

Review

Blockchain-Based Data Breach Detection: Approaches, Challenges, and Future Directions

Kainat Ansar ¹, Mansoor Ahmed ^{1,2} , Markus Helfert ² and Jungsuk Kim ^{3,4,*} 

¹ Department of Computer Science, COMSATS University, Islamabad 44000, Pakistan; mansoor.ahmed@mu.ie (M.A.)

² ADAPT Centre, Innovation Value Institute, Maynooth University, W23 F2H6 Maynooth, Ireland

³ Department of Biomedical Engineering, College of IT Convergence, Gachon University, Sujeong-gu, Seongnam-si 13120, Republic of Korea

⁴ Research and Development Laboratory, Cellico Company, Seongnam-si 13449, Republic of Korea

* Correspondence: jungsuk@gachon.ac.kr

Abstract: In cybersecurity, personal data breaches have become one of the significant issues. This fact indicates that data breaches require unique detection systems, techniques, and solutions, which necessitate the potential to facilitate precise and quick data breach detection. Various research works on data breach detection and related areas in dealing with this problem have been proposed. Several survey studies have been conducted to comprehend insider data breaches better. However, these works did not examine techniques related to blockchain and innovative smart contract technologies to detect data breaches. In this survey, we examine blockchain-based data breach detection mechanisms developed so far to deal with data breach detection. We compare blockchain-based data breach detection techniques based on type, platform, smart contracts, consensus algorithm language/tool, and evaluation measures. We also present a taxonomy of contemporary data breach types. We conclude our study by outlining existing methodologies' issues, offering ideas for overcoming those challenges, and pointing the way forward.

Keywords: data breach detection; data leak detection; blockchain; distributed ledgers

MSC: 37M99



Citation: Ansar, K.; Ahmed, M.; Helfert, M.; Kim, J. Blockchain-Based Data Breach Detection: Approaches, Challenges, and Future Directions. *Mathematics* **2024**, *12*, 107. <https://doi.org/10.3390/math12010107>

Academic Editor: Jan Lansky

Received: 13 November 2023

Revised: 16 December 2023

Accepted: 18 December 2023

Published: 28 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The unintentional or intentional disclosure of personal data to an unauthorized user is known as data leakage [1]. Personal data acquired by firms and organizations includes copyrighted material, banking details, private account information, sanctions information, etc. The number of incidents and the cost to individuals affected is increasing, which presents a serious problem for businesses. The lack of control and monitoring over transferred data as it travels to its destination increases data leakage [2]. The company's insider personnel and digital media can both be used to leak the data. In its 2021 Cost of a Data Breach Report, the Ponemon Institute examined data from 537 global firms that had experienced a data breach. They discovered that the industries with the costliest data breaches were healthcare, finance, pharmaceutical, technology, and energy. Computer networks and telecommunications play a significant role in the flow of information. As valuable information has grown and innovations have become more feasible, risks have also increased. Both internal and external sources of these risks are present in the organization. Such attacks appear challenging to identify and offer a serious security concern [3].

Insider threats may harm an organization's reputation, financial assets, and intellectual property. According to 2018 research on the insider threat, slightly more than half of the dangers (53%) came from within companies in the previous year [4]. To protect companies from an insider data breach, companies should implement an insider breach detection

system that can detect and control attacks before they spread. Unfortunately, the field of insider data breaches is not well understood. Furthermore, the detecting techniques or procedures that can be employed and the limitations of current solutions still need to be investigated. As a result, a thorough examination of existing insider breach detection systems is required [5]. Due to its transformative potential, a specific “Distributed Ledger Technology” known as blockchain is gaining traction across all economic sectors. The capability of blockchain to disrupt the role of mediators in transactions, streamline procedures, and create new operating models and workflows leads to significant cost savings and possible profit increases for businesses working inside it. The immutability of transactions and decentralization of record keeping are two properties of blockchain that have never been achieved.

It is hard to dispute that blockchain has progressed significantly during the previous ten years. It all started with Bitcoin, which has a public blockchain (the first type of blockchain). The blockchain used by Bitcoin is known as the first generation of blockchain technology. We have reached a point where there are numerous types of blockchain technology, each addressing a different set of problems. There are four types of blockchain: public, private, hybrid, and consortium.

This study will analyze the data breach problem descriptively and analytically by examining the attacks to understand their nature better. In addition, one of the goals of this research is to review existing research findings on blockchain-based breach detection systems. We categorized them generally based on the types, such as the type of data breach and blockchain-based solution to detect this type of breach. Comparing our survey to others in the literature, Table 1 outlines the key contributions of our survey. Table 1 also lists some of the findings from research into the blockchain environment and compares the ideas used with the viewpoints of this study. This study primarily aims to accomplish the following goals:

- To explore existing types of data breach attacks.
- To give a complete assessment of research on this topic.
- To categorize blockchain-based breach detection techniques based on attack types.
- To tabulate the most scientific developments from all related articles to provide a quick overview of the field’s progress.

Table 1. Comparison of the key elements of this survey with the features found in the literature.

Features	[6]	[7]	[8]	This Survey
Consensus protocols for data breaches are presented.	X	X	X	✓
Enabling technologies were discussed in order to offer defenses against various aspects of the problem of data leaking.	✓	X	X	✓
Explores the application of blockchain in the domain of data breaches and how it might be improved.	X	X	✓	✓
Identifies potential future directions for creating more reliable leakage prevention systems that can improve on some of the shortcomings of the present ones.	X	✓	X	✓
Provides a more comprehensive and recent analysis of how the blockchain is being used to address data breach issues.	X	X	X	✓
The advantages and drawbacks of blockchain technology for detecting data breaches.	X	X	X	✓
Provides bibliographic information used in the review.	X	X	✓	✓
A taxonomy of current data breach types is presented.	✓	✓	✓	✓
Highlights current and future issues and genuine concerns in the data breach field.	X	✓	X	✓
Compares existing blockchain-based data breach detection solutions based on type, platform, smart contracts, and consensus algorithm.	X	X	X	✓

The rest of the paper is structured as follows. The review methodology and inclusion–exclusion criteria are discussed in Section 2. In Section 2-C, research questions are presented. The types of data breach attacks and previous studies on the usage of blockchain in detecting data breach attacks are discussed in Section 3. Section 4 examines the issues that must be addressed in blockchain adoption in breach detection. Data breach scenarios arising from technical failures are presented in Section 4. Additionally, recommendations are also presented in Section 5. Finally, the conclusion and future work are presented in Section 6.

2. Review Methodology

This section presents a stepwise review methodology employed in this study. Additionally, research questions are also discussed in this section.

A. SEARCH STRATEGY

The initial step in our search method was to discover the flaws in current surveys that suggest non-blockchain-based ways to detect data breaches. This prompted us to clarify our contribution and goals, mostly regarding using blockchain to aid the battle against data breach detection. In the second phase, we employed keywords like blockchain, distributed ledgers, data leak, data breach detection, information leak, and its synonyms to discover relevant research publications on the issue. We used the Google Scholar engine and databases and preprint services, including ACM, ScienceDirect, IEEE Xplore, Scopus, Springer Link, and arXiv, to discover these publications and obtain the full-text versions. The leading search keyword is inserted between the logical AND and OR operators and may be written as

(“Blockchain” OR “Digital Ledger” OR “Distributed Ledger” OR “BLC”) AND (“Data Leak” OR “Data Breach” OR “Information Leak”) AND (“Detection” OR “Technique” OR “Mitigation” OR “Algorithm” OR “Mechanism”)

B. Inclusion and Exclusion Criteria

Most of the papers in this review were chosen based on the titles and abstracts of the retrieved studies—for example, blockchain-based solutions for data breach detection. No study was omitted based on its title and abstract unless a complete text review determined that it was unrelated to the current review. Exclusion criteria used in this analysis include research that reports data breach solutions that are not blockchain-based. Table 2 summarizes the primary criteria for including or excluding research papers.

Table 2. Inclusion–exclusion criteria.

Inclusion Criteria	Exclusion Criteria
The paper must be related to data breaches and blockchain in some way.	Articles that are written in a language other than English.
Publications in the field of information leakage breaches or data breaches.	Duplicate articles that replicate research that has already been published.
Papers that emphasize how blockchain was utilized to prevent data breaches.	Papers that emphasize non-blockchain-based techniques to prevent data breaches.
Papers that focus on how blockchain may be used to address important challenges of breach detection.	Articles in which a survey or review is presented.
From 2017 to 2023, all research on this topic was covered.	Articles that are not part of the broader data breach and blockchain domain.

C. RESEARCH QUESTIONS

The following questions have determined the scope of our work:

- What are the various forms of breaches that might occur? Identify the different types of data breaches documented in the literature.

- How is blockchain used to detect data breaches? What proposals and techniques did the researchers make to address the problems and obstacles they encountered?
- What challenges occur when blockchain technology is used to identify data breaches?

3. Comprehensive Review

When secret information intended to be protected is revealed or exposed, intentionally or unintentionally, it is referred to as a data breach. Financial information, such as credit card numbers, social security numbers, medical histories, and corporate information, such as customer lists, may be exposed to data breaches. When someone who is not explicitly allowed to access such data does so, the organization responsible for securing it is said to have experienced a data breach. In this article, data breach attacks are categorized into four types: phishing, malware/ransomware, distributed denial of service, and malicious insider, as shown in Figure 1. Table 3 presents a summary of the studies included in this review. Furthermore, the taxonomy of reviewed papers is shown in Figure 2.

