



IoT Security Concerns with Non-Fungible Tokens: A Review

Ashwag Alotaibi, Huda Aldawghan, and M. M. Hafizur Rahman*

¹ Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

ARTICLE INFO

Article History

Received: 24-08-2025

Revised: 22-12-2025

Accepted: 05-01-2026

Published: 10-01-2026

Vol.2026, No.1

DOI:

<https://doi.org/10.63180/jsrm.thestap.2026.1.1>

*Corresponding author.

Email:

mhrahman@kfu.edu.sa

Orcid:

<https://orcid.org/0000001-6808-3373>

This is an open access article under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

Published by STAP Publisher.



ABSTRACT

This study summarizes the body of research on the IoT and NFTs overlap, highlighting important security concerns, the function of blockchain technology, and implications for future study and smart environment applications. IoT devices provide creative solutions that boost operational effectiveness and enhance user experiences as they spread throughout different sectors. But there are also serious drawbacks to this expansion, especially in terms of security and privacy. At the same time, NFTs unique digital assets verified by blockchain technology-have become extremely popular because of their unique features and wide range of uses. This paper carefully looks at how security frameworks in digital ecosystems may be impacted by the integration of IoT and NFTs. The results emphasize how urgently this integration must be studied further to minimize new risks and maximize the advantages of IoT and NFTs across a variety of sectors. The study intends to contribute to a more secure and effective IoT ecosystem by examining the difficulties presented by this integration. Contributing to the development of a more robust and secure IoT ecosystem is the ultimate aim of this research. This study aims to open the door for future developments that optimize the benefits between the two technologies while reducing risks by recognizing and evaluating the difficulties brought about by the integration of IoT and NFTs. Both academics and industry stakeholders navigating the rapidly changing IoT and blockchain world will find great significance in the results of this research.

Keywords: Internet of Things, Non-Fungible Tokens, Security, Blockchain

How to cite the article

Alotaibi, A., Aldawghan, H., & Rahman, M. M. H. (2026). IoT Security Concerns with Non-Fungible Tokens: A Review. STAP Journal of Security Risk Management, 2026(1), 1–30. <https://doi.org/10.63180/jsrm.thestap.2026.1.1>

1. Introduction

Connecting a wide range of devices that exchange data and improve operational efficiencies across multiple industries, the IoT has become a disruptive force. This network of linked devices promises to promote creative applications, enhance user experiences, and expedite procedures. However, the security and privacy issues surrounding the deployment of IoT devices are growing along with the number of IoT devices. Simultaneously, NFTs unique digital assets validated on the blockchain have become increasingly popular. Their special qualities make them suitable for use in a wide range of fields. One interesting approach to improving security and traceability in digital ecosystems is the combination of NFTs with IoT. This study examines the relationship between IoT and NFTs, emphasizing the security issues that result from their combination. This review seeks to shed light on the opportunities and difficulties associated with merging these two technologies by synthesizing recent research and literature, ultimately leading to a more secure and effective IoT environment.

1.1. Internet of Things

The IoT is a group of interconnected elements or devices that share information via the Internet. The main goal of the IoT is to make life easier, and the IoT works to improve and increase the efficiency of these elements or devices [1, 2]. As shown in Figure 1, the IoT facilitates many aspects of life, including Smart Homes, Healthcare Innovations, Enhanced Transportation, Agricultural Efficiency, Industrial Automation, and Environmental Monitoring [3]. For smart homes, the IoT allows us to turn.



Figure 1. How IoT Makes Life Easier.

On and off elements or devices such as lighting, air conditioning, and thermostats by giving the device commands from smartphones or by voice [4]. As for healthcare innovations, people can, for example, use a smartwatch to measure their health parameters in real-time to warn them of any potential health problems so that quick action can be taken regarding these problems [1]. Also, the IoT has a major role in enhanced transportation through smart traffic management systems that play a major role in reducing congestion and improving traffic flow, which plays a role in increasing efficiency and safety [4]. The IoT plays a major role in improving agricultural efficiency, as the farmer can, by using sensors, make decisions based on data, which increases productivity and also reduces the resources used as much as possible [1]. The IoT plays a useful role in industrial automation, where sensors are used to reduce maintenance costs by identifying abnormalities in equipment performance to be repaired before any failure occurs, which in turn improves the reduction of working time [2]. The IoT also has a major and useful role in addressing environmental issues through environmental monitoring, where sensors track environmental standards [4].

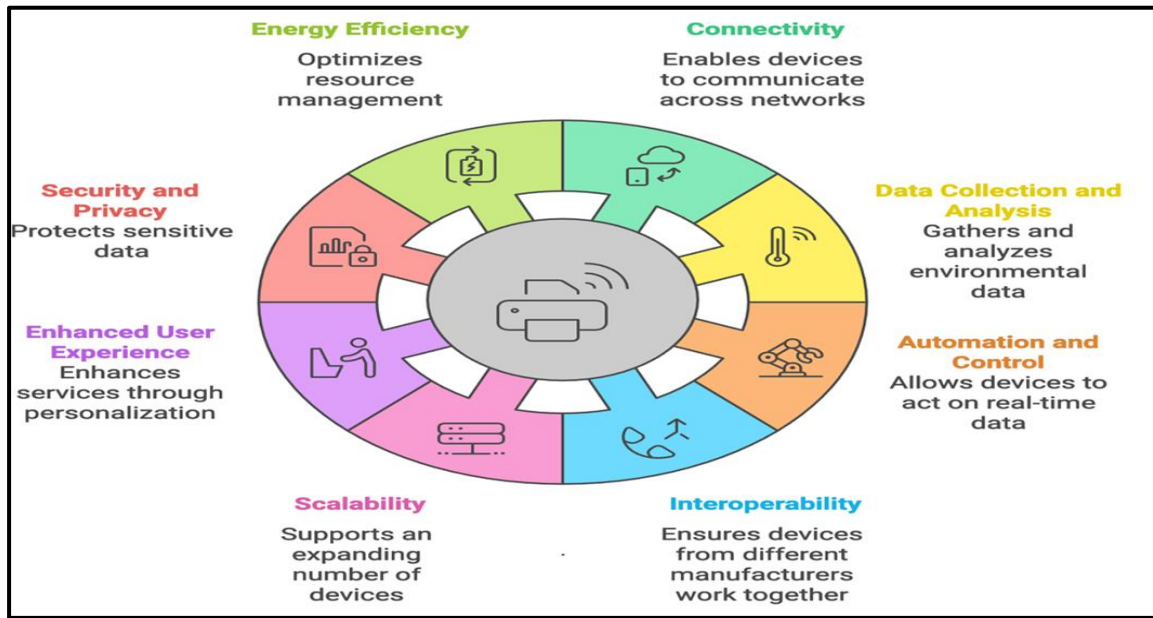


Figure 2. Key Features of IoT.

The presence of the IoT in our lives facilitates a variety of uses in different fields, as shown in Figure 2, which are connectivity, data collection and analysis, automation and control, scalability, interoperability, real-time monitoring, enhanced user experience, and security and privacy [4,5].

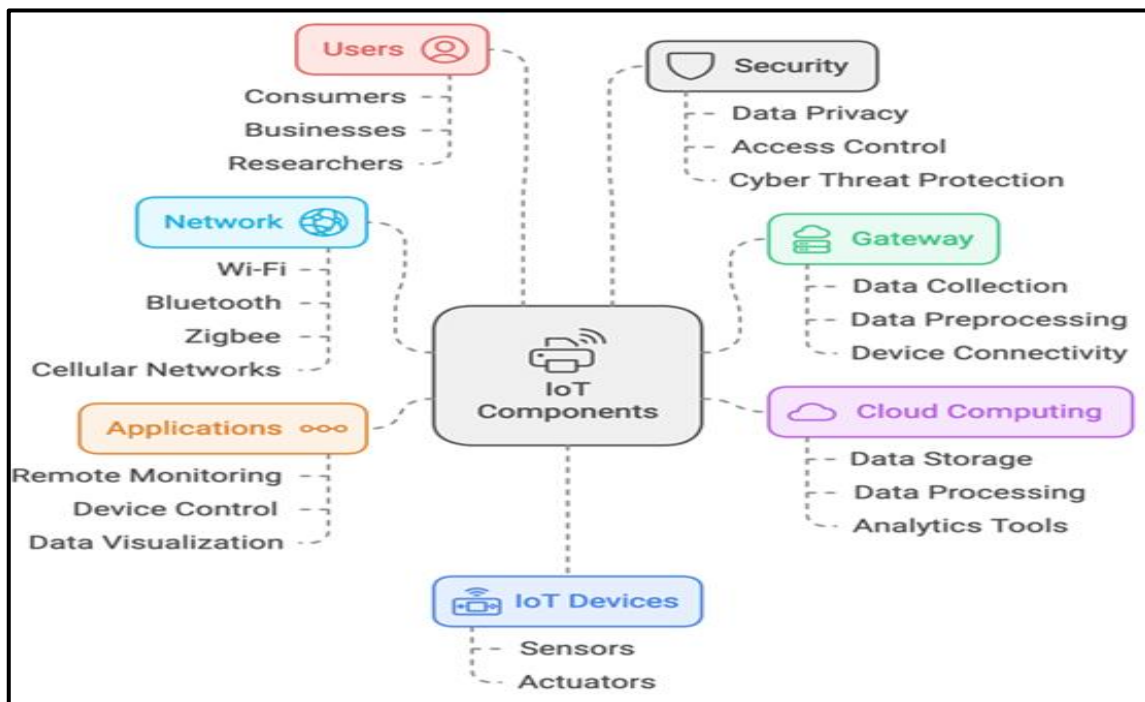


Figure 3. Key Components of IoT.

As shown in Figure 3, devices can connect, interact, and exchange data efficiently thanks to several essential components that make up the IoT. IoT devices, such as sensors that collect environmental data and actuators that take action in response to that data. Reliable data transfer is ensured by these devices' communication over many networks, including cellular, Bluetooth, and Wi-Fi. As middlemen that gather data and send it to the cloud for analysis and storage, gateways are essential. The cloud architecture is crucial for handling the enormous volumes of data collected. Applications for users operate as inter- faces between users and the IoT, enabling remote device control and monitoring. Security covers topics like data privacy and defense against online attacks. Trends like using edge computing to lower latency and integrating AI to improve data processing are becoming more and more common as IoT technology develops [5,6]. There are several significant barriers to the IoT from scaling and spreading effectively. The most significant of these barriers facing the IoT are security and privacy concerns, as many devices do not have strong enough defenses to work against these cyber-attacks, which can lead to data leakage. Another issue is scalability, as managing too many devices can lead to inefficiency and network congestion. Since different devices and protocols operate frequently, compatibility is very important and can make exchanging this information more difficult. To obtain valuable insights, there is also a great need for effective management and analytics techniques. Energy efficiency is also vital and critical for battery-powered devices that require extended operation. Last but not least, to address these new challenges, regulatory and compliance concerns must change, requiring companies to negotiate complex legal environments. For IoT technology to continue to advance, these barriers must be removed [7, 8]. With its many advantages, the IoT is revolutionizing the way we interact with technology. But to realize its full potential, the problems and challenges it faces during its implementation must be solved. To overcome these challenges and develop seamless IoT applications, continuous research and development will be essential [9].

1.2 Non-Fungible Tokens

The idea of NFTs is that they are digital identifiers that are recorded on the blockchain. These tokens are not interchangeable and cannot be modified, as they are fixed tokens. They represent unique digital assets that benefit from blockchain technology in their verification. The characteristics of NFT allow for the identification of individual assets [10]. These tokens have several characteristics, each NFT has a unique identifier that distinguishes it from the other, and this is what makes the NFT distinctive and valuable. In addition, NFTs are indivisible, meaning they cannot be divided into smaller units. Despite their rapid growth, they face many challenges, especially when integrated into the IoT [11]. In the field of cybersecurity, NFTs can be applied as they can be used to create a secure and verifiable digital identity that also enhances security against unauthorized access [12]

2. Security Vulnerabilities in IoT Devices

By linking numerous gadgets that collect and share data, the IoT has drastically changed daily life. However, there are serious security flaws brought forth by this inter connection. Figure 4 shows the main aspects of security vulnerabilities in IoT devices. IoT devices are becoming more and more popular targets for hackers as they spread throughout different industries. Their particular difficulties, weak authentication methods, insufficient data encryption, and improper software update procedures can jeopardize system integrity and user privacy. Developing strong security solutions to safeguard IoT ecosystems requires an understanding of these risks.

