, F.S., Miah, S., Daim, T. and Ozdemir, D., (2024). Privacy concerns versus personalisation benefits in social robot acceptance by employees: A paradox theory—Contingency perspective. *Technological Forecasting and Social Change*, *198*, 123034.

[88]. Wang, Y., Zhu, J., Liu, R. and Jiang, Y., (2024). Enhancing recommendation acceptance: Resolving the personalization–privacy paradox in recommender systems: A privacy calculus perspective. *International Journal of Information Management*, *76*, 102755.

[89]. Chen, H.T., (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American behavioral scientist*, *62*(10), 1392-1412.

[90]. Estella, A., (2023). Trust in Artificial Intelligence: Analysis of the European Commission Proposal for a Regulation of Artificial Intelligence. *Ind. J. Global Legal Stud.*, *30*, 39.

[91]. Masseno, M.D., (2022). Brief Considerations on the Foundations of the Proposal of Artificial Intelligence Act from the European Commission. *Journal of Law and Sustainable Development*, *10*(1), 1.