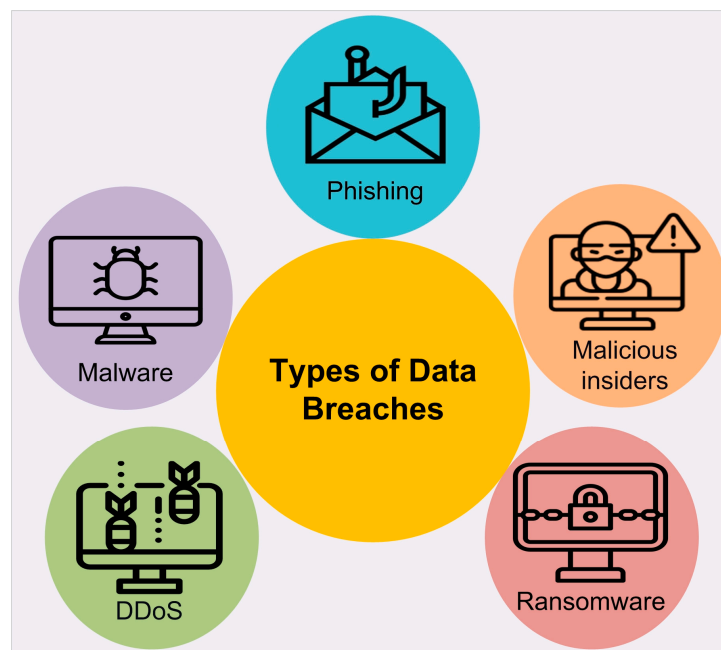


Figure 1. Types of data breach attacks.

Table 3. Summary of the literature review.

Ref.	Blockchain Platform	Consensus Algorithm	Breach Type	Smart Contract	Domain	Implementation	GDPR	Language/Tool Used	Evaluation Metrics
[9]	Not specified	Delegated proof of stake	Insider threat	No	Not specified	Yes	No	Not specified	Response time with respect to node number and test time
[10]	Not specified	Not specified	Insider threat	No	Not specified	Yes	No	Not specified	Not specified
[11]	Ethereum	Proof of work	Insider threat	Yes	IoT	Yes	No	Marvin v.19.9, LoRaWAN v.1.0.4	Time
[12]	Hyperledger Fabric	Not specified	Insider threat	No	Education	Yes	No	Python v.3.8, Hyperledger Fabric v1.4, SQLite v3.11.0	CRUD query runtime

Table 3. Cont.

Ref.	Blockchain Platform	Consensus Algorithm	Breach Type	Smart Contract	Domain	Implementation	GDPR	Language/Tool Used	Evaluation Metrics
[13]	Ethereum	Proof of stake	Insider threat	Yes	IoT	Yes	No	Arduino IDE v.1.8, LoRaWAN, Marvin device	Time with respect to temperature
[14]	Not specified	Not specified	Malware	No	Mobile devices	Yes	No	FlowDroid v.2.7	Time, cost, accuracy, and recall rate
[15]	Ethereum	Proof of work	Ransomware	Yes	Not specified	Yes	No	Not specified	Storage and execution costs
[16]	Not specified	Not specified	Ransomware	No	Cerber	Yes	No	Not specified	Average time to mitigation
[17]	Ethereum	Delegated proof of stake	Malware	Yes	IoT	Yes	Yes	Solidity v.0.5.0	TPR, FPR, Accuracy, and running time
[18]	Ethereum	Proof of work	Malware	Yes	Cybersecurity	Yes	No	Not specified	Accuracy, TPR
[19]	Ethereum	Proof of stake	Malware	Yes	IoT	Yes	No	Node.js, Web3 library, solidity v.0.5.0	Number of requests per second
[20]	Ethereum	Proof of work	Malware	Yes	Not specified	Yes	No	Geth v1.13.1 and Python v.3.8	False-negative rate and false-positive rate
[21]	Ethereum	Proof of stake	Malware	Yes	Android	Yes	No	Not specified	Accuracy, precision, recall, and f-measure
[22]	Not specified	Not specified	Malware	No	Mobile app store	No	No	Not specified	Not specified
[23]	Ethereum	Proof of stake	Phishing	No	Not specified	Yes	No	Not specified	Precision, recall, and F-score
[24]	Ethereum	Proof of stake	Phishing	Yes	Not specified	Yes	No	Not specified	Precision, recall, F1, and AUC
[25]	Hyperledger Fabric	Dpos and BFT	Phishing	No	Alibaba, PayPal, Chase, and Facebook URLs and crowd-sourcing	Yes	No	Hyperledger Fabric 1.1	Performance throughput
[26]	Quorum	Byzantine Fault Tolerance	Phishing	Yes	Alibaba, PayPal, Chase, and Facebook URLs and crowd-sourcing	Yes	No	Solidity v.0.5.0	Ac, pre, rec
[27]	Ethereum	Proof of stake	Phishing	No	Not specified	Yes	No	Not specified	Precision, recall, and f-measure
[28]	Hyperledger	Not specified	DDoS	No	IoT	Yes	No	Python v.3.8, Stacheldraht v.1.666	Not specified
[29]	Ethereum	Proof of stake	DDoS	Yes	IoT	No, only proof of concept	No	Ethereum Go client nodes v1.13.6, solidity v.0.5.0	Not specified

Table 3. Cont.

Ref.	Blockchain Platform	Consensus Algorithm	Breach Type	Smart Contract	Domain	Implementation	GDPR	Language/Tool Used	Evaluation Metrics
[30]	Ethereum	Proof of stake	DDoS	Yes	IoT	No, only proof of concept	No	Ethereum Go client v1.13.6 (geth)	Not specified
[31]	Ethereum	Proof of stake	DDoS	Yes	IoT/Fog Computing	Yes	No	Python v.3.8	Accuracy, detection rate, and false alarm
[32]	Ethereum	Proof of stake	DDoS	Yes	Not specified	Yes	No	Ethereum Virtual Machine v1.13.8, solidity v.0.5.0	Gas cost
[33]	Ethereum	Not specified	DDoS	Yes	IoT	Yes	No	Not specified	Number of packets with respect to time
[34]	Not specified	Not specified	DDoS	Yes	IoT	No	No	Not specified	Not specified

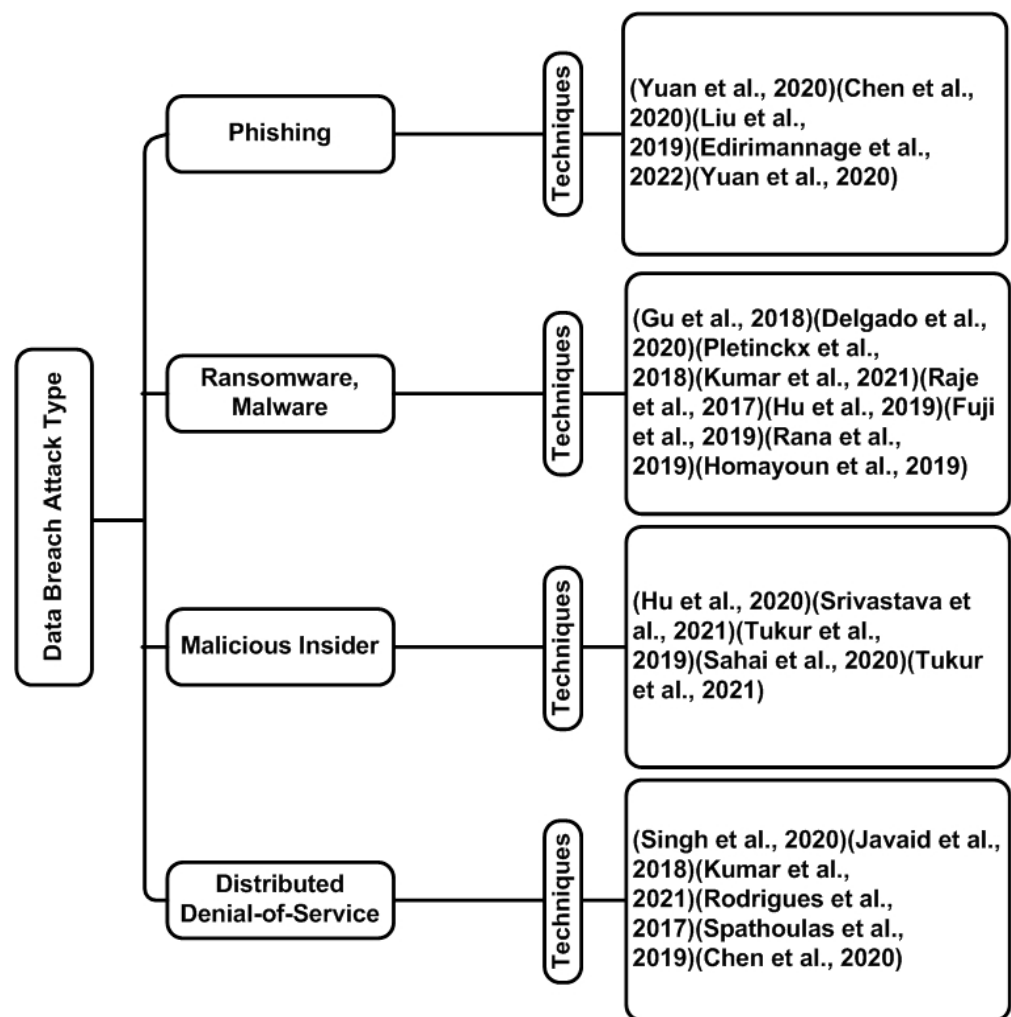


Figure 2. Taxonomy of the literature review [9–34].