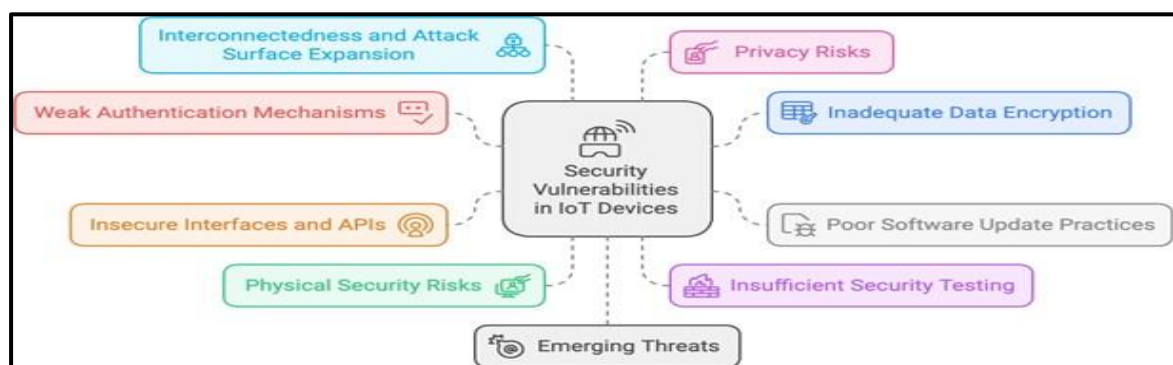


Figure 4. Security Vulnerabilities in IoT Devices

1.2 Weak Authentication Mechanisms

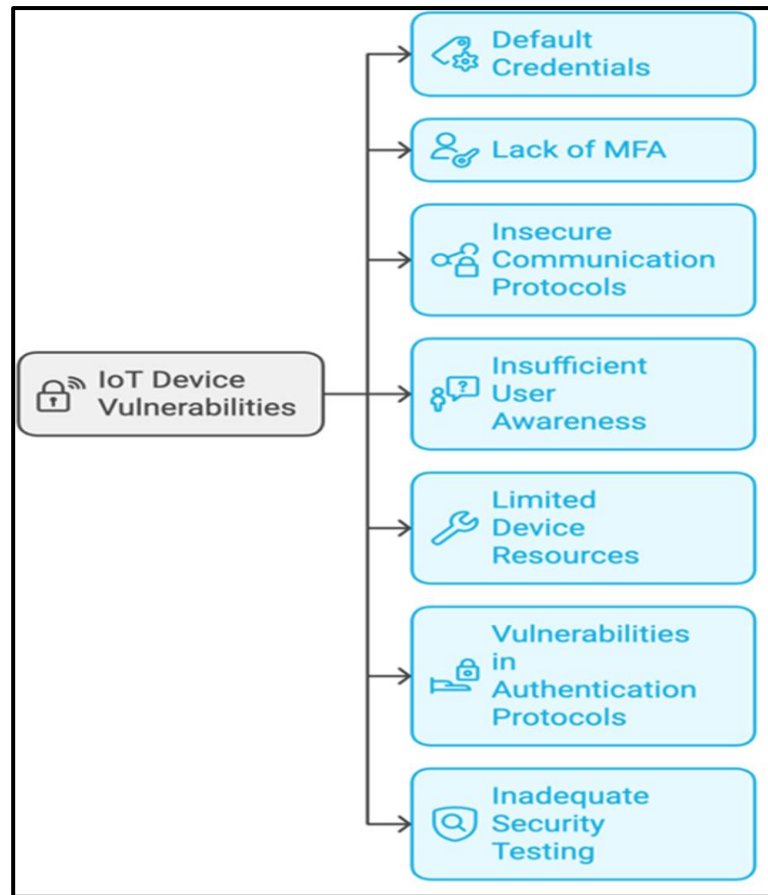


Figure 5. Key Points Regarding Weak Authentication Mechanisms.

IoT devices with weak authentication systems continue to be a serious security risk as they can be exploited and accessed by unauthorized parties. As shown in Figure 5, these are some important details about this problem. Many IoT devices come with default usernames and passwords that are well-known or simple to figure out, and users frequently forget to update them, making the devices open to intrusions. This problem worsens because most IoT devices lack MFA, which removes a crucial security measure that may stop unwanted access even if main credentials are stolen [13].

Additionally, many IoT devices use insecure communication protocols that leave authentication credentials vulnerable to interception by hackers since they don't sufficiently safeguard them during transmission. Another important consideration is user knowledge; many people are unaware of how important it is to secure their IoT devices, which causes them to be careless when it comes to altering default settings or putting in place more robust security measures. IoT devices' resource limitations also make it difficult for them to implement strong authentication techniques, which frequently leads to the adoption of less secure, simpler solutions [14].

Furthermore, certain devices can be more susceptible to exploitation because they use antiquated or badly constructed authentication methods that don't adhere to modern security requirements. Many IoT devices are rushed to market, which frequently leads to insufficient security testing, including evaluations of their authentication systems, which might overlook serious flaws. Manufacturers must work together to strengthen authentication procedures, and users must adopt better security practices to address these problems [7].

2.2 Inadequate Data Encryption

Since IoT devices handle sensitive data and are regularly the target of cyberattacks, inadequate data encryption in these devices presents serious security threats. As shown in Table 1, there are some important details about the shortcomings of data encryption in IoT devices.

Table 1. Shortcomings of Data Encryption in IoT Devices

<p>Prevalence of Unencrypted Data Transmission</p>	<p>Sensitive information is easily intercepted by hackers because many IoT devices send data over the internet without proper encryption. According to studies, 98 percent of internet communication from IoT devices is unencrypted, making it susceptible to eavesdropping and MITM assaults, among other forms of cyberattacks.</p>
<p>Weak Encryption Protocols</p>	<p>Despite the use of encryption, many IoT devices still use antiquated or ineffective encryption algorithms. This might involve using outdated algorithms that are no longer regarded as secure and are simple for hackers to crack. Reliance on such insecure encryption techniques compromises the data's overall security throughout transmission.</p>
<p>Lack of End-to-End Encryption</p>	<p>The implementation of end-to-end encryption, which guarantees that data is encrypted at the source and only decrypted at the destination, is often overlooked by IoT systems. Data breaches and illegal access are more likely to occur when this degree of protection is lacking since data might be exposed at different stages of transmission.</p>
<p>Insecure Storage of Encryption Keys</p>	<p>Encryption key protection is crucial to the security of encrypted data. But a lot of Internet of Things devices don't keep these keys safe, which leaves them vulnerable to theft or illegal access. The data may be readily decrypted by an adversary who obtains the encryption keys, making the encryption useless.</p>
<p>Challenges in Implementing Strong Encryption</p>	<p>Implementing robust encryption methods is difficult due to the resource limitations of many IoT devices, including low memory and computing capacity. Because of this, manufacturers frequently choose less secure encryption techniques that might not be sufficient. Devices may become susceptible as a result of this performance-security trade-off.</p>
<p>Inconsistent Security Standards</p>	<p>Data encryption is done inconsistently across various IoT devices due to the absence of established security standards. Because devices made by various manufacturers might not follow the same security procedures, this fragmentation can lead to vulnerabilities and make it simpler for hackers to take advantage of flaws in less secure devices.</p>

Increased Attack Surface

The possible attack surface increases with the number of IoT devices connected. Poor encryption techniques used on a large number of devices can have a compounding impact that jeopardizes the IoT ecosystem's overall security. Attackers can obtain access to additional devices within the same network by taking advantage of flaws in one device.

One major security issue that might result in serious vulnerabilities in IoT devices is inadequate data encryption. Manufacturers must work together to address these problems by putting strong encryption procedures into place, ensuring that keys are managed securely, and following established security guidelines [7,15,16].

3.2 Poor Software Update Practices

IoT devices with inadequate software update procedures have serious security flaws that hackers may take advantage of. Since many IoT devices require users to actively check for and install updates, the absence of automated updates is a significant problem. Devices running out-of-date firmware, which frequently has known vulnerabilities that are simple to attack, may result from this. Because of its annoyance or because they are unaware of its significance, users usually ignore the update procedure. Additionally, consumers may be discouraged from keeping their devices up to date due to the complicated and confusing upgrade procedure. Also, many manufacturers neglect to deliver frequent updates, especially for consumer-grade or low-cost goods, leaving them vulnerable to security risks for an extended period. Even when updates are made available, they cannot be thoroughly tested, which might lead to the introduction of new flaws or vulnerabilities that jeopardize the security and operation of the device. Furthermore, some manufacturers put more emphasis on introducing new features than fixing security flaws, which leaves devices open to abuse. Users have a substantial lack of awareness about the dangers of out-of-date firmware and the procedures required to upgrade it. The problem is made more difficult by the fact that many IoT devices rely on outdated systems that do not have the infrastructure to handle contemporary update processes. All things considered, strengthening software update procedures is essential for boosting IoT device security, requiring an emphasis on automated upgrades, streamlined procedures, extensive testing, and raised user awareness [17].

4.2 Insecure Interfaces and APIs

IoT devices with insecure interfaces and APIs are particularly vulnerable, presenting major security concerns that can result in data breaches, illegal access, and system exploitation. Because these vulnerabilities act as the conduits for communication between IoT devices and their management systems, which include mobile apps, online interfaces, and APIs, they are extremely important. These interfaces can serve as entry points for hackers, giving them the ability to alter device functions or get private data if they are not properly protected [15].

The absence of appropriate authentication and authorization procedures is one of the most frequent problems linked to insecure interfaces. Unauthorized individuals can access sensitive functions because many IoT devices lack strong authentication procedures. For instance, improper access restrictions may be included in APIs, enabling attackers to run commands or obtain data without authorization. Another major risk is presented by insecure communication methods. Since many IoT devices send data via unencrypted channels, it is simple for hackers to intercept and alter the data being transferred. A significant portion of communication from IoT devices is not encrypted, leaving it vulnerable to MITM attacks and other threats. These weaknesses can have serious consequences. Data breaches brought on by insecure APIs can have serious repercussions for individuals and companies as they provide unauthorized access to private data. Additionally, by taking advantage of weak interfaces, attackers can take over IoT devices and perhaps initiate malicious actions like DDoS attacks or alter device features. Inadequate security measures can lead to unlawful data gathering and sharing, endangering users and perhaps breaking regulations. This raises concerns about privacy issues as well [15,18].

Finally, in the context of the IoT, it is critical to address the risks linked to insecure in-terfaces and APIs. The growing usage of IoT technology necessitates the implementation of strong security measures to shield user data and devices from any

dangers. To improve the overall security posture of IoT settings and drastically lower the risks associated with these vulnerabilities, stakeholders should prioritize security in the design and implementation of IoT systems [19].

5.2 Physical Security Risks

IoT devices' physical security threats are a major worry, especially as these gadgets are incorporated more and more into vital infrastructure and daily life. Since many IoT devices are placed in easily accessible areas, they are susceptible to illegal manipulation, making device tampering one of the main hazards. Attackers can physically modify equipment, perhaps obtaining access or control that results in service interruptions or data breaches. Attackers can circumvent security measures and jeopardize the integrity of the systems they are intended to safeguard by tampering with surveillance cameras and smart locks [20].

Moreover, employing hardware Trojans, which are malicious features purposefully incorporated into equipment during production to allow attackers to see or manage them undetected; compromised devices can have dire repercussions [21]. Unauthorized access is another important factor. Attackers can alter linked systems to make them inoperable after they physically take control of IoT devices. An attacker may take control of security cameras or alarms, for instance, if they manage to infiltrate a smart home hub. This would jeopardize a house's complete security system. The lack of tamper-resistant features in many consumer-grade IoT devices makes them simple targets for physical penetration, which increases the danger. Furthermore, since IoT devices commonly send private data via wireless networks, data interception is a danger. An attacker who has physical access to a device may use techniques like eavesdropping on unencrypted communications to intercept this data, which may contain security credentials or personal information [22].

Furthermore, IoT devices are vulnerable to environmental threats since things like high humidity, harsh temperatures, and physical shocks can cause problems that hackers might take advantage of. A broken security camera, for example, could not capture important events, creating security coverage gaps that could be harmful in high-risk situations. The supply chain is also in danger since manufacturing or transportation may jeopardize the physical security of IoT devices. Before the devices even reach customers, vulnerabilities might be created, such as the possibility of malware or backdoors being installed, which could then be triggered after the device is deployed. This emphasizes how crucial supply chain integrity and safe manufacturing procedures are [23].

Additionally, a lot of IoT devices have inadequate security features; sometimes, they don't have strong physical security features like locked enclosures or alarms that warn users of tampering. Manufacturers must give physical security priority in their designs, as the lack of security measures makes it simpler for hackers to obtain access and take advantage of weaknesses. Lastly, the vulnerabilities to physical security might significantly increase if IoT devices are connected to other systems, such as smart grids or healthcare infrastructures. Critical infrastructure operations might be disrupted by a hacked IoT device, which could have wider security ramifications that impact service dependability and public safety [24].

In conclusion, IoT devices provide a variety of physical security concerns that need all-encompassing mitigating techniques. To protect against these weaknesses, organizations and people must place a high priority on physical security measures, such as secure installation procedures, tamper-resistant designs, and routine device monitoring. In an increasingly linked world, addressing these risks is crucial to guaranteeing the ongoing security and operation of IoT networks [25].

