Mitigating IoT Data Management Security Concerns through Blockchain and Machine Learning Based Solutions: Study and Conceptual Design

L. van den Eeden

Supervisors: Chhagan Lal, Mauro Conti

[1]EEMCS, Delft University of Technology, The Netherlands

A Research Paper Submitted to EEMCS Faculty Delft University of Technology,
In Partial Fulfilment of the Requirements
For the Bachelor of Computer Science and Engineering
February 10, 2023

Name of the student: Lars van den Eeden
Final project course: CSE3000 Research Project
Thesis committee: Chhagan Lal, Mauro Conti, Jorge Martinez

Abstract

The Internet of Things industry is expanding rapidly. However, many security breaches occur, and privacy is often at stake in traditional IoT networks. These centralized systems will not be able to cope with dynamically changing environments. In light of these risks, it is crucial to prevent and minimize the chances of attacks occurring. Researchers have attempted to use blockchain for IoT security to ensure data consistency and availability. Fully public decentralized solutions for IoT still face data breaches. On the other hand, machine learning models detect potential attacks to create an effective defense system.

This paper surveys state-of-the-art works looking to integrate blockchain with machine learning to protect data management for the IoT. Before exploring the various implementations, an analysis of multiple surveys that dive deeper into such integrations is made; then, five different blockchain and machine learning integrations. Many papers need a complete security analysis, and the experiments are limited. From studying the relevant integrations, this article presents a new scheme to protect IoT data using a sharded pBFT consensus algorithm to train a global model by distributing machine learning tasks, leveraging transparency to guarantee security.

1 Introduction

The current landscape of the internet of things (IoT) and its security is full of challenges. The IoT consists of billions of small, network-connected devices. If we want to protect our companies, governments, and ourselves, we need a more accurate way to prevent these attacks in a dynamically changing environment. It is predicted that the IoT market will grow by more than a factor of two in 2030 [1]. The demand for secure data transmission is high, networks and storage locations need to be resistant to attacks, and the low latency of data transmission in the IoT is necessary [2]. In 2016, a hacker group launched the Mirai botnet, a network of infected IoT devices [3]. The swarm of hijacked devices was responsible for the outage of multiple major networks. Many more security breaches have affected IoT devices. Even in 2022, a security flaw was found in a video doorbell more than 10 million people are using, enabling a malicious entity to intrude into the system and extract private information [4]. With that in mind, it is paramount that data collection, transmission, and storage happen securely.

Machine learning (ML) and blockchain (BC) technologies have revolutionized many industries. The power of BC is that it provides reliability, transparency, and data accountability inter alia. Meanwhile, ML allows for thorough data analysis, pattern recognition, and modeling vast amounts of data. It provides insights and enables intelligent decision-making through its probabilistic nature. However, not much previous work has been done on combining these two technologies to enhance security in IoT systems. Blockchain-based IoT data management solutions only can alleviate some of the security concerns. ML can identify and prevent malicious IoT data access and modification based on learning from previous attacks [5]. How can we combine BC and ML-based solutions to address security concerns in IoT data management? This survey aims to present a comprehensive analysis of the state-of-the-art BCML integrations.

Traditional IoT networks rely on IoT devices connecting with centralized services backed by data centers. As the IoT continues to expand, trusted data management is crucial for maintaining the data's integrity, confidentiality, and availability. By prioritizing these key factors, the world can accelerate the adoption of IoT technology and unlock its full potential. Earlier studies have proposed secure BC consensus mechanisms and attack detection, using ML models to mitigate attacks that current IoT networks cannot prevent [6] [7] [8] [9] [10]. Previous work has presented a broad overview of the integrations, yet it has not gone into detail with sufficient depth [5] [11] [12]. State-of-the-art research works are often limited to explaining integrations without providing an extensive security analysis of the broad range of attacks that are conceivable in IoT networks. Therefore, extensive research has yet to be conducted on integrating BC and ML (BCML) to handle secure data management.

The main contributions of this paper are:

- Provide an overview of different security attack vectors within the IoT: Section 2.
- A security analysis of state-of-the-art research works on BCML integrations: Section 3.
- A proposal of a secure and generic BCML integration: Section 3.3.