A. PHISHING: Third-party hackers carry out phishing attacks by creating websites that look entirely legitimate. They may, for example, construct a site that appears precisely

like PayPal and encourage you to log in to make a necessary change. You will log in and realize that you have given your password to someone else instead of logging in to your account. The hacker can then access the login credentials and do anything they want. Once again, a phishing scam might jeopardize the security of any critical information you or your business own. Many studies on identifying phishing attacks have been conducted to solve this issue. Consider the following examples.

Phishing scam, a typical form of scamming, has a new way of scamming in the blockchain scenario. A practical solution for phishing detection is needed to establish a secure environment for investors. Yuan et al. [23] proposed a framework for mining Ethereum transaction data to detect phishing frauds. The authors have created an Ethereum network based on provided transaction records. The authors used a support vector machine (SVM) to see whether the account was phishing. The experimental results show that the presented phishing detection method's F-score may reach 0.846, indicating that the model is valid.

Phishing scams have taken a massive amount of money and have become a significant risk to the financial security of blockchain users. To address this problem, Chen et al. [24] presented a system in which they offered a systematic way of detecting phishing accounts based on blockchain transactions. The authors used Ethereum as an example to demonstrate its usefulness. Extensive testing has shown that the suggested algorithm can detect phishing fraud.

The consortium blockchain was used to implement the phishing data-sharing technique, as demonstrated by Liu et al. [25]. The four distinct node types—reporting, accounting, service, and supervisory—have their respective tasks represented in the suggested model. It serves as a forum for openness, cooperation between multiple parties, effective coordination, multi-source reporting, and anti-tamper accounting.

Blacklisted URLs are a common Internet security strategy that shields users from malicious websites, financial fraud, and other cyberattacks. In contrast, the Phish Chain technique for blacklisting phishing URLs was presented by Edirimannage et al. [26]. Phish Chain is a transparent, totally decentralized phishing URL blacklisting system run by a group of people as opposed to a single organization. Smart contracts on the Quorum blockchain are used to implement the intended feature.

Yuan et al. [27] proposed a novel approach to solving the phishing detection problem on Ethereum. The authors used an approved platform to retrieve the marked phishing addresses and transaction data. The authors construct many relevant subgraphs based on the transaction records obtained. To determine whether the address is a phishing scammer, the authors used an SVM (support vector machine). The experimental findings reveal that the proposed methodology outperformed the competition in the final classification challenge for phishing detection on Ethereum.

B. MALWARE/RANSOMWARE: Malware or viruses can infect users' computers to erase their data. Any company, specifically those that depend on data, might be affected. If a computer virus infects a hospital, it can potentially wipe out millions of individuals' information. Users should not click on anything they are unsure about to prevent the computer from becoming infected with this malware. Many studies on identifying malware attacks have been conducted to solve this issue. Consider the following examples: Gu et al. [14] proposed a blockchain-based framework comprising a consortium and public chains. To tackle detecting malicious coding in malware and retrieving the corresponding proofs in mobile devices. The authors developed a multi-feature detection approach for an Android-based system to identify and categorize malware. Furthermore, the authors created a fact-based Android harmful software using blockchain technology. The experiments' results reveal that, compared to previous studies' algorithms, the new suggested technique may achieve greater detection accuracy in less time with reduced false-positive and false-negative rates. A blockchain-based innovative method for identifying malware activities is presented by Kumar et al. [17]. Millions of Android program features were kept in the blockchain database to increase security for IoT devices in real-time scenarios.

The smart contract verifies the malicious application while uploading and downloading Android programs over the network. It can approve or reject the distribution and download of potentially harmful Android applications.

The design and implementation of a decentralized firewall system driven by a unique malware detection engine are described by Raje et al. [18]. Blockchain technology is used to construct firewalls. The detection engine classified Portable Executable (PE) files as malicious or benign. A deep-belief neural network (DBN) is used as the detecting engine for file classification. The DBN is trained using an extensive data set of 10,000 files. Validation is performed on 4000 files that have never been exposed to the Internet. Building consensus in the blockchain network based on proof of work is the final decision on whether to accept or block a file.

An innovative firmware update mechanism for IoT devices is proposed by Hu et al. [19]. The suggested solution is built on blockchain technology and uses smart contracts to ensure firmware integrity and virus resistance. Furthermore, by validating several request signatures the suggested platform dramatically enhances system scalability. Compared to the existing literature, extensive analysis and performance simulations have shown that the proposed strategy may achieve high operational efficiency for IoT devices in computing costs and communication overhead.

Fuji et al. [20] presented a blockchain technology system to distribute and use signatures of suspicious malware files. Without a centralized entity, this approach attempts to rapidly transmit signatures of suspicious items among users and increase the accuracy of malware detection and elimination. The authors built a prototype of the suggested system and tested its accuracy in identifying and eliminating malware in the testing experiment. According to the evaluation results, the proposed approach enhanced the FNR by around 4% and the FPR by about 2.5 percent.

Rana et al. [21] investigated various machine-learning models in a consortium blockchain network for a specific dataset. The decentralized network provides transparency, enhances security, and reduces the expense of managing all crucial data by eliminating intermediaries. The authors built a blockchain-based malware detection system to detect and stop unexpected hostile attacks on a network. The authors conducted additional experiments to improve malware detection using different datasets and machine-learning techniques.

Homayoun et al. [22] presented a blockchain-based malware attack detection mechanism for identifying fraudulent mobile apps in mobile app marketplaces. The structure comprises a dual private blockchain with two private blockchains (internal and external) and a consortium blockchain for the ultimate decision. The external blockchain saves detection results as blocks for current versions of apps, while the internal private blockchain keeps feature blocks extracted by feature extractors. The proposed system also allows third parties to contribute feature blocks, which aids antimalware providers in providing more accurate solutions.

Ransomware is usually utilized against firms that require immediate access to information, such as hospitals. However, this is not always the case. A hacker gains access to the firm's computer system and disables it. The company or user is charged money to restore or wipe their data. Many studies on identifying ransomware attacks have been conducted to solve this issue. Consider the following examples:

Pletinckx et al. [16] propose the first blockchain-based ransomware solution, which utilizes smart contracts and primitive cryptographic primitives. Smart contracts would allow additional ransomware capabilities, such as paying for specific files or returning the ransom to the victim within a certain time. The Ethereum Ropsten test network has been adopted to implement the proposed methodology. Finally, the findings show no practical alternatives if these strategies are implemented in public blockchains. As a result, we are concerned that it is becoming increasingly essential to notice and investigate this issue to develop new regulations and innovative solutions.

The discovery of a new sort of malware coordination based on the blockchain is described by Delgado et al. [15]. This method, seen in the Cerber ransomware field, allows

the malware owner to alter the site of the control system in real time without generating a single NXDomain packet, making network-based anomaly detection more difficult.

C. DISTRIBUTED DENIAL OF SERVICE: A distributed denial-of-service (DDoS) attack occurs when a website receives a significant number of requests, making it unavailable to other users. Using this form of attack will make it difficult for employees to sign into the system. While the data is not necessarily lost, the company must halt operations until the security problem is fixed. A data breach of this type is more likely to occur in larger companies. Because it takes a well-coordinated effort, individuals are rarely targeted.

There are two ways to defend against (DDoS) attacks. First and foremost, protect your network, resources, and other data assets from this massive assault. Second, to prevent your network from becoming a botnet that launches threats on different networks and resources, an operations center should primarily control your network. The author's focus was the invention of a blockchain-based botnet deflection system for the Internet of Things (IoT) [28]. The authors simulated and investigated ways to identify and combat botnets using blockchain and software-defined networking and protect our devices from falling into the hands of attackers.

Researchers have developed several strategies to combat DDoS attacks. The study [29] uses blockchain technology, one of the newest and most promising technologies, to combat DDoS attacks. Research on blockchain-based DDoS solutions is presented by Singh et al. [29]. The authors have also assessed and analyzed existing blockchain-based DDoS mitigation solutions. This proposed study makes it easier to build future research ideas in blockchain technology, which is still in its early stages.

Javaid et al. [30] proposed a system that integrates IoT devices with blockchain to overcome DDoS security challenges in the IoT. This work replaces the IoT infrastructure with a decentralized one using Ethereum, a blockchain variation, and smart contracts. Smart contracts are then used to allow IoT devices to connect to the network. By leveraging static resource allocation for instruments, the IoT and Ethereum combine to protect unauthorized devices from accessing the server and solve DDoS attacks.