6.2 Insufficient Security Testing

One major issue that might result in vulnerabilities and possible exploitation by criminals is inadequate security testing in IoT devices. The security threats connected to IoT devices are frequently underestimated by developers. Many people overlook the significance of strong security measures in favor of user experience and functionality. This omission may result in weaknesses that attackers can quickly take advantage of [26]. This issue also discusses some of the main aspects.

First the limited scope of security testing. Many IoT devices only undergo basic security testing, emphasizing usefulness over thorough security evaluations. Because manufacturers might not be completely aware of the risks that their devices could encounter, this frequently leads to the overlooking of important vulnerabilities [7].

Additionally, lack of standardized testing protocols. IoT device security testing lacks a global standard, and in the absence of such a standard, testing procedures are inconsistent, resulting in disparate and inconsistent security standards among manufacturers. Since certain devices may go through extensive testing while others do not, this discrepancy may result in serious security flaws [27].

Moreover, lack of expertise and knowledge. Effective security testing may be limited by IoT developers' lack of specialized security knowledge. There may be serious gaps in device security as a result of many teams' inadequate training in locating and fixing security flaws [28].

Finally, poor post-release examination. Some IoT devices do not go through ongoing security evaluations after deployment. Because of this lack of continuous testing, recently found vulnerabilities might go unfixed, leaving devices vulnerable to abuse [7]. Manufacturers must implement standardized testing procedures, provide security training for developers, and adopt more stringent testing techniques. This can better protect customers and strengthen the security status of IoT devices.

7.2 Interconnectedness and Attack Surface Expansion

The attack surface is greatly increased by the interconnection of IoT devices, posing new cybersecurity risks and difficulties. The security environment becomes more complex when more devices are linked since each is a possible point of entry for cybercriminals. Many vulnerabilities introduced by interconnectedness lead to serious privacy concerns because of the huge amount of data that linked devices gather and send. Sensitive information intercepted during transit can result in potential security breaches and the exploitation of personal information [29].

Additionally, devices that are connected can let malware spread quickly throughout networks. Once malware has infected one device, it can spread to additional devices that are linked, increasing the impact of cyberattacks like DDoS [29]. Moreover, there are many different types of devices in the IoT ecosystem, each having special features and security flaws. Because of this diversity, there are more attack points, which enables adversaries to take advantage of flaws in various device types [30]. Finally, IoT devices frequently function in intricate networks, interacting with other systems and devices. Because of this interconnectedness, a flaw in one device may compromise the network because compromised devices can act as entry points to access safer systems [30].

8.2 Privacy Risks

IoT devices pose serious and complex privacy risks, mostly because of how common-place they are and the sensitive information they frequently gather. The following are some major privacy risks. First, data collection and surveillance. Large volumes of personal data are often gathered by IoT devices, and this information may be utilized for monitoring frequently without users express consent [31].

Additionally, inadequate privacy policies. IoT device privacy policies are frequently long, complex, and challenging for the typical user to understand. According to research, very few users read these policies, which may result in uninformed consent about the use and sharing of data [32]. Finally, unauthorized access and data breaches. IoT devices may be vulnerable to illegal access, which could result in data breaches. Sensitive personal data that is kept on or sent across a network can be accessed by attackers if an IoT device is compromised. Because IoT devices are interconnected, a breach in one device may result in vulnerabilities in other devices on the same network, increasing the risk [32]. Users and manufacturers must carefully evaluate the substantial privacy issues connected to IoT devices.

9.2 Emerging Threats

There are serious security and privacy vulnerabilities associated with the growing complexity and sophistication of emerging threats in IoT devices. The following are some key emerging threats. First, APTs focus on protracted cyberattacks in which an attacker enters a network and stays hidden for a long time. IoT devices are especially vulnerable to APTs because of their interconnection and frequently weak security protocols. These dangers can obtain illegal access and go unnoticed by taking advantage of flaws in IoT devices [33].

Moreover, data breaches and privacy violations. Large volumes of personal data are frequently collected by IoT devices, which makes them desirable targets for data breaches. Weak security measures can be used by attackers to obtain sensitive data without authorization, resulting in privacy violations. This risk is increased by the fact that many IoT devices lack strong encryption and authentication systems [34].

Finally, supply chain attacks. Supply chain breaches are becoming more likely as IoT devices get increasingly connected. Before devices are delivered to customers, attackers can inject vulnerabilities or harmful code by infiltrating the software supply chain or manufacturing process. Since this kind of attack takes place before the device is ever deployed, it can be difficult to identify and stop [34]. IoT devices are seriously threatened by attacks since they compromise their availability, confidentiality, and integrity. Strict security measures are necessary to defend against these threats.

In conclusion, there are significant hazards associated with the security flaws in IoT devices, which might negate the advantages of this technology. These problems, which range from inadequate encryption and insufficient authentication mechanisms to delayed software updates, highlight the pressing need for improved security procedures and practices. Addressing these vulnerabilities is crucial to protecting user data and preserving confidence in IoT applications as the IoT grows and becomes more integrated into important facets of daily life. To create a more secure IoT ecosystem, manufacturers, developers, and consumers must work together effectively.

3. NFTs Security Challenges

The inclusion of NFTs into digital ecosystems poses serious security problems as they become more popular across a range of industries. NFTs have special benefits like improving digital identification and verifying ownership, but they also come with flaws that bad actors might take advantage of. Developers, consumers, and stakeholders must comprehend these security issues to successfully reduce risks and guarantee the secure integration of NFTs with other technologies, such as the IoT. Figure 6 shows the main aspects of NFTs' security challenges.



Figure 6. NFTs Security Challenges.

1.3 Scalability

A key component of the NFT ecosystem is scalability, which immediately impacts blockchain networks' ability to manage growing transaction volumes without sacrificing efficiency. Blockchain networks may get overloaded by the many transactions generated by IoT devices, particularly during periods of high usage [35]. Furthermore, as it directly impacts their scalability, data storage is a crucial component of NFTs. The efficiency and reliability of the NFT ecosystem as a whole can be greatly impacted by the way NFT data is stored, and as NFTs usually include large and complicated data, effective on-chain storage is difficult [36].

2.3 Latency

Latency can be a problem, particularly for applications that must process data in real-time. IoT system performance may be impacted by delays introduced by blockchain transactions. Depending on network congestion, the length of time may change [37]. High latency can also negatively impact the user experience, especially in situations when fast access to data is essential. Effective data sharing may be hampered by NFT transaction delays [38]. These issues must be resolved to successfully integrate NFTs into IoT ecosystems.

3.3 Interoperability Risks

Since NFTs are developed and maintained on several blockchain systems, interoperability issues are a major worry. Cross-platform challenges occur in NFTs since they are issued on many blockchain platforms, each with its own set of rules and regulations. When trying to engage across diverse ecosystems, this variety might cause serious security problems. For instance, the smart contracts that control those NFTs could not work properly when they are moved from one blockchain to another. During the transfer procedure, this incompatibility may expose the assets to risks that might result in loss or illegal access. Therefore, the inconsistency among blockchain platforms makes NFT transactions more difficult and emphasizes the necessity of more established protocols to enable safe interactions [35, 39].

Because there are no consistent standards for its generation and transmission, standardization problems are a major obstacle in the NFT ecosystem. The implementation of distinct token standards by different blockchain platforms due to this lack of standardization makes it more difficult to design applications that are intended to support NFTs across several ecosystems. Because different techniques for confirming ownership might be exploited by bad actors, such inconsistencies can lead to security flaws. As a result, the danger of fraud and asset loss rises in the absence of a unified framework for NFT standards, highlighting the pressing need for cooperation to create standard protocols that improve security and interoperability throughout the NFT ecosystem [40, 41]. Through the mitigation of interoperability issues, the NFT ecosystem may improve user experience, increase security, and encourage wider use of NFTs across different blockchain platforms.

4.3 Environmental Concerns

The environmental issues around blockchain technology and NFTs are continuing to increase in popularity. Some of the environmental issues with NFTs have been resolved by Ethereum's switch from a PoW to a PoS consensus mechanism, which has drastically decreased its energy usage. PoW systems are known for their high energy requirements since they need a lot of processing power to protect the network and confirm transactions. Environmentalists are alarmed by this method's significant contribution to greenhouse gas emissions. Ethereum's transition to PoS has improved its scalability and efficiency while also lowering its energy needs. To support the expanding NFT industry while reducing its environmental effect, this shift is a crucial step in making blockchain technology more sustainable [42].

On blockchain networks, high transaction volumes can cause severe congestion, which harms transaction prices and performance and raises serious security issues. Users may see delays in transaction processing when the network is crowded, which can cause annoyance and confusion. Because users may try to speed up their transactions by raising fees, this congestion might jeopardize the dependability of NFT transactions and foster a competitive bidding market. Under such circumstances, the network may be vulnerable to dangers like front-running and double-spending. In the end, these problems show that blockchain networks require scalable solutions to guarantee that NFT transactions are safe and effective

even during spikes in demand [43]. Blockchain technology's environmental implications, especially about NFTs, highlight the necessity of critically analyzing network efficiency and energy usage. The blockchain community may strive toward a future in which innovation does not come at the price of the environment by emphasizing sustainability.

In conclusion, as technology advances, the security issues around NFTs must be continuously addressed due to their complexity. To promote a safe NFT ecosystem, issues including scalability, latency, interoperability hazards, and environmental concerns need to be addressed. Stakeholders may improve the robustness of NFT apps and eventually open the door for their wider adoption and integration in a safe digital environment by identifying and addressing these issues.

4. The integration of IoT and NFT

When NFTs and IoTs are combined, their properties are greatly leveraged to enhance security in digital ecosystems. This combination can improve traceability and ownership of IoT devices and their data. Given the many ways in which the two technologies can be combined, this is an emerging area of research. An example of their use is linking an IoT device to an NFT, as the role of NFTs is to create a unique digital identity for each device, which enables them to track the life cycle of the device from beginning to end. This link can identify malicious or counterfeit devices through tracking, thus facilitating the identification of only legitimate devices within the network [44]. This integration also enables secure recording of data on the blockchain, where each piece of data emitted from IoT devices is linked to an NFT, which acts as proof of authenticity and ownership. This helps ensure the integrity of the data and that it has not been tampered with during its collection from IoT devices [44, 45]. Some studies have shown that NFTs can be used to validate IoT assets in smart cities, as devices and users are verified before any data exchange occurs, which helps enhance efficiency and security in urban environments[45]. User identities are tokenized, on blockchain networks, by generating distinct contract addresses. An NFT is used to represent each user's digital identity, creating a safe and impenetrable link between the person and their cryptographic keys in IoT networks, this enables decentralized user identity management [46]. In the ever-changing world of IoT technology, the overall goal of integrating IoT and NFTs is to establish a more user-centric, transparent, and safe authentication ecosystem. Just as this integration has created improvements in the field of security, it also creates security concerns, which is what will be focused on during this research.

1.4 Blockchain technology

Blockchain technology is a digital system that securely and openly records transactions. It makes it difficult to alter or remove any data after it has been captured since it keeps it in blocks that are connected in a chain. Because there is no need for a central authority, this method fosters user trust. Blockchain has several applications, including supply smart contracts, cryptocurrency, and chain tracking [47].

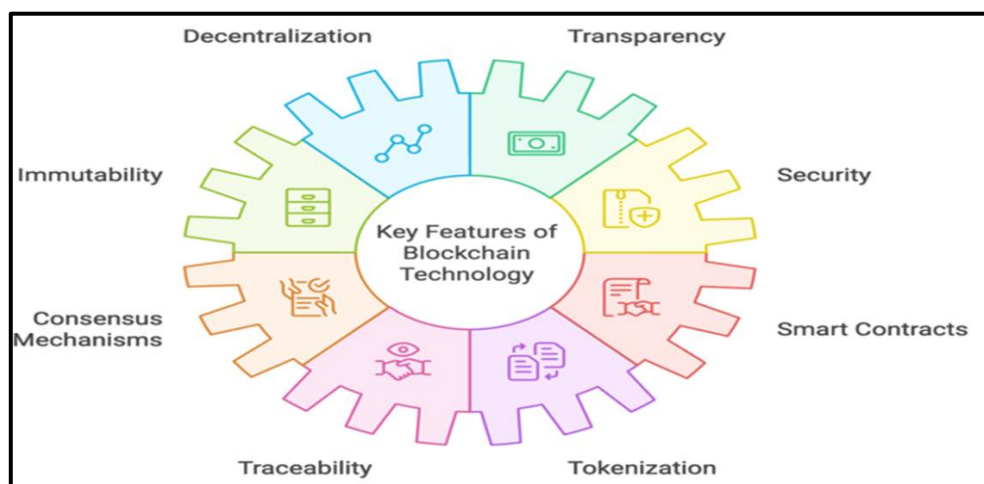


Figure 7. Key Features of Blockchain Technology.

As shown in Figure 7, there are several basic characteristics of blockchain technology, the most prominent of which are those that increase its usefulness and attractiveness. Firstly, decentralization is essential because it strengthens security, and by doing this, the chance of a single point of failure is decreased. Secondly, transparency so users' trust is increased because every transaction on a blockchain is accessible to all parties. Additionally, Immutability is if a transaction cannot be removed or changed after it has been entered into the blockchain. This creates a trustworthy record. Finally, the important feature is security, so cryptographic methods are used by blockchain to protect data from modification and unauthorized access [39, 48].