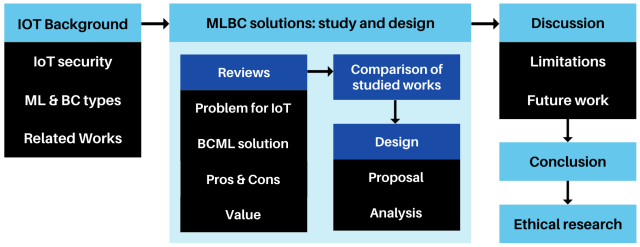

Figure 1: Outline of the structure of this paper

As seen in Figure 1, the report explores the attack concerns first, then comprehensively analyzes various BCML integrations to enhance IoT security, then a design is made, and lastly, the discussion, future research, ethical research, and conclusion will finalize the report. This paper does not fully assess privacy since it is outside the scope of the research question.

2 Background

Before surveying specific integrations, it is necessary to understand the security challenges associated with data management in the IoT. First, the section presents security concerns and examines attacks in the IoT. Second, the BC vulnerabilities and the dangers associated with ML will be explained. Last, relevant similar review works are discussed.

2.1 Security concerns in IoT

Generally, IoT devices are small-sized and are limited in storage capacity and computing power. Therefore, storing a

large amount of information and processing a wide range of functions requiring significant computing power is challenging. Moreover, the security of the devices is often weak, and firmware needs to be updated regularly [13]. Also, the data transmission requirements in most IoT industries are massive: the latency must be less than 10 ms, and the network needs 99.99999% reliability, all while the required throughput is $1 - 100$ Mbps in most sectors [14].

Security can be categorized into three types, the security triad: data Confidentiality, Integrity, and Availability, as seen in Figure 2. Authenticity and non-repudiation are the two values that ensure data integrity. IoT networks are subject to two attacks: active attacks, in which an attacker actively manipulates or modifies the data a device transmits, and passive attacks, in which an attacker gains unauthorized access without being noticed [13]. Solutions to attacks can be categorized into detection, prevention, and mitigation [13].

Table 1 lists the various security concerns for the IoT. Each attack is ranked on a scale of zero to two, with two indicating the highest level of vulnerability to a BC, an ML model, or an IoT network. Zero means that there is a low attack possibility. Finally, the table also includes the likelihood of the attack occurring.

Two papers have suggested 38 solutions to prevent attacks in the IoT [15] [13]. These solutions range from using hashing and signature-based encryption to analyzing node behavior to detect anomalies. However, a one-type solves all security issues solution has yet to exist.

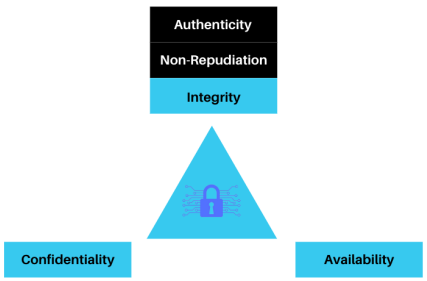

Figure 2: The CIA: confidentiality, integrity, and availability triad.

2.2 Blockchain and Machine Learning

Satoshi Nakamoto introduced the first implementation of BC in 2009 [20]. For the first time, it was achievable to trust unknown participants in a network trying to reach a consensus without reaching central servers. A BC is a chronological list of blocks containing transactions, where each block connects to the longest chain of blocks through cryptographic primitives. In the network, miners validate each new block using consensus algorithms. The "distributed ledger" is nearly unchangeable due to the computational complexity required to perform an attack. After the emergence of the first BC, transactions have become programmable with smart contracts (SC) [21]. These programmable interfaces allow participants to execute and verify code on a BC. The strength of BC is that it offers traceability, fault tolerance, immutability, non-repudiation, and decentralization. Nevertheless, the dilemma with BC remains that it is challenging to satisfy security, scalability, and decentralization simultaneously. This is also known as the BC trilemma.