Kumar et al. [31] focused on different vulnerabilities and cyberattacks in smart contract-based blockchain IoT systems, including DDoS attacks. This article presents a distributed intrusion detection architecture based on fog computing for detecting DDoS attacks. For early threat detection, the proposed system incorporates AI and fog nodes. Furthermore, to keep data off-chain, IPFS-based distributed file storage is recommended. The proposed framework's performance is assessed using a real BoT-IoT dataset and compared to various current state-of-the-art methodologies regarding accuracy, precision, F1 score, and detection rate. The suggested distributed framework's findings demonstrate that it successfully detects attacks such as DoS, DDoS, and other current threats in the blockchain IoT network.

Smart contracts and blockchain technologies were used by Rodrigues et al. [32] to develop a unique architecture. The blockchain offers a simple and efficient structure for developing a collaborative approach to DDoS attack mitigation as a distributed and mostly public storage system. The presented architecture may be used with existing DDoS defense systems to provide extra security.

Spathoulas et al. [33] recommended using lightweight agents to collaboratively identify DDoS attacks (using IoT device botnets). Agents, in particular, transmit outward traffic information to detect potential DDoS victims. A blockchain smart contract controls this information flow, ensuring the integrity of the operation and the data. Chen et al. [34] presented a blockchain DDoS attack protection mechanism for IoT devices. This technique collects network traffic features from edge nodes, analyzes retrieved data, identifies irrational behavior from terminal devices, and implements DDoS attack protection using smart contracts in the blockchain network.

D. MALICIOUS INSIDERS: Your employees know how your company works and operates and how important data may be accessed and secured. Therefore, personnel must be properly taught, and security processes must be enforced. Access controls are an essential aspect of a company's security procedures. Employees can only view records

relevant to their employment by using these to limit the information available to them. Meanwhile, sensitive material should be subject to significant restrictions to guarantee that only trusted top-level staff can access it. This lowers the chances of an employee intentionally leaking personal or financial information.

One of the most critical concerns in cybersecurity has always been the insider threat. The attacker has permitted access to the system on the internal network [35]. They may also have a thorough grasp of the system's security rules and methods, allowing them to circumvent its security features quickly. Many non-blockchain-based studies [36–50] for detecting insider threat have been conducted. However, our focus in this survey is on blockchain-based data breach detection studies. Several blockchain-based studies have been conducted to solve the insider threat issue. Consider the following examples:

Hu et al. [9] presented a blockchain-based internal network insider threat model that uses real insider threat scenarios. The proposed blockchain-based system also includes data format, transactional structure, consensus mechanism, information storage algorithm, data retrieval algorithm, and other features to protect user data security. By developing this blockchain-based system and performing tests in a simulated setting, the authors show that the blockchain can accomplish the primary mission of reducing internal attack risks. Srivastava et al. [10] presented a data alteration detection approach based on blockchain technology's tamper-resistant characteristic. The model has been evaluated, and it discovered that any illegal database changes might be identified using the blockchain database API. The authors constructed and tested the concept on a web-based application to make it resistant to insider attacks. In the future scope of this study, the authors address a machine-learning-based detection approach. The results of the experiments demonstrate that the suggested design performs well, and the comparative findings show that the proposed architecture outperforms similar models.

Tukur et al. [11] examined the insider threat to the IoT to investigate the impact of tampering with the sensing environment on the entire IoT system. The authors intended to see how changing the ambient state in the IoT perception layer impacts the data integrity received by sensors and propose a technique to keep the system data safe. According to the authors, insiders affect physical features about which data are gathered and communicated, fooling sensors into receiving false data. The authors designed a system that connects the blockchain platform and edge computing to execute checks and maintain the integrity of transmitting sensor data before it is examined, processed, and stored.

Sahai et al. [12] presented Verity, a one-of-a-kind solution for detecting insider threats in databases. Verity is a dataless system that allows any blockchain network to record fixed-length signatures of records from any SQL database without requiring complete data movement. Verity employs a methodology for monitoring SQL queries' responses to validate the tuples' integrity using the blockchain's fingerprints and identifying insider attacks. The authors used Hyperledger Fabric and an SQLite database to develop this strategy. Results show that any tuple integrity checking cost remains unchanged per row and grows linearly.

Tukur et al. [13] developed an edge-based blockchain-enabled anomaly detection solution for IoT insider threats. The method uses edge computing to minimize latency and bandwidth needs by bringing computation adjacent to the IoT nodes, thus enhancing availability, and reducing single points of failure. It then employs some components of sequence-based outlier detection while combining distributed edge with blockchain, which provides smart contracts for detecting and correcting anomalies in sensor data. The approach was evaluated using realistic IoT system datasets and fulfilling the intended goal while assuring data quality and availability, which are essential to IoT success. Researchers have developed several non-blockchain-based approaches [43–46,48,51–74] to detect data breaches (phishing, malware, insider attack, and distributed denial of service). However, our focus in this survey is on blockchain-based data breach detection studies. Blockchain technology has the potential to improve data breach detection and prevention, but it

also introduces new challenges and complexities. These challenges are discussed in the subsequent section along with recommendations.

How has previous research specifically utilized blockchain to enhance data breach detection?

Previous studies have effectively used blockchain technology to improve data breach detection in many different areas. Showing its potential to strengthen security procedures, here is an in-depth analysis of how blockchain has been used:

Sharma et al. [75] employed a tamper-free and transparent ledger to create a tamper-free and visible data storage system. A blockchain has a distributed ledger, which means that data are stored on multiple nodes in a network. This makes it impossible for the attackers to manipulate information by simply hacking a system. The process makes unauthorized changes difficult, hence ensuring confidentiality.

Authentication processes are improved by employing blockchain consensus techniques and cryptographic algorithms. Blockchain has been found to enhance user authentication security by Kang et al. [76] in the identity verification process. This is more important in preventing frauds and ensuring confidentiality of such data.

Azbeq et al. [77] used smart contracts, which are self-executing contracts where the conditions of the agreement are embedded into the code, to enforce access control policies. They used smart contracts to control access in authoring. Also, these programmable contracts run predefined rules in the background, and only authorized people or systems access some data. This helps to control data access and prevent data breaches.

Blockchain has been applied to real-time monitoring and alerting in data breach detection using the transparent and auditable feature. Blockchain is time-stamped and cannot be altered in each of its transactions or transaction alteration made. Pelekoudas et al. [78] have used this functionality to create tamper-proof audit trails that make it possible for organizations to detect and respond to data breaches quickly.

Chatziamanetoglou et al. [79] explored using blockchain to create decentralized systems for sharing threat intelligence. This allows different entities, like companies or security agencies, to share information about potential risks or breaches securely, without risking the confidentiality of the data.

Parlak et al. [80] used blockchain's immutability feature to create immutable forensic recordings. This ensures that if an incident occurs, the records relating to the breach are preserved and can be used for post-event analysis, forensic investigations, and compliance purposes.

In summary, previous studies have identified the potential of blockchain in enhancing data breach detection by developing safe, transparent, and auditable systems, as summarized in Table 4. These deployments cover data storage, authentication, access control, monitoring, and even collaborative threat intelligence. This highlights blockchain's diversity in improving cybersecurity.

Which components or aspects of traditional data breach detection systems were replaced or augmented by blockchain technology??

Previous research has shown that blockchain technology can be integrated into numerous components of traditional data breach detection systems, either replacing or enhancing existing techniques. A more in-depth analysis is discussed below Table 5:

Table 4. Blockchain utilization to enhance data breach detection.

Features	References	Employed	Domain
Distributed and tamper-proof ledger	Sharma et al. [75]	For transparent data storage system	Multitenant data storage
Authentication process	Kang et al. [76]	For controlling and monitoring data access	Product traceability
Smart contracts for access control	Azbeq et al. [77]	To enforce access control policies	Disease management
Monitoring and alerting mechanisms	Pelekoudas et al. [78]	For real-time monitoring and alerting	Healthcare monitoring system
Decentralized threat intelligence sharing	Chatziamanetoglou et al. [79]	To securely share information	Cyber threat intelligence
Immutable forensic records	Parlak et al. [80]	To create immutable forensic records	Vehicle accidents in insurance

Table 5. Components augmented by blockchain technology.

Reference	Components/Aspects	Blockchain Replaces
Azbeq et al. [81]	Data Storage Level	Centralized databases with distributed ledgers, ensuring redundancy. It augments storage with cryptographic hashing, ensuring security.
Asif et al. [82]	Authentication Process	Traditional authentication with decentralized identity management, enhancing security through cryptographic techniques and user-controlled cryptographic keys.
Namane et al. [83]	Access Control	Centralized access control with smart contracts for decentralized and automated authorization, augmenting access control with transparent access logs.
Pelekoudas et al. [78]	Monitoring and Alerting Mechanisms	Centralized monitoring with decentralized mechanisms for real-time visibility and augments it with tamper-proof audit trails for enhanced breach detection.
Aslam et al. [84]	Transaction Verification and Consensus	Centralized transaction verification with decentralized consensus, reducing fraud risk. Augmentation enhances verification integrity for robust data breach detection.

Traditional centralized databases (prone to single points of failure) have been replaced in [81] by blockchain's decentralized and distributed ledger systems. In blockchain, each network participant keeps a copy of the whole data ledger, ensuring redundancy and reliability. By introducing cryptographic hashing and consensus methods, blockchain augments data storage. The adoption of these technologies secures the integrity and immutability of data. Thus, tamper-proof records prevent unauthorized alterations and give an extra layer of security.