Scalability and improved security within IoT networks are at the core of the link between blockchain and IoT. To safely handle the enormous volumes of data produced by IoT devices, blockchain technology offers a decentralized and unchangeable ledger that addresses important concerns [49]. IoT devices can reduce their susceptibility to hackers and increase device trust by using blockchain technology to do away with the requirement for centralized control [50]. Additionally, the use of lightweight consensus techniques enhances scalability and throughput by facilitating effective transaction processing in IoT contexts with limited resources [49]. In addition to facilitating safe data sharing, this technological convergence makes it possible to create autonomous systems in which IoT devices may function as separate economic actors, making choices and conducting transactions on their own [50,51].

NFTs are made possible by blockchain technology, which provides the fundamental framework for their creation, ownership, and transfer. NFTs are unique digital tokens that signify ownership of certain digital. They are kept on a blockchain, which uses cryptography to guarantee their origins and authenticity. The decentralized structure of the blockchain removes the need for middlemen, improving market security and efficiency for NFT transactions. The NFT market structural features have been brought to light by recent research, which also shows how blockchain technology supports interactions and transactions in this quickly changing environment [52, 53]. All things considered, blockchain is a huge advancement in the way we handle and validate digital data.

5. Privacy Concerns

Significant privacy issues are raised by the integration of IoT devices with NFTs, which need to be resolved to safeguard user information and preserve trust in these technologies. The possibility of abuse or illegal access becomes a serious worry as IoT devices gather enormous volumes of private and sensitive data. The dynamics of privacy are further complicated by the special qualities of NFTs, which can stand in for ownership and identification. This section examines the several privacy dangers that come with IoT- NFT integration, such as data collection methods and the consequences of data breaches in a digital environment that is becoming more interconnected by the day. Figure 8 shows the main aspects of privacy concerns.

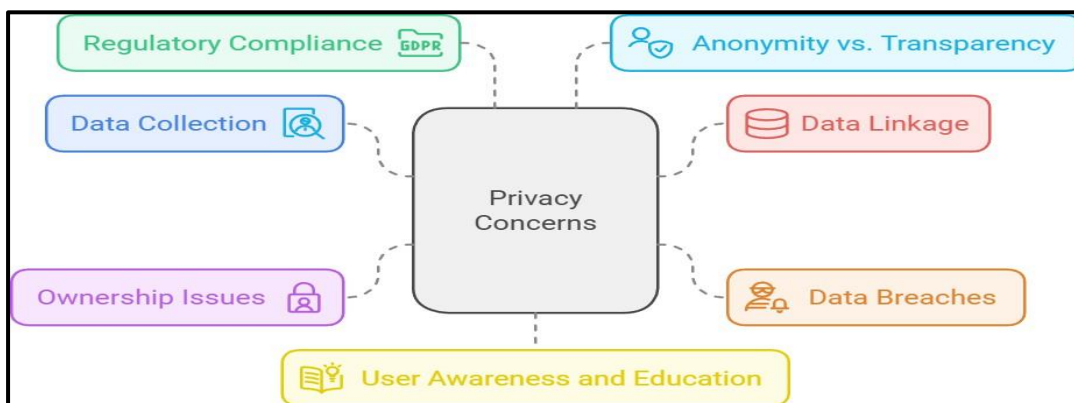


Figure 8. Main Aspects of Privacy Concerns.

5.1 Data Collection and Surveillance

Because of the nature of the data being gathered, data collection via IoT devices presents serious privacy issues. IoT devices can collect a vast array of data, including behavioral information that monitors user trends and preferences as well as personal information like names, addresses, and contact details. This can include environmental parameters from sensors and information on how users engage with their smart home equipment. Due to their ongoing operation, many IoT devices generate a steady flow of data that can be examined to uncover personal information about users [45, 54, 55].

Because IoT devices continuously gather data from their surroundings, they may unintentionally create a surveillance environment. This can result in a wide range of surveillance possibilities. Significant privacy concerns are brought up by this ongoing monitoring since personal data may be gathered without express consent [56]. Devices can, for instance, monitor activity and record conversations. Additionally, the devices' data is frequently shared with other parties, such as service providers or manufacturers, raising additional privacy concerns. Functionality may be given precedence over security by manufacturers, leading to products that enable monitoring without sufficient protection [55]. Among the malicious uses of this data are identity theft and stalking. Linking individual identities to data gathered by IoT devices carries a danger of enabling illegal tracking and profiling of people [56]. Users might not fully understand what information is being gathered and how it will be used, which could allow malicious individuals to monitor people and obtain their personal information [55].

Privacy concerns are made more difficult by the combination of NFTs and IoT data. NFTs can be connected to digital assets, and if these assets are connected to information gathered from IoT devices, it may result in the development of comprehensive user profiles. Complex issues about data ownership and governance arise when IoT data is connected to NFTs. When data is tokenized, users may no longer have control over it. Businesses can utilize this connection to learn more about user preferences and behavior, which they can then use to target ads or engage in other potentially intrusive activities. Making sure people have control over their data and are aware of how it is used is a challenge [57].

2.5 Linkage of Personal Data

There are serious privacy issues when personal information is connected among IoT devices and NFTs. The capacity to link different datasets together to create a thorough profile of a person is referred to as linkage. When combined with NFT-related data, the data generated by IoT devices can provide comprehensive insights into a user's identity, preferences, and behavior. This sets up a situation where ownership of digital assets can be linked to seemingly harmless data from common devices, potentially resulting in privacy violations [58].

This linkage could involve PII, which includes names, addresses, and sensitive data that needs to be kept confidential. IoT devices also record behavioral data, such as usage patterns from smart appliances or health and performance indicators from physical activities. When connected to NFTs, this information can help create a comprehensive profile that malicious actors could use against individuals [59].

Data linkage has significant consequences and presents issues with data ownership and privacy. Ensuring that users have control over their data is crucial. The risks of exposure rise significantly as more data becomes connected. De-anonymization and the unapproved release of personal information linked to IoT devices may result from an NFT platform hack. Furthermore, when connectivity increases, new vulnerabilities may arise. For example, attackers may use linked data to design tailored phishing attacks or other cyber threats, using precise knowledge of an individual's preferences and habits to increase the effectiveness of their efforts [40, 60].

Finally, anonymity loss is one of the privacy issues connected to data linking. Anonymity could be further compromised if unauthorized parties were able to access user data. Users might not be completely aware that holding an NFT could put them under investigation, particularly if ownership is made publicly available on a blockchain [59]. Using related information for marketing or other reasons without the user's express authorization could lead to data misuse and ethical privacy issues [61].

3.5 Data Breaches and Unauthorized Access

Data breaches and unauthorized access pose significant risks in the intersection of IoT and NFTs. IoT devices are vulnerable to a variety of cyberattacks, which can result in data breaches. For instance, malware can be used by attackers to compromise Internet of Things devices. Attackers may be able to obtain private data and maybe steal NFTs if these devices are connected to NFTs. IoT device ransomware may use special tactics adapted to the particular weaknesses of these devices [62, 63]. Furthermore, unauthorized access to private information and transactions can be made possible by MitM attacks, which can intercept communications between an IoT device and its server or between the device and an NFT marketplace. MitM attacks pose serious security threats by jeopardizing the availability, confidentiality, and integrity of data transferred between IoT devices [64]. Another issue is that because of their interconnectedness and frequently inadequate safety measures, IoT devices are vulnerable to DDoS attacks, which makes them prime targets for criminals. Overloading networks with IoT devices can interfere with services that oversee NFT transactions and perhaps allow illegal access during these outages [65].

4.5 Ownership and Control of Personal Data

In the digital era, ownership and management of personal data have grown in importance, especially with the emergence of decentralized technologies like NFTs and IoT devices. With the widespread usage of these technologies, consumers frequently encounter a complicated environment where it is difficult to define who owns what data. Many people might not be completely aware of who owns the data produced by their gadgets or how businesses utilize it. Lack of informed consent and privacy violations may result from this uncertainty. Therefore, improving privacy and trust in digital ecosystems requires defining precise rules for data ownership and making sure users are aware of their rights [44].

Table 2. Concepts of Data Ownership and Informed Consent

Data Ownership	
Ambiguity in Ownership	Users frequently lack a clear understanding of who is the owner of the data produced by IoT devices. Because users may unintentionally give up their data rights, manufacturers or service providers may take advantage of this ambiguity and cause privacy violations.
Terms of Service	IoT device terms of service sometimes include intricate legal jargon that obfuscates consumers’ rights. Many users accept these conditions without fully understanding the ramifications, such as the potential use or sharing of their data with outside parties.
Implications for Privacy	There is a greater chance of misuse when consumers do not have clear control over their data. Without the express authorization of the user, data can be accessed and shared, potentially resulting in privacy breaches.
Informed Consent	
Lack of Transparency	Data collecting procedures are opaque because IoT devices frequently function with little user input. Particularly when the data is connected to NFTs, users might not be aware of what information is being gathered, how it is kept, or who has access to it.
Complex Data Practices	Users’ comprehension of data usage and the consequence of their agreement is complicated by the complex nature of IoT data practices, such as real-time collecting and cloud storage. Unintended effects may result from this complexity, particularly when personal data is combined with NFTs
Empowering Users	Businesses must make their data-gathering procedures easily understandable to encourage informed consent. It should be possible for users to revoke their permission at any time and to opt in or out of data gathering.

As shown in Table 2, a broader understanding of the ideas of informed consent and data ownership, especially as they relate to IoT devices and NFTs. In the context of IoT and NFTs, the questions of data ownership and informed permission are

essential. Users must be fully aware of their rights about the data that their devices produce and the consequences of connecting that data to digital assets. To empower people and protect their privacy in a world that is becoming more and more data-driven, transparent procedures, user education, and strong regulatory frameworks are crucial [66–68].

5.5 Regulatory Compliance

There are several obstacles to navigating regulatory compliance in the context of IoT and NFTs, especially the GDPR and the data minimization principle. The EU's GDPR is a comprehensive data protection regulation that aims to improve individual privacy rights by regulating the collection, processing, and storage of personal data. It applies to every company that handles the personal information of citizens of the EU, including NFT platforms and IoT manufacturers [69].

Organizations are required by the GDPR's core principles of lawfulness, fairness, open-ness, purpose limitation, and data minimization to gather only the information required for certain purposes. However, following these guidelines is made more difficult by the nature of IoT devices, which frequently produce enormous volumes of data. It might be difficult to restrict data collection to that which is required because many IoT devices are constantly gathering sensitive and personal data. Furthermore, when NFTs contain identifiable information, they may carry metadata connected to personal data, which makes compliance even more difficult. The GDPR's rights for users, such as the rights to access, correction, erasure, and data portability, must also be considered. This is especially important because blockchain data is unchangeable, which may clash with the right to be forgotten [70, 71]. Organizations should use privacy by design principles, carry out frequent data audits, and inform users of their data rights to guarantee compliance. To ensure that data practices respect user privacy and enable enterprises to take advantage of IoT and NFTs, working with legal specialists may also assist in traversing the difficulties of GDPR [71].

6.5 Anonymity vs. Transparency

Blockchain technology's conflict between anonymity and transparency, especially about NFTs, brings up significant issues with user privacy, data security, and responsibility. Blockchain functions as a decentralized public ledger in which all transactions are publicly recorded and transaction histories, including NFT transfers, are accessible to everybody. Traceability is made easier by the fact that every transaction has a distinct wallet address. These wallet addresses can be connected to people through a variety of channels, including transactions or services that need identity verification, even if they don't necessarily include personal data. This openness can raise serious privacy issues because a user's whole transaction history is revealed if their wallet address is linked to their identity. Their spending habits and digital asset holdings may be made public by this exposure, which might raise concerns about user privacy and data security in the blockchain ecosystem [72].

There are substantial obstacles to anonymity in blockchain transactions, especially when researchers and data analysts apply de-anonymization techniques. By using these methods, data from several sources may be correlated, enabling the connection of blockchain activities to actual individuals. For example, users' anonymity is essentially taken away when they engage with centralized exchanges that demand identity verification because transactions may be tracked. Furthermore, public attention is frequently drawn to high-profile NFT transactions, which may result in unwelcome scrutiny or harassment. The conflict between the requirement for individual privacy and the openness of blockchain technology is highlighted by the possibility that users may want to conduct transactions without worrying about their names or financial activity being made public [73].

In the blockchain ecosystem, striking a balance between responsibility and privacy is a difficult task. On the one hand, because it promotes confidence among participants and helps avoid fraud, transaction openness is crucial for guaranteeing accountability. Because of this openness, users can confirm the legitimacy and ownership of NFTs, which is essential to preserving their integrity and worth. However, a lot of people worry about their privacy, especially in a digital world where data breaches and spying are commonplace. If people believe their names and transaction histories may be revealed, their desire to keep financial activities secret may discourage them from using blockchain technologies. Therefore, promoting the wider use of blockchain technology requires striking a balance between the advantages of openness and user privacy [74].