Attack		Damage			CIA			Risk
Type	**Category**	**BC**	**ML**	**OSI**	**Confidentiality**	**Integrity**	**Availability**	**Likelihood**
Double spending	Double spending	2 [16]			2	2	2	1
51% attack	Consensus	2 [16]				2		1
Sensor overwhelming	Dos	2 [16]		2	1		2	2
(D)Dos attack	Dos	2 [16]		2	1		2	2 [17]
Jamming attack	Dos	2		2	1		2	2
Exhaustion attack	Dos			2			2	2
Buffer overflow	Software	2 [16]		2		2		1 [17]
Adversarial attack	Injection		2 [18]			2		1
Trojan attacks	Malware		2 [18]			2		1
Eavesdropping	MiTM	2 [17]		1 [15]	2			2
Spoofing	MiTM	2 [17]		2 [15]	2	2		2
Routing attacks	Network	2 [16]		2 [15]	1		2	2
Hole attacks	Network	2		2 [15]		2		2
Sybil	Network	2 [16]		2 [15]	2	2		2
Node replication	MiTM		1	2	1	2	2	2
Physical node tampering	Physical		1	2	2	2	2	1
Private key compromise	Cryptography	2 [16]		2	2	2		1
Model stealing	Extraction		2 [19]		2			1
Zero Day attack	Software	1 [16]			2			1
Code vulnerabilities	Software	2 [16]		2 [15]	2		2	1 [15]
Private data extraction	Extraction	1 [16]	2 [19]		2			1

Table 1: The various attack types and their impact on BC, ML, OSI layer technologies; the security CIA triad; the likelihood of the attack. [15] [13] [18] [19]

There are different types of BC. A permissionless BC is accessible and transparent to everyone; a permissioned BC is only accessible to a limited amount of people. A private BC allows one organization to control the BC consensus. In a consortium BC, multiple private BCs join together. A hybrid BC has permissioned and permissionless features. An advantage of a permissioned BC is that it offers access controls and high throughput. A disadvantage of permissioned BCs is that the owners of the consensus nodes need to be trusted. A permissionless BC has upsides: transparency and decentralization, while it also has downsides. It is hard to scale, slow, and frequently energy-inefficient [22].

Ensuring scalability requires a low time-to-finality (TTF) of a transaction, decentralization, and security [23]. Combining the BC trilemma with IoT standards requires a scalable, fault-tolerant, and highly available system, as seen in Figure 3. Off-chain solutions provide ways to ensure scalability. However, the off-chain solutions are centralized and less secure than on-chain solutions due to their local distribution [24] [7]. Zero-knowledge rollups hold the promise to mitigate the trade-offs that sidechains produce. Rollups are designed to let party A show party B they own a secret without disclosing it. For example, ZK-STARKs in PoS are quantum-proof and secure to scale [25]. Despite being proposed, it has yet to be implemented and undergo thorough testing.

Moreover, multiple storage techniques exist. The Inter-Planetary File System (IPFS) is an effective way to store decentralized data, with a retrieval time of 4.3 times that of HTTPS [26]. It uses a Distributed Hash Table (DHT) that references verifiable records. If the user desires data storage on the BC, it can be accomplished through on-chain methods. However, that may result in significant overhead.

The most significant vulnerabilities of the BC are network

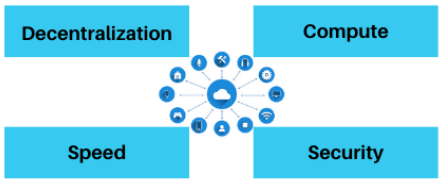

Figure 3: BCML IoT quadrilemma.

attacks. If a group of nodes accumulates more than 51% of the hash power or stake, these may conspire to take control of BC consensus decisions. In the practical Byzantine Fault Tolerance (pBFT) consensus algorithm, the most significant vulnerability is Sybil attacks [16]. Almost all SC-enabled BCs are susceptible to injection attacks [16]. Furthermore, a BC can be forked, creating two distinct chains, and this process comes with some vulnerabilities.

ML can be used to protect the IoT from data access and storage vulnerabilities as an Intrusion Detection System (IDS). ML can be classified into four main categories: supervised, unsupervised, semi-supervised, and deep reinforcement learning [10].