Asif et al. [82] have proposed blockchain-based decentralized identity management systems to replace standard username/password-based authentication. In this system, users retain control over their identities through the use of cryptographic keys, eliminating their dependence on centralized authorities. By utilizing cryptographic mechanisms, blockchain improves authentication. The users have their cryptographic keys that are linked to their identities, thereby improving security and resistance against fraud.

In [83], smart contracts have been used to replace access control lists and access management systems. In a nutshell, these self-executing contracts automate access control based on the pre-established rules in a decentralized and automated permissions manner. Transparent access logs provide an added boost to access control. The blockchain ensures

that the details of every transaction are stored and can be audited securely and unalterably. This increases visibility, leading monitoring and breach detection.

Pelekoudas et al. [78] have proposed a blockchain-based healthcare monitoring system. The systems have major features such as real-time network visibility and automated notifications regarding suspicious activities. Blockchain improves monitoring and alerting through tamper-proof audit trails. Time-stamped records in the blockchain provide a foundation for forensic analysis and breach detection.

Aslam et al. have used blockchain technology that replaces the centralized authorities (that verify transactions) with decentralized consensus methods. This includes consensus-based verification techniques such as proof of work or proof of stake to improve transaction verification with blockchain. These methods make the verification more accurate, thus contributing to better data breach detection.

Conclusively, prior research has integrated blockchain technology in multiple aspects of the conventional data breach detection mechanism. Through blockchain technology, data storage, authentication, access control, monitoring, and verification of transfers are made better, with the result that security, resilience, and transparency are ensured in the event of a data breach.

4. Breach Scenarios Arising from Technical Failures

The security of transaction verification for a variety of shards and transaction types is examined by the authors of paper [85]. The results imply that transaction security may be impacted by the size of shards and the quantity of validating nodes. The paper highlights that these effects can be lessened by distributing attesting nodes randomly, which will ultimately improve the consensus's dependability within shards.

In the paper [86], wireless blockchain networks (WBNs) with varying consensus mechanisms (CMs) are introduced, and the issue regarding which communication resources are needed to run such a network is addressed. It starts by describing how communication functions within the four steps of the blockchain process. Next, the emphasis switches to examining the connection between WBN performance and communication resource provisioning, with a particular examination of three widely used blockchain CMs: proof of work (PoW), practical Byzantine Fault Tolerant (PBFT), and Raft. The final section of the study [86] presents simulated and analytical results that show how blockchain performance is affected by communication resource provisioning.

The following scenarios of data breaches highlight how crucial it is to fix technical issues, whether they stem from communication protocols, mining vulnerabilities, sharding, consensus algorithms, forking strategies, or detrimental consensus practices. Gaining an understanding of these situations might help strengthen cybersecurity protocols and systems in order to prevent and reduce such breaches.

Flaw of Consensus Algorithms: A consensus algorithm is used by a decentralized network to validate transactions. A weakness in the consensus algorithm compromises the decision-making process, which gives bad actors the ability to rig transaction approvals. Because the compromised consensus is unable to maintain the network's security, this breach leads to unauthorized access to private user data.

Vulnerability of Sharding: To achieve scalability, a blockchain network uses sharding to spread data among several nodes. Attackers can compromise the integrity of the entire system by taking advantage of flaws in one shard thanks to a sharding implementation vulnerability. Unauthorized data access results from this breach because the compromised shard serves as a gateway for hostile activity.

Exploitation of the Forking Technique: A software update or community disagreement causes a blockchain network to split. By using the fork to start a parallel chain, malicious actors can reroute transactions and jeopardize the integrity of the network. By taking advantage of the lack of synchronization, this hack permits unauthorized access to data on both the original and forked chains.

Negative Consensus Behaviors: A malicious party gains control of the majority of staking power on a proof-of-stake blockchain, jeopardizing the consensus process. Because of this concentration of power, the attacker can tamper with transaction validations and alter the ledger without authorization. Unauthorized access to private information and data modification are the outcomes of the breach.

Manipulation in Mining: An attacker takes control of a sizable amount of the mining power in a proof-of-work blockchain. By interfering with the validation procedure, this modification gives the attacker access to add false transactions to the blockchain. The breach jeopardizes the general security of the network and causes transaction records to be altered without authorization.

Failure of the Communication Protocol: Node interactions in a dispersed network are dependent on a particular communication protocol. An attacker can intercept and alter communication between nodes if there is a protocol breakdown. The security and integrity of the data are put at risk because of this breach, which makes it possible for unauthorized parties to access sensitive information being transferred over the network.

Exploitation of Smart Contracts: Smart contracts are used by decentralized applications (DApps) to carry out transactions. Attackers can take advantage of flaws in the smart contract code to carry out unauthorized transactions and manipulate data. The DApp’s user data and financial transactions are compromised as a result of this hack.

Inadequate Communication Encryption: A dispersed network fails to provide strong encryption for node-to-node communication. Attackers use this carelessness as a means of intercepting and decoding private data being sent back and forth between nodes. The compromise jeopardizes the confidentiality of communications within the network by allowing unauthorized access to sensitive data. Furthermore, potential challenges and problems associated with blockchain in data breach detection are presented in Table 6.

Table 6. Potential challenges and problems associated with blockchain in data breach detection.

Challenge	Problem
Public blockchain networks have scalability issues when they handle a large number of transactions in parallel.	When handling data breach detection situations, the network might get congested, resulting in slower transaction processing times and increased costs.
Reaching agreement in blockchain networks is a time-consuming process, and, therefore, the speed of transaction is affected.	Responses must be timely in data breach detection. As a result, slow transaction processing can hamper timely detection and response.
Blockchain technology may not fit into legacy systems.	For organizations with existing infrastructure, integration of blockchain into the data breach detection systems can be hard and may require a lot of modification.
For instance, many common blockchain consensus mechanisms use PoW, which is quite costly in terms of energy.	Environmental concerns and high operational costs are due to the high energy consumption.
The development of blockchain technology may be much faster than regulatory frameworks.	Regulation adherence is necessary for data breach detection systems, and noncompliance with current laws may serve as grounds for legal action.
Interoperability of different blockchain platforms.	Detecting data breaches requires smooth communication between different systems.

Specific Use Cases and Successful Implementations:

1. **Guardtime—KSI Blockchain:** Guardtime’s Keyless Signature Infrastructure (KSI) [87] blockchain verifies the integrity of the data. Real-time data integrity and log-tampering protection are also guaranteed by KSI. Data breaches have been successfully detected by using it in the security and healthcare industries.
2. **IBM Food Trust:** Blockchain technology is used by the food supply chain IBM Food Trust [88] to enable traceability. Blockchain technology has also proven to be use-

ful in quickly detecting and identifying compromised food goods throughout the supply chain.

3. Walmart's Blockchain for Pharmaceutical Traceability: Walmart [89] uses blockchain technology to monitor the pharmaceutical supply chain. In order to guarantee the legitimacy and security of goods, the system also enhances traceability and assists in identifying breaches in the pharmaceutical supply chain.

In summary, blockchain offers significant advantages in terms of data breach detection; however, factors such as scalability, interoperability, and regulatory compliance should be taken into account. Blockchain can be utilized for breach detection and sensitive information security, as demonstrated by some successful traceability and integrity verification applications. Lessons from these examples can be applied in the future to develop robust data breach detection systems using blockchain technology.

5. Challenges and Recommendations for Future Directions

Blockchain technology can potentially improve data breach detection and prevention but also brings new difficulties and complexities. When using blockchain technology to detect data breaches, the following difficulties could arise:

Incompatibility: The regulatory environment for data protection and blockchain is continually developing. It can be difficult to comply with data protection standards like GDPR while using blockchain to detect data breaches. While the General Data Protection Regulation (GDPR) gives individuals in the EU and EEA more control over their data, the rising blockchain technology appears to be against a significant challenge in complying with the new regulation. While the GDPR provides EU and EEA citizens more control over their data, the emerging blockchain technology faces significant compliance challenges with the new rule. Blockchain and the GDPR are incompatible. GDPR promises to give consumers more control over their data by allowing them to see how it is used and the ability to change or remove it.

On the other hand, blockchain technology has "immutability" as one of its cores. Blockchain makes it challenging to alter or remove any data kept on the chain by combining cryptography and decentralization. If any personal data is maintained on a blockchain, this is a clear violation of the GDPR, exposing the organization to GDPR penalties. As a result, if a blockchain's architecture is developed adequately with GDPR in mind, with only public keys saved on the blockchain and any off-chain personal data encrypted and unavailable to blockchain developers or miners, GDPR's rights to deletion, correction, and data transfer are unaffected.

Recommendations: The GDPR requirements can be met to solve the problem by making the data inaccessible. Data should be made unavailable when someone requests that it be destroyed by utilizing encryption. Ciphertext or encrypted entries are stored on a blockchain, while the key pair is kept off the chain. The data controller can remove the key if the data owner requests that the data be deleted, rendering the information unreachable. Another solution is to keep the personal information "off the chain" instead of "on the chain". Deleting or changing the information on a blockchain is hard, since it is accessible on an open network or "on the chain".

Latency: The difficulty is that blockchain transactions need consensus methods, which might cause latency. Transaction processing delays could not be acceptable in cases involving time-sensitive data breaches.