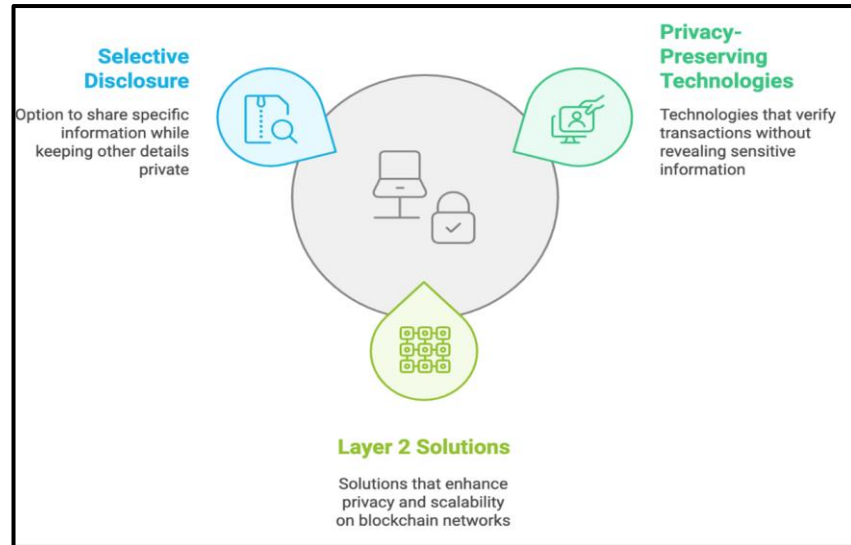


Figure 9. Enhancing Privacy and Scalability in Blockchain.

As shown in Figure 9, effective privacy solutions are becoming more and more important as blockchain technology and digital assets like NFTs develop. Blockchain's openness increases trust and accountability, but it also puts user privacy in danger. Several creative strategies have been developed to overcome these issues. These consist of privacy-preserving technologies like zero-knowledge proofs, scalability and privacy-enhancing Layer 2 solutions, and techniques for selective disclosure that give users control over their data. When combined, these solutions seek to preserve the integrity of the underlying technology while offering consumers interacting with blockchain and NFTs a more private and secure environment [75,76]. There are several potential problems associated with the conflict between anonymity and transparency in blockchain and NFTs. Building trust and promoting wider use of blockchain technology require striking a balance between the requirement for transparent transactions and users' rights to privacy. To properly address these issues as the environment changes, constant communication between technologists, users, and regulators will be essential.

7.5 User Awareness and Education

To solve the privacy problems related to IoT devices and NFTs, user education and awareness are essential. Many people don't fully comprehend these technologies' workings or the consequences of their data usage. People may not be aware of the dangers connected to the gadgets they use or the digital assets they interact with, which can result in serious vulnerabilities. For example, although consumers are typically aware of the security dangers associated with smartphones and personal computers, they frequently ignore comparable issues when it comes to IoT devices, such as wearables and smart home appliances [77].

Improving user education on the privacy settings and data management procedures related to IoT devices and NFTs is essential to reducing these threats. Users with more education are better able to decide which technologies to utilize, including knowing what kinds of data are gathered and how they are shared. In addition to helping people safeguard their data, this empowerment via knowledge also motivates them to hold service providers and manufacturers accountable for improved security procedures. A more secure digital environment where users actively participate in protecting their privacy might result from cultivating an awareness culture [77, 78].

In conclusion, it is critical to raise consumer knowledge and educate them about the privacy implications of NFTs and IoT devices. We can improve users' capacity to use these technologies responsibly and securely by providing them with the information they need.

In summary, the integration of IoT and NFTs raises complex privacy issues that need 645 thoughtful analysis and preventative action. It is impossible to ignore the concerns related to data collecting, user permission, and possible breaches as these technologies develop and integrate further. Strong privacy safeguards are essential for preserving user confidence and protecting private data. Stakeholders may reduce risks and provide an improved safe framework that enables users to use the advantages of IoT and NFTs by putting thorough privacy measures into place and following best practices.

6. Regulatory and Compliance Challenges

As the integration develops further, more regulatory and compliance issues arise. These difficulties result from the requirement to protect user information, guarantee privacy, and preserve security across networks. Rapid technological advancement frequently surpasses current regulatory frameworks, creating vulnerabilities that can be taken advantage of. Additionally, different governments enforce different laws, which makes compliance more difficult for businesses doing business internationally. The intricacies of regulatory standards, their effects on organizations, and the need for flexible regulatory policies in the quickly evolving digital landscape will all be covered in this part.

1.6 Cybersecurity Regulations

To safeguard private data and guarantee system integrity against online attacks, cybersecurity laws were created. These rules address several topics, such as incident response, data protection, and risk management procedures, which are very important for businesses using IoT devices and NFTs [79, 80]. IoT security standards and best practices are being developed and promoted by groups such as the OCF and the IIC [80].

Organizations can use the Cybersecurity Framework offered by the NIST to control and lower cybersecurity risk. The five main functionalities of this framework—Identify, Protect, Detect, Respond, and Recover—can be modified to handle particular threats related to IoT and NFTs. Additionally, many laws mandate that businesses notify authorities and impacted parties in the event of a data breach, which can be difficult for businesses that use IoT devices. Addressing security breaches involving IoT and NFTs requires the creation and upkeep of incident response procedures [10, 44].

2.6 Emerging Regulatory Bodies

The rate of IoT and NFT innovation frequently exceeds the capacity of regulatory organizations to develop efficient frameworks. Neglecting to appropriately handle new threats and technology, can result in regulations that are out-of-date or ineffectual by the time they are put into place. A vast array of parties is involved in the IoT and NFT ecosystems, including developers, manufacturers, consumers, and regulators. Since each stakeholder may have different objectives and concerns about security, privacy, and market access, balancing the interests of these diverse groups might make the regulating process more difficult [10,81].

In summary, developing a safe and reliable digital environment involves addressing the legal and compliance issues brought on by integrating IoT and NFTs. Regulations must change to keep up with technological advancements while maintaining a focus on user privacy and data security. While implementing proactive compliance measures, organizations must manage the complexities of differing rules across jurisdictions. Stakeholders may reduce risks, improve consumer confidence, and support the responsible development of cutting-edge technology in a world growing more interconnected by adopting adaptive regulatory methods.

7. Related study

This section examines earlier research on IoT security issues with non-fungible tokens by synthesizing findings from recent studies. It highlights the difficulties associated with this integration and aims to give a thorough grasp of the significant elements of that integration, with a particular emphasis on security concerns.

1.7 Selection of research papers for review

The selection of research papers is based on a systematic and rigorous process of reviewing the literature related to IoT Security Concerns with Non-Fungible Tokens to ensure the comprehensiveness of the topic. Databases that provide academic research are first searched using keywords related to the research topic. Papers are evaluated in terms of their relevance and contributions to the field. The goal is to collect a sufficient amount of literature to gather enough results to identify and fill gaps in the field. In this research review, the PRISMA 2020 flowchart was used as shown in Figure 10.

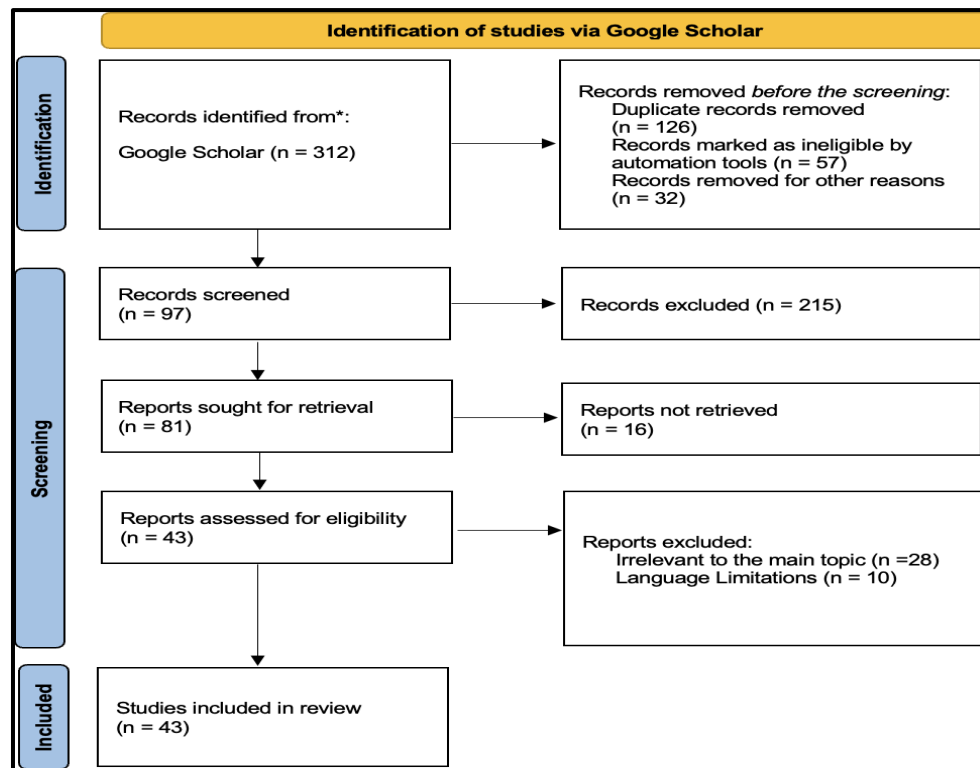


Figure 10. Selection of papers for literature review using PRISMA 2020.

2.7 Related work

Ananna and Saifuzzaman [1], introduction to IoT, including its background, salient features, benefits, and a range of uses in industries. It addresses important issues, including security and privacy, while highlighting the revolutionary effects of IoT on consumer services and decision-making processes. The paper's emphasis on fundamental ideas and current research rather than thoroughly examining cutting-edge technology or creative applications that might further propel the development of IoT is a significant drawback, perhaps creating gaps in knowledge of the most recent developments in the area.

In addition to highlighting the transformative potential of IoT in daily life, Mouha [2], introduces and offers a thorough overview of the IoT landscape, covering its definition, architecture, and essential components. It does, however, recognize important limits that may prevent the full benefits of IoT from being realized, especially regarding issues with security, privacy, interoperability, and the complexity that arises from the integration of many technologies.

Chataut et al. [3], introduce and explore the quick development and uses of IoT technology in several industries. It addresses the factors that have led to the growth of IoT devices while highlighting their revolutionary potential to improve automation and efficiency. The paper's recognition of the persistent security and privacy issues with IoT devices, which are still serious issues that can prevent broad adoption and successful integration into social structures, is a major drawback.

Kumar1 et al. [4], introduce an analysis of the IoT as technology affecting several industries, including smart cities, healthcare, and transportation. It talks about the architecture, uses, difficulties, and importance of data analytics on IoT. A significant drawback of the study is that, although it identifies several difficulties, it might not go into great detail on particular fixes or frameworks to deal with these problems, which leaves a gap in useful advice for scholars and practitioners wishing to successfully deploy IoT systems.

Elgazzar et al. [5], explore the development and significance of the IoT, emphasizing its uses in several industries. It examines the quick expansion of IoT devices and industry trends while highlighting the application of AI and advanced data analytics to improve decision-making and user experiences. The study does, however, point out several drawbacks that prevent IoT systems from reaching their full potential and scalability, notably those about data heterogeneity, device compatibility, and privacy and security issues. These difficulties make it difficult for IoT devices to integrate and work together seamlessly, leading to disjointed systems that inefficiently exchange data.

Allioui and Mourdi [6], introduce and look at how the IoT might improve operational efficiency and financial management in a variety of industries. In addition to stressing the necessity of efficient data management, interoperability, and privacy protections, it talks about the importance of IoT in enhancing decision-making, data management, and general productivity. One significant drawback of the paper is that, although it offers a thorough analysis of the body of literature already in existence and highlights present obstacles in the adoption of IoT, it might not include case studies or empirical evidence to support its assertions, which could restrict the findings' usefulness in actual situations.

To improve the security of IoT systems, Mazhar et al. [7], look at the major security issues that these systems face and how AI, more especially ML and DL techniques, can be used. It draws attention to the growing complexity of cyber threats that are difficult for conventional security measures to handle and promotes AI-driven solutions for efficient threat detection and mitigation. The study's shortcomings, however, include the difficulty of making sure that ML models can generalize effectively across various IoT contexts and adjust to changing threats, as well as a possible lack of thorough assessment of the suggested AI techniques in practical settings.

The extended lifespan of industrial components and the bigger scope of IIoT networks in comparison to consumer IoT provide special security goals, which are discussed by Serror et al. [8], along with the security potential and difficulties of the IIoT. It offers a thorough overview of current research initiatives focused on protecting IIoT deployments, including a range of risks, vulnerabilities, and suitable defenses. The paper's limitation is that, although it recognizes and talks about the unique security issues of the IIoT, it might not adequately address the threats' quick evolution and the requirement for adaptable security measures that can react to new vulnerabilities as they appear in this dynamic environment.