ML is also vulnerable to attacks. Attackers target the state space, reward function, action space, and model space [18] [19]. Common vulnerabilities include adversarial, and trojan attacks [18]. The primary defenses can be mitigated by adversarial training, defensive distillation, robust learning, adversarial detection, benchmarking, watermarking, game theoretic approaches, and pruning. Apart from the attack vulnerabilities of ML, it is a black box: it would be beneficial if it were more transparent and understandable why the model predicted this specific output when attacks occur.

Different BCML solutions exist. Federated learning uses edge devices to train ML models while storing the data on the devices. Other types include using many BC-recorded ML operations and detecting anomalies within a network or system. These IDSs can be categorized into four types. The first two are the detection and prevention of threats. The last two are network-based and host-based intrusion detection or prevention systems: HIDS, NIDS, HIPS, and NIPS. Every type will now be referred to as an IDS. An IDS can be either pre-trained (static), trained while in operation (dynamic), or a mix of both (hybrid).

2.3 Related reviews

This section summarizes and analyzes surveys investigating the junction of ML and BC for IoT. The precise contributions, advantages, and limitations of each work and their value to the research community are explored. This analysis aims to discover the strengths and drawbacks of survey papers that, like this paper, endeavor to provide an exhaustive overview of state-of-the-art integrations.

IoT threats and countermeasures [5] The paper written by Waheed et al. provides an overview of challenges and solutions to security issues in the IoT. First, the paper lists threats in the IoT, both for security and privacy. Then, the authors considered BC and ML solutions separately, examining various algorithms and techniques. Nazar et al. note that BC can provide secure key management, access control, and trust management in IoT systems. They also state that the BC can be used to audit the IoT network and ensure integrity. At the end of the paper, the authors take a step back and look at all issues in the IoT using BCML from a privacy and security perspective.

According to the authors, a hybrid IDS improves detection accuracy, and a dynamic NIDS is practical for securing IoT. The authors have stated that BC papers focusing on security have mentioned the importance of research into intrusion detection and prevention, collective safety, and predictive security for IoT. They note that DL is valuable for detecting zero-day attacks. A critical view of the datasets used to train the DL models is given, suggesting that anyone can change them to train ML models. Therefore, they state that the datasets to be used should be able to be public, removing the possibility of a malicious party to tamper the datasets.

The authors analyze multiple ML-based attack detection papers that address IoT security and privacy concerns. Many IoT use cases, algorithms, datasets, and feature selection methods produce different ML model prediction accuracies. The detailed overviews are useful to obtain a good understanding of the system. However, it is still being determined which of those metrics influenced the prediction accuracies of the ML models and if the accuracy can be improved by training on more datasets.

Waheed et al. categorize the attacks in the IoT well: the overview lists many types of attacks, ML-based IDSs, and BC-based IoT data management methods. A downside is that the analyzed MLBC papers only address spoofing and android attacks. The MLBC integrations are limited to IDSs, even though more types of integrations exist. Also, the research needs quantifiable data and detailed information about the limitations of each integration. Nazar et al. confirm this. They mention that the papers need a more inclusive method to address the privacy and security problems in full detail.

Deep reinforcement learning for BC in IIoT [11] The survey examines how the IoT is used in the Industrial IoT (IIoT) and how this is renewing existing organizations through automation. The amount of data produced by IoT devices is expected to rise quickly in the coming years. However, they note that attacks will become more prevalent, and new types will arise.

The paper's authors pinpoint these hazards and propose solutions by examining various approaches that use DRL for network management and quality of service improvement in IIoT networks. These solutions include hierarchical and decentralized distributed DRL frameworks, federated learning approaches, and ML-based IDSs. To guarantee secure data collection, the authors suggest BC-based strategies. Selections include digital twin solutions for edge networking, federated learning, a BC-based collective Q-learning, and BC-based distributed IDSs. They also highlight the potential of BC technology to improve the adaptability of IoT systems and enhance Deep learning (DL). In the survey, the authors present research that uses IoT devices as data sources and state that selecting the appropriate consensus algorithm is essential to reduce computational overhead. The authors have also devoted a detailed section about open issues in the field. For example, they mention that storage and computing costs must be reduced to improve future data management. They state a fully secure decentralized IoT network becomes feasible by reducing the overhead of storage, having different types of BC, and finding a consensus with a minimum amount of peers that keep the blockchain secure.