Recommendations: To ensure that threat detection and response can occur on time, addressing latency issues with blockchain technology while detecting data breaches is essential. Traditional real-time detection technologies can be combined with blockchain in hybrid strategies to help address this issue.

Privacy issues: Blockchains can present privacy issues when handling sensitive data breach information due to their intrinsic transparency. On blockchain, privacy may be compromised by excessive information disclosure.

Recommendations: Strategies like zero-knowledge proofs and private transactions can be used to increase privacy on blockchain networks while maintaining the ability to identify data breaches. Employ privacy-preserving techniques like zero-knowledge proofs, confidential transactions, and differential privacy to conceal sensitive data while enabling validation to improve privacy in blockchain-based data breach detection. Inquire about utilizing consortium blockchains with controlled access and privacy-focused coins. Keep only the bare minimum of data on-chain, encrypt it, and permit selective publication. To balance data security and privacy, adhere to privacy laws, provide users control over their data and the option to consent, and emphasize suitability rather than visibility.

Resource Intensiveness: Blockchain systems can require a lot of resources, particularly in computing and energy use. For certain organizations, implementing resource-intensive solutions might not be feasible.

Recommendations: Blockchain platforms and resource-efficient consensus techniques may solve this problem. Techniques like layer-2 scaling solutions, efficient smart contracts, and off-chain processing should be utilized to minimize the resource-intensive nature of blockchain technology in data breach detection. To maximize the use of resources, use parallel processing, effective data structures, and resource monitoring. Resource allocation can be optimized through hybrid techniques, distributed processing, and selective blockchain utilization. Regular performance testing, energy-efficient hardware, load balancing, and resource-aware design will all contribute to successful resource management without jeopardizing the security and efficacy of blockchain-based data breach detection.

Integration Barrier: The difficulty is that integrating blockchain-based solutions with current security procedures and infrastructure can be time-consuming and expensive. Compatibility problems could occur.

Recommendations: Adopt techniques prioritizing compatibility and seamless interaction with current security infrastructure to overcome integration challenges when deploying blockchain technology for data breach detection. Use blockchain interoperability tools to fill gaps between systems and guarantee continuous data flow. Implement standardized APIs and communication protocols that simplify integrating security and old software. To simplify the onboarding process for security personnel, create clear documentation and offer strong support. Work closely with IT and security professionals to design and perfect the blockchain integration and ensure it complies with the organization's unique security demands and compliance regulations.

User Adoption: Because blockchain technology may not be well known to users and businesses, it might be difficult to implement and successfully administer.

Recommendations: Through training and education programs, users can learn how to interact with blockchain-based security solutions. Focus on user education and engagement to overcome the difficulty in getting users to accept blockchain technology for data breach detection. Create thorough training courses and other materials to inform users of the advantages of blockchain technology and how it improves security.

6. Conclusions and Future Work

Blockchain's potential is extensive as it is cutting-edge technology. Researchers and businesses worldwide have used blockchain's advantages to tackle the issue of data breaches. Many authors discussed breach detection methods based on blockchain technology. However, to the best of our knowledge, no survey covers all these blockchain-based options for detecting data breaches, so we decided to fill that research gap. In this survey, we investigate blockchain-based data breach detection techniques developed so far to deal with data breach detection. We compare existing blockchain-based data breach detection solutions based on type, platform, smart contracts, consensus algorithm language/tool, and assessment measures. A taxonomy of current data breach types is also presented. We conclude our research by summarizing the challenges that present approaches experience, proposing solutions, and guiding the way forward. This survey aims to comprehensively review and highlight current and future issues and genuine concerns in this field. We

believe that our research may be used as a guide for researchers interested in investigating the usage of blockchain in data breaches.

Future researchers in the rapidly developing field of cybersecurity will greatly benefit from this study. This study will act as a thorough review of current approaches, difficulties, and new developments in blockchain-based data breach detection, giving academics a vital starting point for comprehending the current environment. It will highlight areas that are ready for investigation, which encourage future research directions in addition to pointing out gaps and limitations. This survey will serve as a guide, providing information on the advantages and disadvantages of the methods already in use. This will help researchers advance their understanding and improve the quality of their innovative work. It will also function as a benchmarking tool, enabling researchers to compare their results with the existing literature and promoting a comparative study of various approaches.

Furthermore, the future directions for blockchain-based data breach detection systems are as follows:

Examine how modern AI/ML algorithms and blockchain may work together to find anomalies with greater complexity. Develop hybrid systems which utilize the analytical powers of AI and the tamper-proof nature of blockchain to improve detection accuracy and reduce false positives and negatives.

- To obtain additional scalability and fewer transaction fees, check into Layer 2 solutions or alternative blockchain platforms.
- Examine blockchain networks' privacy-preserving techniques by paying particular attention to how they handle sensitive personal data. Develop and examine techniques like homomorphic encryption and zero-knowledge proof to preserve privacy and safeguard breach detection procedures.
- Examine the potential and benefits of hybrid blockchain technologies in order to achieve a balance between efficiency and transparency. Adopt hybrid solutions to provide a safe and adaptable environment for identifying data breaches. These solutions combine the advantages of public and private blockchains.
- Conduct extensive testing in many real-world scenarios to fully validate the system. To simulate sophisticated insider attacks, conduct more complex penetration testing or stress testing for high transaction volumes.
- Collect feedback and views from prospective end users and other stakeholders, such as data protection authorities. When making system enhancements, consider user feedback to ensure that it meets practical requirements and is compliant.
- Study the possibility of incorporating blockchain-based detection of data breaches seamlessly into the existing security systems in a typical organization. Develop solutions that would allow easy integration and compatibility between diverse security frameworks for large-scale adoption and effectiveness.

The future directions seek to enhance the blockchain-based data breach detection with regards to scalability, privacy, real-world applicability, and regulatory compliance. Such exploration will help the researchers to come up with more robust, efficient, and widely adopted mechanisms to avert data breaches.

Funding: This research was funded by National Research Foundation of Korea, grant number NRF-2022R1A2C1012037. This work was also supported in part by the Energy and the Korea Institute of Industrial Technology Evaluation and Management (KEIT), in 2023, under Grant 20022793.

Data Availability Statement: Data sharing is not applicable to this article.

Acknowledgments: The authors are thankful to Science Foundation Ireland (Nos. [13/RC/2106_P2] and [20/SP/8955]) at the ADAPT SFI Research Centre at Maynooth University. ADAPT, the SFI Research Centre for AI-Driven Digital Content Technology is funded by Science Foundation Ireland through the SFI Research Centres Programme.

Conflicts of Interest: Author Jungsuk Kim was employed by the Cellico Company R&D Lab. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The Cellico Company R&D Lab had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

- Samanta, M.; Pal, P.; Mukherjee, A. Prevention of information leakage by modulating the trust uncertainty in Ego-Network. In Proceedings of the 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru, India, 4–8 January 2017; IEEE: New York, NY, USA, 2017; pp. 377–378.
- Kumar, J.; Singh, A.K. Dynamic resource scaling in cloud using neural network and black hole algorithm. In Proceedings of the 2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS), Bhopal, India, 8–9 December 2016; IEEE: New York, NY, USA, 2016; pp. 63–67.
- Homoliak, I.; Toffalini, F.; Guarnizo, J.; Elovici, Y.; Ochoa, M. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Comput. Surv.* **2019**, *52*, 1–40. [CrossRef]
- Insiders, Cybersecurity. Crowd Research Partners. Insider Threat 2017. 2018. Available online: <https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf> (accessed on 15 December 2023).
- Ko, L.L.; Divakaran, D.M.; Liau, Y.S.; Thing, V.L. Insider threat detection and its future directions. *Int. J. Secur. Netw.* **2017**, *12*, 168–187. [CrossRef]
- Ghosh, A.; Dhar, P.; Banerjee, A.; Sanyal, M. A Survey of Data Leakage Detection in Cloud Computing Platform. *Int. J. Sci. Res. Eng. Manag.* **2023**, *7*, 1–6.
- Rauf, U.; Mohsen, F.; Wei, Z. A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. *J. Cyber Secur. Mobil.* **2023**, *12*, 221–252.
- Ebadinezhad, S. A Systematic Literature Review on Information Security Leakage: Evaluating Security Threat. In Proceedings of the Third International Conference on Sustainable Expert Systems: ICSES, Lalitpur, Nepal, 9–10 September 2022; Springer Nature: Singapore, 2023; pp. 993–1007.
- Hu, T.; Xin, B.; Liu, X.; Chen, T.; Ding, K.; Zhang, X. Tracking the Insider Attacker: A Blockchain Traceability System for Insider Threats. *Sensors* **2020**, *20*, 5297. [CrossRef] [PubMed]
- Srivastava, S.; Mohit; Kumar, A.; Jha, S.K.; Dixit, P.; Prakash, S. Event-driven data alteration detection using block-chain. *Secur. Priv.* **2021**, *4*, e146. [CrossRef]
- Tukur, Y.M.; Thakker, D.; Awan, I.U. Ethereum blockchain-based solution to insider threats on perception layer of IoT systems. In Proceedings of the 2019 IEEE Global Conference on Internet of Things (GCIoT), Dubai, United Arab Emirates, 4–7 December 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
- Sahai, S.; Atre, M.; Sharma, S.; Gupta, R.; Shukla, S.K. Verity: Blockchain based framework to detect insider attacks in dbms. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; IEEE: New York, NY, USA, 2020; pp. 26–35.
- Tukur, Y.M.; Thakker, D.; Awan, I. Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4158. [CrossRef]
- Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. Consortium blockchain-based malware detection in mobile devices. *IEEE Access* **2018**, *6*, 12118–12128. [CrossRef]
- Delgado-Mohatar, O.; Sierra-Cámara, J.M.; Anguiano, E. Blockchain-based semi-autonomous ransomware. *Future Gener. Comput. Syst.* **2020**, *112*, 589–603. [CrossRef]
- Pletinckx, S.; Trap, C.; Doerr, C. Malware coordination using the blockchain: An analysis of the cerber ransomware. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; IEEE: New York, NY, USA, 2018; pp. 1–9.
- Kumar, R.; Wang, W.; Kumar, J.; Zakira; Yang, T.; Ali, W. Collective intelligence: Decentralized learning for Android malware detection in IoT with blockchain. *arXiv* **2021**, arXiv:2102.13376.
- Raje, S.; Vaderia, S.; Wilson, N.; Panigrahi, R. Decentralised firewall for malware detection. In Proceedings of the 2017 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 1–2 December 2017; IEEE: New York, NY, USA, 2017; pp. 1–5.
- Hu, J.-W.; Yeh, L.-Y.; Liao, S.-W.; Yang, C.-S. Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices. *Comput. Secur.* **2019**, *86*, 238–252. [CrossRef]
- Fuji, R.; Usuzaki, S.; Aburada, K.; Yamaba, H.; Katayama, T.; Park, M.; Shiratori, N.; Okazaki, N. Investigation on sharing signatures of suspected malware files using blockchain technology. In Proceedings of the International Multi-Conference of Engineers and Computer Scientists (IMECS), Hong Kong, 13–15 March 2019; pp. 94–99.
- Rana, S.; Gudla, C.; Sung, A.H. Evaluating machine learning models on the Ethereum blockchain for Android malware detection. In *Intelligent Computing; Proceedings of the Computing Conference*; Springer: Cham, Switzerland, 2019; pp. 446–461.