Laghari et al. [9], introduce and explore IoT as a technology that links objects, facilitating automation and data sharing across a range of applications, such as cloud and fog computing. It discusses security and privacy concerns while outlining IoT architecture, technology, and applications. The paper's identification of numerous unresolved research issues and challenges in the field of IoT, especially about the integration of IoT with cutting-edge technologies like 6G and the requirement for standardized architectures and protocols, is a major drawback. These issues have not been addressed in the literature as of yet.

The study offers by Taherdoost [10] a thorough analysis of NFTs, examining their possible uses, distinctive features, and surge in popularity. The author talks about how NFTs—which are distinct digital assets stored on a blockchain—can aid in preventing counterfeiting and provide new sources of income for artists. Despite their increasing importance, the study shows that there are still gaps in our knowledge of the legal, financial, and environmental ramifications of NFTs, as evidenced by the paucity of existing literature in comparison to other cryptocurrencies. Clarifying the present status of NFT research, pointing out obstacles, and proposing future lines of inquiry—such as token omics, metaverse integration, regulatory concerns, and asset valuation—are the objectives of the article. In the end, it highlights the necessity of more research to fully utilize NFTs while resolving questions about their application and effects.

Hammi et al. [11] present a thorough analysis of NFTs, examining their technological underpinnings, uses, and difficulties. They define NFTs as distinct digital assets protected by blockchain technology, which makes it easier to manage and verify ownership of digital goods, especially in the gaming and art industries. The study explores several applications for NFTs, such as their use in digital twins, the Metaverse, and as evidence of authenticity for tangible products. It also underlines the need for improvements to facilitate wider adoption of NFTs by highlighting issues including, digital asset security, privacy concerns, and the environmental impact of blockchain technologies.

Elzweig and Trautman [12] examine the intricate regulatory environment about NFTs and how U.S. law classifies them as securities. They talk about the emergence of NFTs and look at their many uses, which can include financial instruments and collectibles. The article highlights how the regulatory approach to NFTs is mostly determined by the underlying technology, blockchain, and its particular use cases. Referencing the Howey Test, the authors examine whether an NFT might be considered a security and explore the U.S. SEC's views of crypto-assets. The paper's ultimate goal is to improve knowledge of NFTs' effects on securities markets as well as their function in capital formation and economic expansion.

Three primary topics are covered by Zhao et al. [14], discussing authentication methods in the IoT: privacy protection using a blockchain-based cross-domain authentication system, trust management on the IoV, and IoT authentication techniques. It tackles several security issues, including the necessity for effective privacy safeguards, network assaults on IoT devices, and the dependability of information in IoV. This paper's main drawback is that it just offers theoretical models and solutions without doing thorough empirical research or examining actual deployment situations. This might have an impact on the technologies' usefulness in various IoT contexts.

Baho and Abawajy [15], highlight the growing security risks brought on by an increase in assaults on IoT devices by methodically reviewing current frameworks for evaluating vulnerabilities in these devices. It identifies research challenges and aims to provide a comprehensive understanding of current vulnerability assessment methodologies. A major drawback of the research, though, is that, despite its thorough examination, it does not provide a novel framework or approach for vulnerability assessment, which might have advanced the subject by filling in the gaps and shortcomings found in preexisting frameworks.

The growing number of IoT devices and the related cybersecurity risks are covered by Bakhshi et al. [17], paying special attention to firmware vulnerabilities that are frequently disregarded during development and deployment. It divides the IoT ecosystem into eight areas of concern and provides a thorough analysis of the auditing methods and resources currently in use for evaluating these risks. A significant drawback of the paper is that, although it offers a comprehensive review of vulnerability assessment techniques, it might not go into great detail about the usefulness and practical applications of these methods in actual situations, which could make it more difficult to integrate strong security features into IoT firmware.

With a focus on the vulnerabilities brought about by the extensive use of IoT devices and the need for strong cybersecurity measures, Tariq et al. [19] offer a thorough analysis of the security issues facing the IoT. It offers a methodical way to create safe IoT ecosystems while going over the main security issues with connectivity, communication, and management protocols. The absence of comprehensive security solutions and protocol standardization across various IoT applications are among the drawbacks acknowledged in the report, which makes it more difficult to develop a single security framework. It also emphasizes the necessity of more study to handle new security threats related to IoT device integration with current systems.

With an emphasis on problems like theft and vandalism, Yang et al. [20] examine the difficulties and developments in guaranteeing the physical security of IoT equipment. It highlights how AI may improve security measures while discussing a variety of countermeasures, such as circuit design, extra sensing technologies, biometrics, and tracking techniques. One of the paper's main limitations is its focus on technologically oriented solutions, which may cause it to ignore more general systemic issues and real-world implementation difficulties that might compromise the efficacy of the suggested security measures in actual situations.

Mishra and Pandya [25], offer a thorough analysis of the IoT environment, emphasizing its uses, security issues, and different kinds of attacks, especially DDoS attacks. It examines several IDS and anomaly detection methods and discusses

the vulnerabilities present at various IoT levels. The paper's scope, which is mostly focused on security problems without going into great detail about the wider implications of IoT technology on privacy, ethical issues, or the societal impact of widespread IoT adoption, is one of its main limitations.

Tawalbeh et al. [26], discuss IoT privacy and security issues with particular attention paid to problems, including incorrect device upgrades, lax security measures, and user ignorance. To improve security and privacy, it examines different security methods, current solutions, and a new layered paradigm for IoT that combines cloud and edge computing. The paper's emphasis on a general overview of IoT security rather than going into particular applications or in-depth analyses of the risks and weaknesses encountered by various IoT environments is a major drawback that could restrict its usefulness in a variety of real-world situations.

Pajouh and Parizi [28], offer a thorough examination of security concerns in the context of the IoT, emphasizing the many obstacles and possible fixes found in the various IoT design tiers. Using a three-layer architecture, which is application, network, and edge layers, it categorizes IoT security threats and vulnerabilities and talks about the particular security needs required to lessen these risks. The paper's primary focus on surveys and existing research from the last 10 years, however, may leave gaps in knowledge of the most recent security issues since it may not take into account new risks and quickly developing IoT technology.

Chang et al. [32], covered the growing privacy hazards of IoT devices, which highlights how consumers frequently aren't aware of the data that these devices are gathering and sharing. It presents the UTCID PPA, a smartphone software that evaluates the hazards connected to the IoT and offers practical advice to help users understand and manage their privacy. The paper's dependence on current privacy rules and the difficulties in assessing them is a significant drawback, as it could not adequately handle the wide range of quickly changing IoT privacy threats. Furthermore, user involvement and knowledge are critical to the efficiency of the suggested solutions, which can be difficult considering users' frequently poor levels of privacy policy awareness.

Sahu and Mazumdar [34], highlight threats like DoS attacks, unauthorized access, and data breaches, among other security issues brought on by the quick spread of IoT devices. It highlights how crucial it is to put strong security measures in place and investigates cutting-edge technologies like edge computing, blockchain, and machine learning as possible ways to reduce these dangers. The paper's main drawback is that, although it offers a thorough analysis of security risks and suggested remedies, it might not include case studies or empirical data proving the solutions' efficacy in actual IoT deployments, which makes it challenging to assess their impact and practical applicability.

The technical aspects of NFTs, market dynamics, security assessments, and possible possibilities and difficulties within the NFT ecosystem are all covered by Wang et al. [36]. The authors demonstrate how NFTs, which are based on blockchain technology, make it possible for distinct digital ownership and make trading digital assets easier. The study does, however, also note several drawbacks, including the infancy of NFT technology, the dearth of systematic research on NFTs, and persistent issues like expensive transactions, sluggish confirmation times, and security flaws that may impede user confidence and broad adoption.

To facilitate time-bound access and the commercialization of private data, Madine et al. [38], examine a blockchain-based platform that makes use of NFTs. To guarantee data ownership and security, it suggests a decentralized application that enables users to upload encrypted material, mint it as NFTs, and control access through licensing or purchase. The difficulty of Ethereum's computing performance, which limits the implementation of intricate smart contracts, and the requirement for off-chain solutions to manage massive data storage, which might introduce trust concerns if not handled correctly, are two significant limitations that have been brought to light.

Habib et al. [39], present and thoroughly analyze blockchain technology, emphasizing its development, range of industry applications, and cloud computing integration. It talks about the benefits of blockchain's decentralization, transparency, and security, as well as its uses in industries including digital identification, supply chain management, and banking. To fully realize the potential of blockchain technology in real-world applications, the paper also identifies important limitations, such as issues with scalability, energy consumption, and the difficulty of integrating blockchain solutions with current systems.

Das et al. [40], provided an in-depth examination of the security dynamics in the quickly changing NFT market. In addition to analyzing weaknesses in leading NFT markets and pointing out several frauds and malevolent practices that might result in monetary losses, it highlights important players in the ecosystem, including users, marketplaces, and external entities. The paper's main drawback is that, although it offers a methodical summary and analysis of security concerns, it might not cover all new dangers in the constantly changing NFT environment, especially when new technology and market trends emerge over time.

Ali et al. [41], offer a thorough analysis of NFTs, examining their market dynamics, technological underpinnings, and particular difficulties in their early phases of development. It highlights the special qualities and prospective uses of NFTs in a variety of industries, highlighting how they have produced a new digital asset economy in contrast to fungible cryptocurrencies. A major drawback of the article, nevertheless, is the paucity of systematic and definitive research on NFTs, which prevents a more thorough comprehension of their consequences and difficulties, especially regarding privacy, security, usability, and governance in the developing NFT ecosystem.

Arcenegui et al. [44] present a unique method for merging smart NFTs with PUFs to improve the safety of IoT devices. They present the idea of smart NFTs, which not only serve as distinct IoT devices on the blockchain but also give these devices the ability to create secure communication channels, actively participate in blockchain transactions, and demonstrate their reliability of operation through mutual authentication procedures. By guaranteeing that both the software and the hardware of IoT devices are reliable, this framework seeks to avoid problems associated with device malfunction or unauthorized access. The Ethereum blockchain and ESP32-based IoT devices are used by the authors to illustrate their concept, showing the usefulness and possible uses of this safe combination.

Through the use of NFTs, Khalil et al. [45] present a unique blockchain-based architecture that improves the security and authenticity of IoT assets in smart cities. It highlights the problems with the present frameworks for smart cities, especially security flaws and the shortcomings of conventional token standards like ERC721. Without requiring hardware changes, the suggested architecture combines decentralized technologies and fog computing to offer reliable authentication methods for IoT devices. It focuses on developing a decentralized infrastructure that enhances urban resource management's efficiency, security, and transparency while filling in knowledge gaps in NFT applications in cyber-physical systems.

Tripathi et al. [47], present an overview of blockchain technology. It covers its fundamental principles, application areas, historical evolution, different consensus algorithms, and obstacles to its widespread adoption. It draws attention to how blockchain technology has the potential to revolutionize several industries, including supply chain management, healthcare, and banking. The paper's primary focus on theoretical features and current literature, however, is a significant shortcoming. It does not provide actual data or case studies that illustrate the usefulness and practical application of blockchain solutions in real-world circumstances. Furthermore, the debate on the problem is sometimes too general and may have more detailed examples and case studies to further clarify the difficulties with blockchain adoption.

Justinia [48], presents how blockchain technology can revolutionize the biological sciences and healthcare industries, emphasizing its uses in supply chain management, automated claims processing, interoperability, and safe patient data exchange. It summarizes 20 actual use examples to show how blockchain may be used to solve current issues in the healthcare industry. The study does, however, also note several drawbacks, such as the early stages of blockchain use, worries about data security and privacy, the requirement for established protocols, and legal obstacles that would prevent broad adoption.

To overcome the scalability problems that traditional blockchain systems have when working with a large number of IoT devices, Haque et al. [49], present a scalable blockchain-based framework for effective IoT data management. It does this by using a lightweight consensus algorithm called DPoS. Although the paper offers a promising approach, one of its limitations is that it does not fully address the practical difficulties of putting the suggested system into practice on a large scale, especially regarding the resource limitations of different IoT devices and the difficulties of real-world deployments.

Sandner et al. [50], explore the confluence of blockchain, IoT, and AI, making the case that their combination will open up new autonomous business models in which gadgets may behave as separate economic agents with the ability to make

decisions and conduct financial transactions. It emphasizes how this convergence might improve IoT system scalability, privacy, security, and data management, implying that AI can streamline procedures and blockchain can standardize data formats. The paper's lack of technical information on the integration of various technologies is a drawback, though, since it focuses more on providing a conceptual overview than on discussing the particular difficulties and complexity associated with implementing.

George [51], presents IoT and blockchain technology. The paper focuses on how blockchain can improve security and trust in IoT ecosystems while addressing vulnerabilities and scalability issues. It highlights important issues, including resource limitations, interoperability, and the difficulties of connecting blockchain with various IoT devices. One significant drawback of the article is its dependence on case studies, which could not adequately convey how dynamic and ever-evolving blockchain and IoT technologies are. This could restrict the results' applicability to other industries and applications.