Overall, Wu et al. positively contributed to the research community by sharing insights about papers that might help them solve a specific problem by providing researchers with contributions that help mitigate various flaws in the IoT. An improvement would be to include a thorough review of each article assessed. The survey lacks quantifiable data about the security aspects of each paper. Therefore, the survey would be more inclusive by providing a more critical overview.

BC and AI for security and privacy in smart environments [12] The main problems proposed in this paper are that IoT BC networks are vulnerable to network, malware, and availability attacks. Then, the researchers point out that it is feasible to leverage AI to solve some of these BC-related problems. Using AI, security mechanisms within networks can be enabled to detect many types of attacks.

The authors explain the use of BC in different industries and the advantages of using different types of integrations between BC and AI. According to the authors, scalability, cost, security, and trust are the biggest challenges to using BC in smart environments. The authors thoroughly analyze all types of relevant works for MLBC integrations in the paper. It starts with listing the issues for BC and illustrates different methods of how AI is used to prevent attacks. Most surveyed integrations focus on anomaly detection. Oumaima et al. mention that many integrations lack specific BC analysis. A future research direction is to look at how a multi-purpose ML model can use different datasets. Also, anomaly detection engines need to have higher performance.

One of the areas for improvement in this work is the long explanation of the definitions and method. The analysis is exhaustive and includes many integrations ranging from anomaly detection to privacy preservation and scalability boosting types. However, it is limited in providing security details for each solution. Also, the paper loses focus on the original target: finding integrations of BC and AI. Most papers focus on AI instead. Overall, the analysis is broad and covers many papers.

Year	Scheme	Summary
2020	Waheed et al. [27]	Survey on security and privacy-preserving BC and ML solutions. Limited specific BCML integrations are mentioned.
2021	Wu et al. [7]	Assessment of DRL types for IIoT security. Unbiased view, clear perspective on future challenges. Missing critical and detailed analysis.
2022	Oumaima et al. [12]	Assessment of many different BCML integrations for security and privacy, pointing out research gaps in the field. The authors mention there is no one-size fits all solution.

Table 2: A summary of the reviewed surveys.

3 Study of BCML integrations

This section will examine the latest BC and ML-based integrations for IoT solutions that focus on secure data management—reviewing security aspects of the BC consensus and ML types. Afterward, the integrations are compared.

3.1 Review of BCML integrations

Each analysis will give an in-depth look at the convergence of BC and ML for the IoT, as described in Section 2.2. For each integration, the review covers the problem statement for the IoT, an explanation of the solution, a security assessment, an analysis of the experiment, future challenges, and the relevance for the scientific community.

All reviews are summarized in Table 3, a general overview figure of each type is illustrated in Figure 4, and a more extensive overview can be seen in Table 5. Each attack type resistance category is rated based on the ML model effectiveness and the attack resistance in the dataset used, as seen in Table 4.

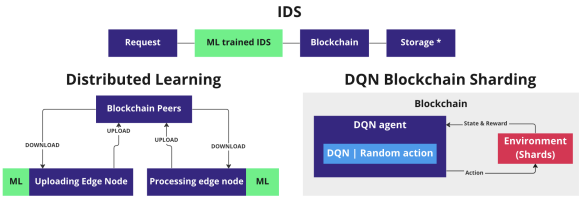

Figure 4: A generalized illustration of the BCML types.

Fortifying against Advanced Persistent Threats [27] Advanced persistent threats (APT), well-organized and strategic cyber adversaries, have become a growing issue for big companies and governments. These cyber adversaries attack by injecting malware into their systems by taking advantage of security vulnerabilities inside edge servers. The malware can stay undetected for a long time; the authors state that there does not exist a low-cost edge-compliant solution that eliminates the threat. In the proposal, Rahman et al. strive to mitigate APTs by detecting and logging the threat in a consortium BC. The authors do this by running a pre-trained ML model inside an edge server using DTL and a BC to offer access control such that APTs can be detected and mitigated on time. The authors train the detection model using two datasets as seen in Table 5. The article outlines the use of certificateless, identity-based encryption to register devices. By creating partial secrets, a central authority can be omitted.