22. Homayoun, S.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A blockchain-based framework for detecting malicious mobile applications in app stores. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; IEEE: New York, NY, USA, 2019; pp. 1–4.
23. Yuan, Q.; Huang, B.; Zhang, J.; Wu, J.; Zhang, H.; Zhang, X. Detecting phishing scams on ethereum based on transaction records. In Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, 12–14 October 2020; IEEE: New York, NY, USA, 2020; pp. 1–5.
24. Chen, W.; Guo, X.; Chen, Z.; Zheng, Z.; Lu, Y. Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem. In Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20), Yokohama, Japan, 11–17 July 2020; pp. 4506–4512.
25. Liu, D.; Wang, W.; Wang, Y.; Tan, Y. Phishledger: A decentralized phishing data sharing mechanism. In Proceedings of the 2019 International Electronics Communication Conference, Okinawa, Japan, 7–9 July 2019; pp. 84–89.
26. Edirimannage, S.; Nabeel, M.; Elvitigala, C.; Keppitiyagama, C. PhishChain: A Decentralized and Transparent System to Blacklist Phishing URLs. *arXiv* **2022**, arXiv:2202.07882.
27. Yuan, Z.; Yuan, Q.; Wu, J. Phishing detection on Ethereum via learning representation of transaction subgraphs. In *Blockchain and Trustworthy Systems. BlockSys 2020. Communications in Computer and Information Science*; Springer: Singapore, 2020; pp. 178–191.
28. Qaisar, S.; Basit, A. DDoS botnet prevention using blockchain in software defined internet of things. In Proceedings of the 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 8–12 January 2019; IEEE: New York, NY, USA, 2019; pp. 624–628.
29. Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of blockchain for mitigating the distributed denial of service attacks. *Secur. Priv.* **2020**, *3*, e96. [\[CrossRef\]](#)
30. Javaid, U.; Siang, A.K.; Aman, M.N.; Sikdar, B. Mitigating IoT device-based DDoS attacks using blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 71–76.
31. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4112. [\[CrossRef\]](#)
32. Rodrigues, B.; Bocek, T.; Hausheer, D.; Lareida, A.; Sina, R.; Burkhard, S. *Blockchain-Based Architecture for Collaborative DDoS Mitigation Using Smart Contracts*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 1–4.
33. Spathoulas, G.; Giachoudis, N.; Damiris, G.-P.; Theodoridis, G. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. *Future Internet* **2019**, *11*, 226. [\[CrossRef\]](#)
34. Chen, M.; Tang, X.; Cheng, J.; Xiong, N.; Li, J.; Fan, D. A DDoS attack defense method based on blockchain for IoTs devices. In *Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science*; Springer: Singapore, 2020; pp. 685–694.
35. Silowash, G.J.; Spooner, D.L.; Costa, D.L.; Albrethsen, M.J. *Low-Cost Technical Solutions to Jump Start an Insider Threat Program*; Carnegie-Mellon University: Pittsburgh, PA, USA, 2016.
36. Al-Mhiqani, M.N.; Ahmad, R.; Abidin, Z.Z.; Abdulkareem, K.H.; Mohammed, M.A.; Gupta, D.; Shankar, K. A new intelligent multilayer framework for insider threat detection. *Comput. Electr. Eng.* **2021**, *97*, 107597. [\[CrossRef\]](#)
37. Hong, W.; Yin, J.; You, M.; Wang, H.; Cao, J.; Li, J.; Liu, M. Graph intelligence enhanced bi-channel insider threat detection. In Proceedings of the International Conference on Network and System Security, Denarau Island, Fiji, 9–12 December 2022; Springer Nature: Cham, Switzerland, 2022; pp. 86–102.
38. Haq, M.A.; Khan, M.A.R.; Alshehri, M. Insider Threat Detection Based on NLP Word Embedding and Machine Learning. *Intell. Autom. Soft Comput.* **2022**, *33*, 619–635.
39. Lee, J.; Alghamdi, A.; Zaidi, A.K. Creating a digital twin of an insider threat detection enterprise using model-based systems engineering. In Proceedings of the 2022 IEEE International Systems Conference (SysCon), virtual conference, 25–28 April 2022; IEEE: New York, NY, USA; pp. 1–7.
40. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Detecting Insider Threat via a Cyber-Security Culture Framework. *J. Comput. Inf. Syst.* **2021**, *62*, 706–716. [\[CrossRef\]](#)
41. Ye, X.; Han, M.-M. An improved feature extraction algorithm for insider threat using hidden Markov model on user behavior detection. *Inf. Comput. Secur.* **2020**, *30*, 19–36. [\[CrossRef\]](#)
42. Al-Harrasi, A.; Shaikh, A.K.; Al-Badi, A. Towards protecting organisations' data by preventing data theft by malicious insiders. *Int. J. Organ. Anal.* **2021**, *31*, 875–888. [\[CrossRef\]](#)
43. Pal, P.; Chattopadhyay, P.; Swarnkar, M. Temporal feature aggregation with attention for insider threat detection from activity logs. *Expert Syst. Appl.* **2023**, *224*, 119925. [\[CrossRef\]](#)
44. Alslaiman, M.; Salman, M.I.; Saleh, M.M.; Wang, B. Enhancing false negative and positive rates for efficient insider threat detection. *Comput. Secur.* **2023**, *126*, 103066. [\[CrossRef\]](#)
45. Li, X.; Li, X.; Jia, J.; Li, L.; Yuan, J.; Gao, Y.; Yu, S. A High Accuracy and Adaptive Anomaly Detection Model with Dual-Domain Graph Convolutional Network for Insider Threat Detection. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 1638–1652. [\[CrossRef\]](#)
46. Singh, M.; Mehtre, B.M.; Sangeetha, S.; Govindaraju, V. User Behaviour based Insider Threat Detection using a Hybrid Learning Approach. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 4573–4593. [\[CrossRef\]](#)
47. Al-Shehari, T.; Alsowail, R.A. Random resampling algorithms for addressing the imbalanced dataset classes in insider threat detection. *Int. J. Inf. Secur.* **2022**, *22*, 611–629. [\[CrossRef\]](#)