Alizadeh et al. [52], offer a thorough network analysis of the NFT market, emphasizing its development, structural features, and player interactions. It looks at the networks of transactions between NFT buyers and sellers and finds that most addresses are rarely used, while a few users make up the majority of trades. The lack of research that offers a comprehensive perspective of the historical and contemporary aspects of NFTs and their transactions is a major limitation mentioned in the paper. As a result, NFT creators and traders are unable to fully comprehend the relationships between different NFT projects and how the NFT community as a whole changes over time. An et al. [53], explore the NFT ecosystem on Ethereum. It looks into NFT formation, transfer, and holding patterns using graph analysis and novel metrics to spot possible market bubbles. The paper's dependence on data only from Ethereum is one of its limitations; this might distort conclusions and applicability across the whole NFT industry by failing to present a complete picture of the larger NFT ecosystem.

Taherdoost [54], examines the security situation of the IoT today, emphasizing the major security issues brought on by the increasing number of connected devices and the difficulties in defending them against cyberattacks. It highlights the necessity of strong security frameworks to solve these vulnerabilities and includes several research findings on data integrity, authentication, and authorization. The paper's recognition of the ongoing nature of IoT security research, which implies that many security concerns are still open and need further study to produce thorough answers, is one of its primary limitations.

Jurcut et al. [55], highlight the numerous risks, vulnerabilities, and attack vectors that IoT devices encounter while discussing the crucial security issues related to the IoT ecosystem. In addition to offering solutions for risk reduction and security framework enhancement, it highlights the significance of protecting these networked devices for a range of applications, including smart homes and industrial settings. The paper's emphasis on identifying security vulnerabilities rather than offering a thorough analysis of particular case studies or in-depth implementations of the suggested security solutions, which might improve practical comprehension and application in real-world circumstances, is one of its significant limitations.

Rekha et al. [56], address IoT security challenges and solutions, highlighting the increasing demand for strong cybersecurity as smart devices become more widely used in a variety of applications. It describes the many security risks that IoT systems encounter, such as insufficient encryption and illegal access, and suggests remedies like enhanced authentication, encryption tools, and a proactive security approach while developing IoT. The absence of empirical data or case studies to verify the efficacy of the suggested tactics in actual situation is a significant shortcoming of the article, which may restrict its practical usefulness even if it identifies several security issues and possible remedies.

Parry and Ellul [58], examined the combination of NFTs and SSI, along with the potential and difficulties that come with it. It talks about how NFTs can improve personal data governance and digital asset ownership, giving people more control over who they are while overcoming governance, legal, and technological obstacles. The paper's main drawback is that it only offers a theoretical framework with no empirical support or real-world applications, which might restrict the usefulness of the ideas and solutions put forth.

Zelenyanszki et al. [60], discuss the privacy issues surrounding NFTs on public blockchains, which are examined with a special emphasis on how transaction data can disclose private information about user activity. To find relationships between transactions that can reveal privacy-critical information, the authors use graph visualization to examine transaction events from the blockchain-based game Planet IX. The paper's dependence on a single case study, which could not accurately

reflect the wide variety of NFT applications or the wider ramifications of privacy threats across many platforms and ecosystems, is one of its most significant limitations.

Gupta et al. [61], examined the inherent security concerns associated with NFT platforms. They offer a taxonomy of these hazards as well as practical solutions for stakeholders. It looks at how the web has changed from centralized to decentralized systems, emphasizing the weaknesses brought forth by platform operations and user interactions. The paper’s dependence on an informal assessment of security methods in the quickly changing NFT landscape is a major drawback. It might not fully account for all new dangers or sufficiently address the intricacies of user behavior and technology developments in this field.

With an emphasis on adherence to the GDPR, Delgado-von-Eitzen et al. [71], explore a unique model for releasing and confirming academic information using NFTs powered by blockchain technology. It discusses the difficulties posed by fake credentials and the requirement for a trustworthy verification mechanism in the field of education. The intricacy of striking a balance between the immutable nature of blockchain technology and GDPR, particularly regarding the right to data deletion and modification, is a significant drawback of the suggested strategy. Since the GDPR forbids the permanent keeping of personally identifiable information, storing personal data directly on a blockchain presents legal issues and may result in inconsistencies between the two systems.

Table 3. Related Studies of IoT

Reference	Year	Methodology	Technology	Sector/Application	Open Issues	Limitations
[1]	2023	Mixed	IoT, cloud computing	Healthcare, smart homes.	Security, privacy, scalability.	Scope of coverage.
[2]	2021	Qualitative	IoT, M2M	Healthcare, smart homes.	Security, privacy, scalability.	Lack of empirical data.
[3]	2023	Mixed	IoT, AI	Healthcare, smart homes.	Security, cost	Lack of standardization
[4]	2019	Mixed	IoT, cloud computing	Smart cities, healthcare, transportation.	Security, privacy.	Lack of in-depth analyses
[5]	2022	Mixed	IoT	Smart cities, healthcare, transportation.	Security, privacy, scalability.	Lack of empirical data.
[6]	2023	Qualitative	IoT, AI	Smart cities, healthcare.	Security, privacy.	Lack of empirical data.
[7]	2023	Mixed	AI, ML, DL	Smart cities, healthcare.	vulnerabilities in IoT	Potential underrepresentation.
[8]	2020	Mixed	IIoT, Cloud	IIoT	Integration of legacy systems	Not cover all emerging security threats.
[9]	2021	Qualitative	IoT, cloud computing	Smart cities, healthcare, transportation.	Security, privacy, scalability.	Dependency on cloud computing.
[10]	2022	Mixed	Blockchain, NFTs	Finance and Economics	Environmental impact of blockchain	Not cover all emerging trends.
[11]	2023	Qualitative	Blockchain, NFTs	Authentication and identification systems	Security, privacy.	Lack of empirical data.
[12]	2022	Mixed	Blockchain, NFTs	Securities law and digital assets	Regulatory clarity	Scope of analysis
[14]	2023	Mixed	Blockchain, cloud computing	IoV, IoT	High communication costs	Reliance on specific technologies
[15]	2023	Mixed	IoT, CVSS	Smart cities, healthcare.	IoT vulnerabilities	limited by the availability and quality of existing literature
[17]	2024	Mixed	IoT	Smart cities, healthcare.	Capabilities of IoT devices	Not address emerging threats
[19]	2023	Mixed	IoT, BLE	IoT Security	Protocol standardization	Specificity of selected issues
[20]	2022	Mixed	AI, Biometric	smart home, smartphones	Lack of comprehensive studies	high implementation costs
[25]	2021	Mixed	IoT	Smart cities, healthcare, transportation.	Resource constraints	Scope limitation
[26]	2020	Mixed	IoT	Smart cities	vulnerabilities in IoT	lacks an exhaustive exploration
[28]	2021	Mixed	Cloud, RFID	Smart cities, healthcare	Security, privacy, scalability.	Focus primarily on literature review
[32]	2024	Mixed	IRR	IoT, privacy	User Awareness	Scope of Data
[34]	2024	Mixed	Blockchain, Edge, and Fog Computing	IoT	Security vulnerabilities in IoT layers	Not cover all emerging security threats
[36]	2021	Mixed	Blockchain	NFTs	Security, privacy.	Lack of systematic studies
[38]	2022	Quantitative	Blockchain, NFTs	Healthcare	Scalability	vulnerabilities in off-chain interactions
[39]	2022	Mixed	Blockchain	Cybersecurity, Healthcare	Scalability	not cover all emerging blockchain technologies
[40]	2022	Mixed	Blockchain	NFT Ecosystem	Security Vulnerabilities	Generalizability
[41]	2023	Mixed	Blockchain	Supply Chain Management	Security, privacy.	A paucity of systematic research

[44]	2021	Mixed	Blockchain, IoT, PUFs	Smart Contracts and NFTs	secure links between tokens and devices	The reliance on specific hardware.
[45]	2023	Mixed	Blockchain, Fog	Smart Cities	Security, reliability	Dependence on existing standards.
[47]	2023	Qualitative	Blockchain	Healthcare, energy	Security, privacy, scalability.	Not cover all possible applications
[48]	2019	Mixed	Blockchain	Healthcare	Security, privacy, scalability.	Lack of Longitudinal Studies
[49]	2024	Mixed	Blockchain	IoT	Security, privacy, scalability.	Resource Constraints
[50]	2020	Qualitative	Blockchain, IoT, AI	Digital transformation in various industries	Security, privacy, scalability.	Lack of empirical data
[51]	2024	Qualitative	Blockchain	Smart cities, healthcare, transportation.	vulnerabilities in blockchain	Potential biases in the studies.
[52]	2023	Quantitative	Moralis platform	blockchain and digital asset sector	limited research on the NFT	The analysis is constrained
[53]	2023	Quantitative	Blockchain	Cryptocurrency and Blockchain, NFT	Stability of the NFT	Data Scope
[54]	2023	Qualitative	IoT, Blockchain	Smart cities, healthcare	IoT security	Limited studies
[55]	2020	Mixed	Blockchain	Smart cities, healthcare	Lack of standardized security protocols	Not cover all emerging security threats
[56]	2023	Mixed	IoT	Smart cities, healthcare	Security standards	Focuses on theoretical aspects
[58]	2024	Mixed	Blockchain	Digital identity management	Challenges in integration	Focus on theoretical constructs
[60]	2023	Mixed	Blockchain	Blockchain-based Applications	Privacy risks and enhancements	Focus on a single application
[61]	2022	Mixed	Blockchain	NFT sectors	security in NFT	Not fully addressing risks
[71]	2024	Mixed	Blockchain	Educational sector	Privacy	Not fully developed technology

8. Open Challenges and Limitations

There are several unresolved issues and restrictions with the combination of IoT and NFTs that must be resolved. Scalability is a key concern; blockchain networks frequently find it difficult to manage the large amounts of transactions produced by IoT devices, which might result in congestion and performance deterioration. Furthermore, latency issues come up because NFT transaction processing delays might impair the performance of IoT applications that need to handle data in real-time, which will have a detrimental influence on user experience. Because different blockchain platforms might make it more difficult to transfer NFTs and expose assets to security flaws because of varied protocols and standards, interoperability threats can present serious difficulties.

Furthermore, even with recent advancements like Ethereum's switch to PoS, the environmental effect of blockchain technology is still a major concern, especially with energy-intensive protocols like PoW. Their integration with NFTs is complicated by the inherent security flaws in many IoT devices, which leave them open to breaches and illegal access. These flaws include poor authentication procedures and insufficient data encryption. There is also a dearth of user education and awareness about the security implications of these technologies, which calls for initiatives to educate consumers about blockchain knowledge and best practices for device security.

Moreover, the quickly changing IoT and blockchain world presents regulatory and compliance issues, as firms face ambiguity owing to the lack of defined legal frameworks. Unified standards are necessary to improve interoperability since the absence of established methods for NFT development and maintenance across various platforms results in discrepancies and possible security vulnerabilities. Physical security threats make things much more difficult because a lot of IoT devices may be tampered with, which calls for strong defenses, particularly in delicate settings. Lastly, the growing complexity of cyber threats, such as supply chain assaults and APTs, emphasizes the necessity of constant security measure monitoring and upgrading to successfully counter these new dangers. To fully utilize IoT and NFTs while maintaining user security and confidence in these technologies, these issues must be resolved.

9. Future Work

To improve the integration of IoT with NFTs, future research should concentrate on several critical areas. Establishing standardized communication and interoperability across various blockchain systems, enabling safe interactions, and reducing security concerns all depend on the development of strong protocols. Enhancing scalability solutions is also essential. Strengthening these systems against possible attacks would need improving security frameworks designed to address the vulnerabilities related to IoT and NFTs. Risks can also be reduced by supporting user education programs that raise knowledge and comprehension of security best practices for NFTs and IoT devices. Lastly, investigating ecologically

friendly blockchain processes and technology is essential to reducing the environmental effect of NFT transactions and advancing sustainable development. Stake- holders can ensure a safe and effective digital environment while working to fully realize the promise of IoT and NFT integration by addressing these issues.

10. Conclusions

There are several chances to improve security and traceability in digital ecosystems by combining the IoT with NFTs. This review is about security flaws in IoT devices that might result in illegal access, and data breaches are highlighted in this analysis. These flaws include weak authentication procedures, insufficient data encryption, and unsafe interfaces. The study also emphasizes the special qualities of NFTs, which can improve IoT environment security by offering secure digital identities and making device and data tracing easier.

Despite the potential benefits, the integration of IoT and NFTs poses additional hurdles, including scalability constraints, interoperability risks, and environmental concerns associated with blockchain technology. Because these technologies are constantly changing, it is necessary to research to solve these issues and create strong frameworks for integrating them. There is potential for more secure and effective systems to be created by combining IoT with NFTs but doing so calls for a thorough evaluation of the security risks involved and the application of best practices to reduce these weaknesses. To further this integration and guarantee the security of upcoming apps in diverse areas, academics, developers, and industry stakeholders must continue their partnership.