The paper outlines a step-by-step certificateless authentication protocol. This allows small devices to access the network without using a PKI. Another finding is that the authors have compared the DTL performance to other DL algorithms, where the DTL outperforms all different algorithms.

Several factors undermine the trustworthiness and expandability of this report. The report contains many English mistakes; it has a biased figure. Furthermore, the paper does not include security proof, and the authors needed to have the proposed certificateless authorization in the experiment. Also, Maximum Mean Discrepancy is used to measure the difference between the source and target domains. However, this can fail when the kernels used are non-characteristic [28]. Using CA and DTL to record attacks is an approach that can improve security in IoT edge nodes. The work, however, needs a thorough review of the BC consensus mechanisms and the trade-offs of each, and there is much room for improvement in the detail of the work.

pBFT Sharding, DRL and Q-learning [7] The paper notes concerns when applying BC for the IoT due to the massive amount of IoT data transmitted over a network while

ensuring low latency. The proposed DQNSB scheme involves a pBFT consensus algorithm within a sharded BC infrastructure, in which validators are clustered into different shard groups and verify the integrity of blocks through intrashard consensus [7]. The DRL agents detect and change BC consensus parameters in response to dynamic malicious attacks. This contribution takes many elements from Elastico, a sharded variation of the pBFT, and a DRL-based pBFT consensus algorithm [29] [30] [31].

One key novelty of the DQNSB scheme is that it uses a BC that can be trained and adjusted while the system operates. Additionally, by showing theoretical and experimental results, the authors offer valuable insights into the maximum number of malicious nodes the scheme can withstand with detailed comparisons. The results show that the system still has a 70% consensus success probability when 30% malicious nodes are active in the network. Some of the framework's limitations include preliminary attack vulnerability assessment. While the paper mentions that off-chain solutions cannot be used to scale in a trustless environment, alternative solutions could have been mentioned. Moreover, the framework can be vulnerable to zero-day attacks as the network setup is only briefly mentioned. The random selection of validator nodes could result in re-electing previously misbehaving nodes.

Overall, the work provides valuable insights into the maximum number of malicious nodes the BC can withstand. The solution is promising and shows good results compared to previous works. However, it is crucial to keep the limitations in mind: further research on scalability and real-world testing with different attack vectors needs to be done before it can be used widely.

Smart Vehicular Network Cluster Architecture [6] In the paper, Rabienejad et al. mention that the issue with Smart Vehicular Networks (SVNs) is that they are vulnerable to communication network failures, data privacy, and integrity breaches. An attacker can gain unauthorized access to a smart vehicle and gain control over the vehicle from a distance.

The authors use a cluster-based architecture and a private DPoS BC using Deep Neural Networks to address these vulnerabilities. Each vehicle has been assigned a cluster, and every car node retrieves its private key from the central cluster host. This central host, an ML-based IDS, is trained on the IoTID20 dataset to reject incoming requests based on adversarial training. Vehicles are deterred from the network if the cluster host detects anomalies.

The importance of this approach lies in the cluster-based architecture performing computations in the computation node of each cluster, which solves the issue that most IoT edge nodes need more computing power. The DNN accuracy is high: 99.82%. However, while the paper addresses the proposed problems, the research still needs to improve. The paper needs to mention relevant literature, provide an uncomprehensive BC and ML security analysis, and the experiment is limited. Another limitation is the existence of two critical security vulnerabilities in the system. First, private keys are sent over the network. Second, the DNN attack detection produces false positives, which eject truthful participants. The proof of this is simple; The detection is 99.82% accurate, so every good-behaving car labeled as adversarial (a false negative) is banned from the network, and therefore, the size of the network will gradually decrease over time. Last, the author of the paper presents their "upgraded DPoS" that has not undergone rigorous security testing and is, therefore, to be used with caution. While the high accuracy of the model is satisfactory, an exhaustive comparison with other ML models is necessary to confirm the consistency.