48. Randive, K.; Mohan, R.; Sivakrishna, A.M. An efficient pattern-based approach for insider threat classification using the image-based feature representation. *J. Inf. Secur. Appl.* **2023**, *73*, 103434. [[CrossRef](#)]
49. Sivakrishna, A.M.; Mohan, R.; Randive, K. AUBIT: An Adaptive User Behaviour Based Insider Threat Detection Technique Using LSTM-Autoencoder. In *Recent Trends in Computational Intelligence and Its Application: Proceedings of the 1st International Conference on Recent Trends in Information Technology and its Application (ICRTITA, 22)*; CRC Press: Boca Raton, FL, USA, 2023; p. 267.
50. Zhu, D.; Sun, H.; Li, N.; Mi, B.; Huang, X. SPYRAPTOR: A Stream-based Smart Query System for Real-Time Threat Hunting within Enterprise. In *Proceedings of the 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Rio de Janeiro, Brazil, 24–26 May 2023*; IEEE: New York, NY, USA, 2023; pp. 1055–1062.
51. Wen, T.; Xiao, Y.; Wang, A.; Wang, H. A novel hybrid feature fusion model for detecting phishing scam on Ethereum using deep neural network. *Expert Syst. Appl.* **2023**, *211*, 118463. [[CrossRef](#)]
52. Wang, L.; Xu, M.; Cheng, H. Phishing scams detection via temporal graph attention network in Ethereum. *Inf. Process. Manag.* **2023**, *60*, 103412. [[CrossRef](#)]
53. Xiong, A.; Tong, Y.; Jiang, C.; Guo, S.; Shao, S.; Huang, J.; Wang, W.; Qi, B. Ethereum phishing detection based on graph neural networks. *IET Blockchain*, 2023; *early view*.
54. Pitre, V.; Joshi, A.; Das, S. Blockchain and Machine Learning Based Approach to Prevent Phishing Attacks. In *Proceedings of the 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 25–27 August 2023*; IEEE: New York, NY, USA, 2023; pp. 1–6.
55. Kim, J.; Lee, S.; Kim, Y.; Ahn, S.; Cho, S. Graph Learning-Based Blockchain Phishing Account Detection with a Heterogeneous Transaction Graph. *Sensors* **2023**, *23*, 463. [[CrossRef](#)]
56. Sharma, A.; Rani, S.; Shah, S.H.; Sharma, R.; Yu, F.; Hassan, M.M. An Efficient Hybrid Deep Learning Model for Denial of Service Detection in Cyber Physical Systems. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2419–2428. [[CrossRef](#)]
57. Quincozes, S.E.; Kazienko, J.F.; Quincozes, V.E. An extended evaluation on machine learning techniques for Denial-of-Service detection in Wireless Sensor Networks. *Internet Things* **2023**, *22*, 100684. [[CrossRef](#)]
58. Samaan, S.S.; Jeiad, H.A. Feature-based real-time distributed denial of service detection in SDN using machine learning and Spark. *Bull. Electr. Eng. Inform.* **2023**, *12*, 2302–2312. [[CrossRef](#)]
59. Yaseen, H.S.; Al-Saadi, A. Q-learning based distributed denial of service detection. *Int. J. Electr. Comput. Eng.* **2023**, *13*, 972. [[CrossRef](#)]
60. Seyam, A.; Nassif, A.B.; Nasir, Q.; AlShabi, M.A. Denial of service detection on industrial control system using BLSTM. In *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V*; SPIE: Bellingham, WA, USA, 2023; Volume 12538, pp. 525–532.
61. Aldhyani, T.H.H.; Alkahtani, H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics* **2023**, *11*, 233. [[CrossRef](#)]
62. Shaukat, K.; Luo, S.; Varadharajan, V. A novel deep learning-based approach for malware detection. *Eng. Appl. Artif. Intell.* **2023**, *122*, 106030. [[CrossRef](#)]
63. Alomari, E.S.; Nuiiaa, R.R.; Alyasseri, Z.A.A.; Mohammed, H.J.; Sani, N.S.; Esa, M.I.; Musawi, B.A. Malware Detection Using Deep Learning and Correlation-Based Feature Selection. *Symmetry* **2023**, *15*, 123. [[CrossRef](#)]
64. De Oliveira, A.S.; Sassi, R.J. Behavioral malware detection using deep graph convolutional neural networks. *TechRxiv* **2023**. [[CrossRef](#)]
65. Zhu, H.-J.; Gu, W.; Wang, L.-M.; Xu, Z.-C.; Sheng, V.S. Android malware detection based on multi-head squeeze-and-excitation residual network. *Expert Syst. Appl.* **2023**, *212*, 118705. [[CrossRef](#)]
66. Al-Andoli, M.N.; Sim, K.S.; Tan, S.C.; Goh, P.Y.; Lim, C.P. An Ensemble-Based Parallel Deep Learning Classifier with PSO-BP Optimization for Malware Detection. *IEEE Access* **2023**, *11*, 76330–76346. [[CrossRef](#)]
67. Fasci, L.S.; Fisichella, M.; Lax, G.; Qian, C. Disarming visualization-based approaches in malware detection systems. *Comput. Secur.* **2023**, *126*, 103062. [[CrossRef](#)]
68. Bhat, P.; Behal, S.; Dutta, K. A system call-based android malware detection approach with homogeneous & heterogeneous ensemble machine learning. *Comput. Secur.* **2023**, *130*, 103277.
69. Zhu, H.; Wei, H.; Wang, L.; Xu, Z.; Sheng, V.S. An effective end-to-end android malware detection method. *Expert Syst. Appl.* **2023**, *218*, 119593. [[CrossRef](#)]
70. Herrera-Silva, J.A.; Hernández-Álvarez, M. Dynamic Feature Dataset for Ransomware Detection Using Machine Learning Algorithms. *Sensors* **2023**, *23*, 1053. [[CrossRef](#)] [[PubMed](#)]
71. Liu, C.; Lu, J.; Feng, W.; Du, E.; Di, L.; Song, Z. MOBIPCR: Efficient, accurate, and strict ML-based mobile malware detection. *Future Gener. Comput. Syst.* **2023**, *144*, 140–150. [[CrossRef](#)]
72. Singh, J.; Sharma, K.; Wazid, M.; Das, A.K. SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme. *Comput. Electr. Eng.* **2023**, *106*, 108601. [[CrossRef](#)]
73. Wu, Y.; Li, M.; Zeng, Q.; Yang, T.; Wang, J.; Fang, Z.; Cheng, L. DroidRL: Feature selection for android malware detection with reinforcement learning. *Comput. Secur.* **2023**, *128*, 103126. [[CrossRef](#)]
74. Wu, Y.; Shi, J.; Wang, P.; Zeng, D.; Sun, C. DeepCatra: Learning flow-and graph-based behaviours for Android malware detection. *IET Inf. Secur.* **2022**, *17*, 118–130. [[CrossRef](#)]

75. Sharma, A.; Kaur, P. Tamper-proof multitenant data storage using blockchain. *Peer-to-Peer Netw. Appl.* **2022**, *16*, 431–449. [[CrossRef](#)]
76. Kang, Y.; Li, Q.; Liu, Y. Trusted Data Analysis and Consensus Mechanism of Product Traceability Based on Blockchain. *Comput. Intell. Neurosci.* **2022**, *2022*, 3035231. [[CrossRef](#)]
77. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 1515–1527. [[CrossRef](#)]
78. Pelekoudas-Oikonomou, F.; Zachos, G.; Papaioannou, M.; de Ree, M.; Ribeiro, J.C.; Mantas, G.; Rodriguez, J. Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. *Sensors* **2022**, *22*, 2449. [[CrossRef](#)] [[PubMed](#)]
79. Chatziamanetoglou, D.; Rantos, K. Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus. *Secur. Commun. Networks* **2023**, *2023*, 3303122. [[CrossRef](#)]
80. Parlak, M. Blockchain-based Immutable Evidence and Decentralized Loss Adjustment for Autonomous Vehicle Accidents in Insurance. *arXiv* **2023**, arXiv:2303.18130.
81. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egypt. Inform. J.* **2022**, *23*, 329–343. [[CrossRef](#)]
82. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-based authentication and trust management mechanism for smart cities. *Sensors* **2022**, *22*, 2604. [[CrossRef](#)]
83. Namane, S.; Ben Dhaou, I. Blockchain-Based Access Control Techniques for IoT Applications. *Electronics* **2022**, *11*, 2225. [[CrossRef](#)]
84. Aslam, T.; Maqbool, A.; Akhtar, M.; Mirza, A.; Khan, M.A.; Khan, W.Z.; Alam, S. Blockchain Based Enhanced ERP Transaction Integrity Architecture and PoET Consensus. *Comput. Mater. Contin.* **2022**, *70*, 1089–1109. [[CrossRef](#)]
85. Yu, D.; Xu, H.; Zhang, L.; Cao, B.; Imran, M.A. Security analysis of sharding in the blockchain system. In Proceedings of the 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Virtual Conference, 13–16 September 2021; IEEE: New York, NY, USA; pp. 1030–1035.
86. Zhang, L.; Xu, H.; Onireti, O.; Imran, M.A.; Cao, B. How Much Communication Resource is Needed to Run a Wireless Blockchain Network? *IEEE Netw.* **2021**, *36*, 128–135. [[CrossRef](#)]
87. Mylrea, M.E.; Gourisetti, S.N.G.; Tatireddy, V.; Kaur, K.J.; Allwardt, C.H.; Singh, R.; Plummer, J.; Bishop, R.; Hahn, A.L. *Keyless Infrastructure Security Solution (KISS): VOLTRON™ KSI® Blockchain Design and Specification*; No. PNNL-28310; Pacific Northwest National Lab. (PNNL): Richland, WA, USA, 2018.
88. Nguyen, H.; Do, L. The Adoption of Blockchain in Food Retail Supply Chain: Case: IBM Food Trust Blockchain and the Food Retail Supply Chain in Malta. 2018. Available online: <https://www.theseus.fi/handle/10024/158615> (accessed on 15 December 2023).
89. Pham, H. The Impact of Blockchain Technology on the Improvement of Food Supply Chain Management: Transparency and Traceability: A Case Study of Walmart and Atria. Available online: <https://www.theseus.fi/handle/10024/157299> (accessed on 15 December 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.