Corresponding author

M M Hafizur Rahman
mhrahman@kfu.edu.sa

Acknowledgements

The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No.]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

Funding

NA

Contributions

Conceptualization, A.A; H.A; M.M.A.R; Methodology, A.A; H.A; M.M.A.R; Software, A.A; H.A; M.M.A.R; Validation, A.A; H.A; M.M.A.R; Formal Analysis, A.A; H.A; M.M.A.R; Investigation, A.A; H.A; M.M.A.R; Resources; A.A; H.A; M.M.A.R Data Curation, A.A; H.A; M.M.A.R; Writing (Original Draft), A.A; H.A; M.M.A.R; Writing (Review and Editing), M.M.A.R; Visualization, M.M.A.R; Supervision; M.M.A.R; Project Administration, M.M.A.R; Funding Acquisition, M.M.A.R. All authors have read and agreed to the published version of the manuscript.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Competing interests

All authors declare no competing interests

Abbreviations

AI	Artificial Intelligence
APIs	Application Programming Interface
APTs	Advanced Persistent Threats
BLE	Bluetooth Low Energy
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial-of-Service
DL	Deep Learning
DoS	Denial of Service
DPoS	Delegated Proof of Stake
GDPR	General Data Protection Regulation
IDS	Intrusion Detection Systems
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoV	Internet of Vehicles
IRR	IoT Resource Registries
MFA	Multi-Factor Authentication
MITM	Man-In-The-Middle
ML	Machine Learning
NFT	Non-Fungible Tokens
NIST	National Institute of Standards and Technology
OCF	Open Connectivity Foundation
PII	Personally Identifiable Information
PoS	Proof-of-Stake
PoW	Proof-of-Work
PPA	Personalized Privacy Assistant
PUF	Physical Unclonable Functions
SEC	Securities and Exchange Commission
SSI	Self-Sovereign Identity

References

- [1] Ananna, T. N., & Saifuzzaman, M. (2023). *Introduction to IoT*. arXiv. <https://arxiv.org/abs/2312.06689>
- [2] Mouha, R. A. R. A., et al. (2021). Internet of things (IoT). *Journal of Data Analysis and Information Processing*, 9, 77.
- [3] Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. *Sensors*, 23, 7194.
- [4] Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, 6, 1–21.
- [5] Elgazzar, K., Khalil, H., Alghamdi, T., Badr, A., Abdelkader, G., Elewah, A., & Buyya, R. (2022). *Revisiting the Internet of Things: New trends, opportunities and grand challenges*.
- [6] Alliou, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, 23, 8015.
- [7] Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain Sciences*, 13, 683.
- [8] Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2020). Challenges and opportunities in securing the industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 17, 2985–2996.
- [9] Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. (2021). A review and state of art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, 1–19.
- [10] Taherdoost, H. (2022). Non-fungible tokens (NFT): A systematic review. *Information*, 14, 26.
- [11] Hammi, B., Zeadally, S., & Perez, A. J. (2023). Non-fungible tokens: A review. *IEEE Internet of Things Magazine*, 6, 46–50.
- [12] Elzweig, B., & Trautman, L. J. (2022). When does a non-fungible token (NFT) become a security? *Georgia State University Law Review*, 39, 295.
- [13] El-Sofany, H., El-Seoud, S. A., Karam, O. H., & Bouallegue, B. (2024). Using machine learning algorithms to enhance IoT system security. *Scientific Reports*, 14, 12077.

- [14] Zhao, J., Hu, H., Huang, F., Guo, Y., & Liao, L. (2023). Authentication technology in Internet of Things and privacy security issues in typical application scenarios. *Electronics*, 12, 1812.
- [15] Baho, S. A., & Abawajy, J. (2023). Analysis of consumer IoT device vulnerability quantification frameworks. *Electronics*, 12, 1176.
- [16] Rana, M., Mamun, Q., & Islam, R. (2023). Enhancing IoT security: An innovative key management system for lightweight block ciphers. *Sensors*, 23, 7678.
- [17] Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. *Sensors*, 24, 708.
- [18] Hindka, M. (2024). *Securing the digital backbone: In-depth insights into API security patterns and practices*.
- [19] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. *Sensors*, 23, 4117.
- [20] Yang, X., Shu, L., Liu, Y., Hancke, G. P., Ferrag, M. A., & Huang, K. (2022). Physical security and safety of IoT equipment: A survey of recent advances and opportunities. *IEEE Transactions on Industrial Informatics*, 18, 4319–4330.
- [21] Shah, Y., & Sengupta, S. (2020). A survey on classification of cyber-attacks on IoT and IIoT devices. In *2020 11th IEEE UEMCON* (pp. 406–413). IEEE.
- [22] Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201.
- [23] Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks*, 8, 22.
- [24] Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications*, 26, 92–98.
- [25] Mishra, N., & Pandya, S. (2021). Internet of Things applications, security challenges, intrusion detection, and future visions: A systematic review. *IEEE Access*, 9, 59353–59377.
- [26] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences*, 10, 4102.
- [27] Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & KEBANDE, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, 9, 121975–121995.
- [28] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on Internet of Things security: Requirements, challenges, and solutions. *Internet of Things*, 14, 100129.
- [29] Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P., & Aski, V. J. (2020). Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, 33, e4443.
- [30] Anand, P., Singh, Y., Selwal, A., Singh, P. K., Felseghi, R. A., & Raboaca, M. S. (2020). IOVT: Internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in IoT and its applications towards smart grids. *Energies*, 13, 4813.
- [31] Menard, P., & Bott, G. J. (2020). Analyzing IoT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security*, 95, 101856.
- [32] Chang, K. C., Niu, H., Kim, B., & Barber, S. (2024). IoT privacy risks revealed. *Entropy*, 26, 561.
- [33] Hejase, H. J., Fayyad-Kazan, H. F., & Moukadem, I. (2020). Advanced persistent threats (APT): An awareness review. *Journal of Economics and Economic Education Research*, 21, 1–8.
- [34] Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions techniques for Internet of Things (IoT): From vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, 7, 1397480.
- [35] Bhujel, S., & Rahulamathavan, Y. (2022). A survey: Security, transparency, and scalability issues of NFTs and its marketplaces. *Sensors*, 22, 8833.
- [36] Alsahaim, S., Almaiah, M. A., & Sulaiman, R. B. (2023). Security Threats in Mobile Phones: Challenges, Countermeasures, and the Importance of User Awareness. *International Journal of Cybersecurity Engineering and Innovation*, 2023(1).
- [37] Madine, M., Salah, K., Jayaraman, R., & Zemerly, J. (2023). NFTs for open-source and commercial software licensing and royalties. *IEEE Access*, 11, 8734–8746.
- [38] Madine, M., Salah, K., Jayaraman, R., Battah, A., Hasan, H., & Yaqoob, I. (2022). Blockchain and NFTs for time-bound access and monetization of private data. *IEEE Access*, 10, 94186–94202.
- [39] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration with cloud computing. *Future Internet*, 14, 341.
- [40] Das, D., Bose, P., Ruaro, N., Kruegel, C., & Vigna, G. (2022). Understanding security issues in the NFT ecosystem. In *ACM CCS 2022* (pp. 667–681).
- [41] Ali, O., Momin, M., Shrestha, A., Das, R., Alhajj, F., & Dwivedi, Y. K. (2023). A review of the key challenges of non-fungible tokens. *Technological Forecasting and Social Change*, 187, 122248.
- [42] Li, L. (2024). Mitigating challenges in Ethereum's proof-of-stake consensus: Evaluating the impact of EigenLayer and Lido. arXiv.
- [43] Rožman, N., Corn, M., Škulj, G., Berlec, T., Diaci, J., & Podržaj, P. (2023). Exploring the effects of blockchain scalability limitations on performance and user behavior in blockchain-based shared manufacturing systems. *Applied Sciences*, 13, 4251.
- [44] Arcenegui, J., Arjona, R., Román, R., & Baturone, I. (2021). Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs. *Sensors*, 21, 3119.
- [45] Khalil, U., Malik, O. A., Hong, O. W., & Uddin, M. (2023). Leveraging a novel NFT-enabled blockchain architecture for the authentication of IoT assets in smart cities. *Scientific Reports*, 13, 19785.
- [46] Ibrahim, A., Kadhim, A. F., Hamzah, A. E., & Al-Shareeda, M. A. (2026). A Secure and Scalable IoT Home Automation Architecture with Web and Biometric Control. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).

- [47] Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, 100344.
- [48] Justinia, T. (2019). Blockchain technologies: Opportunities for solving real-world problems in healthcare and biomedical sciences. *Acta Informatica Medica*, 27, 284.
- [49] Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A scalable blockchain-based framework for efficient IoT data management using lightweight consensus. *Scientific Reports*, 14, 7841.
- [50] Kadhim, A. F., Hamzah, A. E., Al-Shareeda, M. A., Hussein, A. I., & Sapiee, N. M. (2026). Accurate Network Intrusion Detection using a Feedforward Neural Network and Bee Colony Optimization Algorithm. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
- [51] George, I. (2024). *Exploring the integration of blockchain in IoT use cases: Challenges and opportunities*.
- [52] Alizadeh, S., Setayesh, A., Mohamadpour, A., & Bahrak, B. (2023). A network analysis of the non-fungible token (NFT) market: Structural characteristics, evolution, and interactions. *Applied Network Science*, 8, 38.
- [53] Tan, Y., Wu, Z., Liu, J., Wu, J., Zheng, Z., & Chen, T. (2023). Bubble or not: Measurements, analyses, and findings on the Ethereum ERC721 and ERC1155 NFT ecosystem. arXiv.
- [54] Taherdoost, H. (2023). Security and Internet of Things: Benefits, challenges, and future perspectives. *Electronics*, 12, 1901.
- [55] Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. *SN Computer Science*, 1, 1–19.
- [56] Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, 80, 3554–3599.
- [57] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in Internet of Things with a focus on emerging technologies. *Internet of Things*, 19, 100564.
- [58] Parry, G., & Ellul, J. (2024). NFTs and self-sovereign identity: Opportunities and challenges. *Authorea Preprints*.
- [59] Al-Sumaidae, G., & Žilić, Ž. (2024). Sensing data concealment in NFTs: A steganographic model for confidential cross-border information exchange. *Sensors*, 24, 1264.
- [60] Zelenyanski, D., Hóu, Z., Biswas, K., & Muthukkumarasamy, V. (2023). Linking NFT transaction events to identify privacy risks. In *International Symposium on Distributed Ledger Technology* (pp. 82–97). Springer.
- [61] Gupta, Y., Kumar, J., & Reifers, A. (2022). Identifying security risks in NFT platforms. arXiv.
- [62] Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2021). Internet of Things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, 22, 105–117.
- [63] Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*, 54, 1–37.
- [64] Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2023). IoT and man-in-the-middle attacks. arXiv.
- [65] Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and DDoS attack recognition in the Internet of Things (IoT). *Electronics*, 11, 494.
- [66] Khatiwada, P., Yang, B., Lin, J. C., Mugurusi, G., & Underbekken, S. (2024). A reference design model to manage consent in data-subject-centered Internet of Things devices. *IoT*, 5, 100–122.
- [67] Al-shareeda, M., & Alrudainy, H. (2026). Sustainable and Secure Energy Optimization Strategies in the Internet of Healthcare Things (IoHT). *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
- [68] Esmaeilzadeh, P., et al. (2023). Evolution of health information sharing between healthcare organizations: Potential of nonfungible tokens. *Interactive Journal of Medical Research*, 12, e42685.
- [69] Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). GDPR compliance verification in Internet of Things. *IEEE Access*, 8, 119697–119709.
- [70] Arabsorkhi, A., & Khazaei, E. (2024). Blockchain technology and GDPR compliance: A comprehensive applicability model. *International Journal of Web Research*, 7, 49–63.
- [71] Alrajeh, M., Almaiah, M., & Mamodiya, U. (2026). Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
- [72] Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, 32, 1779–1794.
- [73] de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, 20, 7171.
- [74] Cornelius, K. (2021). Betraying blockchain: Accountability, transparency and document standards for NFTs. *Information*, 12, 358.
- [75] Burleson, J., Korver, M., & Boneh, D. (2022). *Privacy-protecting regulatory solutions using zero-knowledge proofs*.
- [76] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908–164940.
- [77] Ruffner, J. (2024). *Investigating user awareness of privacy and security concerns in the IoT era*.
- [78] Schrama, V., Gañán, C. H., Aschenbrenner, D., de Reuver, M., Borgolte, K., & Fiebig, T. (2020). Understanding the knowledge gap: How security awareness influences the adoption of industrial IoT. In *WEIS 2020* (pp. 1–17).
- [79] Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, 12, 157.
- [80] Ahmed, S., & Khan, M. (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity. *AI, IoT and the Fourth Industrial Revolution Review*, 13, 1–17.
- [81] Banaeian Far, S., & Hosseini Bamakan, S. M. (2023). NFT-based identity management in metaverses: Challenges and opportunities. *SN Applied Sciences*, 5, 260.