Decentralized distributed learning [32] The IoT faces many threats in cyber-physical systems, and in the IoT, high accuracy and low latency are necessary. Rathore et al. propose a secure and decentralized method for distributing ML model updates at edge nodes to reduce bandwidth and latency. Two types of smart contracts, "learning" and "processing", allow for the local models at edge nodes to be uploaded and then processed by other nodes. Data is verified using majority voting by processing nodes, ensuring data integrity during the update process of the model.

The DeepBlockIoTNet architecture has several advantages over the previously proposed DeepChain architecture. Using edge devices to train the model results in higher availability and improved data integrity: there is no single point of failure. Furthermore, the probability of attacks is carefully evaluated through mathematical analysis, which includes the probability of reaching the fault-tolerant point of the consensus. The paper also has some disadvantages. The authors could have provided additional insight into the choice of BC technology and how it could better address the problems listed in the introduction and explain the choice of why the DL operation is not customizable. Furthermore, a majority voting scheme is used in the ML model, which makes the system vulnerable to a ballot-stuffing attack. Also, the system's accuracy is relatively low at 79%.

DeepBlockIoTNet offers an improvement on previous works. It demonstrates value by utilizing edge layers instead of cloud layers to distribute deep learning tasks. Still, this research has many research gaps, such as improving the consensus mechanism and looking at more ways to train different ML models to achieve higher model accuracy.

Improving Intrusion Detection Systems [8] The paper explores the difficulties of preserving security and trust in a multi-cloud setting, specifically examining the potential for BC attacks and the risk of insider threats during data transfers between cloud providers. It also emphasizes the significance of ensuring transparency in data storage methods. The approach is to make a collaborative intrusion detection system (CIDS) using Long Short-Term Memory (LSTM) networks. IDSs are deployed and authenticated on the blockchain network, generating alerts for suspicious activity. A central coordinator unit (CCU) acts as a Security Information and Event Management tool. Using the CIDS, users and cloud providers can transfer data safely. Lastly, an assessment is done compared to other intrusion detection models. This algorithm is trained on historic cyberattacks from the BoT-IoT and the UNSW-NB15 datasets and should help detect and mitigate the threats.

The upsides of the proposed solution are that data centers will become resilient to interference and data poisoning attacks. It is also worth noting that the proposed solution is hybrid. A hybrid integration means cloud providers can integrate the contribution with existing systems.

The paper effectively addresses several issues. However, the proposed solution has potential security problems, and the model's accuracy could be higher. A security concern

Year	Scheme	Description	BC Type	ML Type	Pros (+), Cons (-)	Storage
2022	[27]	APT detection and recording in BC, multisignature-based certificateless approach	PD	DTL	+ Self-learning + Data encryption starts at edge layer - Missing content, chaotic - ML model vulnerabilities	Off-chain, DHT
2020	[7]	A sharded, DRL controlled, and adjustable pBFT; secure against dynamic malicious attacks	PL	DRL	+ Novel Approach + High throughput + Probabilistic attack analysis - Zero-day attack vulnerability	M
2021	[6]	Detection of adversarial vehicles in cluster networks	Hybrid	DL	+ High ML accuracy - Crucial mistakes - Missing parts	On-chain
2019	[32]	Distributed SC-enabled DL and authenticity majority voting within the edge layer	PD	DL	+ ML comparison + Probabilistic attack analysis - DL operation is not changeable - Low ML accuracy	In edge device(s)
2020	[8]	Enhancing (C)IDS using bi-LSTM models to detect and alert anomalies in a BC	PD	Bi-LSTM	+ Comparison with other ML types - ML model shows degrading accuracy - No BC experiment with analysis	Off-chain

Table 3: A summary of the reviewed research papers, M = Missing, PD = permissioned, PL = permissionless.

is the Central Coordinator Unit, a single point of failure: a potential adversary can disrupt the entire network and its audit data. Also, the detection rate in figure five loses accuracy after the 78th epoch. It still needs to be determined why this happens. The paper has some ambiguity; one of the paragraphs is called "privacy preserving SCs", even though SCs are not private by default. Furthermore, the authors have yet to assess the vast amount of data that needs to be processed in the IoT, and it remains a question whether this system is scalable.

The structure ensures a transparent and safer way for cloud-hosted networks to migrate data using an ML model that takes little time to train. However, the work still needs to be improved before the public can use the system due to its limitations.

3.2 Comparison of State-of-the-art Integrations

As seen in Table 3, several approaches with different types of BC and ML have been analyzed. There are several solutions of IDS proposals, where all solutions have advantages and disadvantages [27] [9] [8]. Other proposals have suggested another type of solution: a BC consensus with a direct ML integration within the consensus process [7] [32]. From the analysis, it is clear that some papers include locally-tested experiments where other authors do mathematically-tested attack analyses to test the security of the IoT network.

Security starts at the edge layer. Therefore, it is paramount that the devices that send data will do so securely. The paper reviewed in Section 3.1 clears the path to using Identity Based Encryption to secure the transmission. Other papers use different types of encryption, often using elliptic curve cryptography.

Furthermore, some papers address a hybrid ML training scheme [7] [8], whereas others have a dynamic or static approach. Choosing the initial training dataset is highly important; the APT detection system and the IDS detection system use the BoT-IoT dataset. These datasets provide relevant historical intrusion data. However, the effects and reasons for using the datasets are sometimes not mentioned in the papers.

Authors in different papers have stated that future research can focus on applying ML to other domains using fusion and DTL [32]. In contrast, other authors of papers mention the need for more research to enable attack resistance, throughput, and scalability.

The SVN architecture and the IDS system have a centralized authority, a single point of failure [6] [8]. This centralized node serves as the network's control point, and its compromise can seriously impact the system's security and operation. A lousy actor might target the central node and gain control of the whole network. To solve these challenges, the authors can consider making a decentralized design.

3.3 Proposed Design

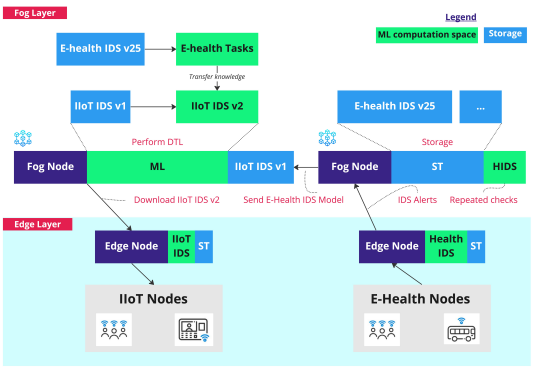

Figure 5: Proposed design of a global ML-based IDS to detect an attack in one sector and transfer knowledge to another sector. ST = storage

Starting with the IoT requirements and looking at the limitations and advantages of BCML solutions, it is possible to propose a design. In Section 2.1, low latency, computation costs, energy efficiency, and secure storage are the main requirements for data management in the IoT. It is evident that IDSs play a crucial role in safeguarding the IoT against malicious attacks [5]. As seen in Section 3.2, multi-domain strategies for training and updating IDS ML models, scalable BCML systems, and a hybrid-trained ML model are of the essence. The design, as seen in Figure 5, is a high-level approach to the integration. Based on previous analysis,

two BC consensus mechanisms and types are the most suitable choices: pBFT and PoS. For private organizations, the DQNSB scheme from Section 3.1 can be implemented once the issues addressed in this paper have been resolved.

To ensure secure and efficient communication, the IoT device and the network must establish trust before any data is transmitted. A lattice-based cryptography algorithm generates the asymmetric keys for each device participating in the network. In the proposed design, the main functions of the Edge Node (EN) are: running an ML model on IoT device requests, reporting attacks to other nodes in the BC, and transmitting data with IoT devices.

A global and transparent IDS training mechanism ensures every EN has access to an ML-based IDS. The EN stores the encrypted data $ENC(d)$ if the IDS does not detect an anomaly. Otherwise, if the IDS has detected an anomaly, the detection result can be either a false positive or a true positive. The EN sends d to a verification party, where d is obfuscated to ensure confidentiality $OBF(d)$. The verification party, an ML model or an oracle, decides on the true nature of the attack. This way, in dynamic attack scenarios, privacy-preserving alerts ensure accurate, accessible, and multi-domain hybrid global models.

Scalability, low latency, and energy efficiency are also of high importance. The amount of nodes is limited in the DQNSB scheme, and it takes time until the block is considered final. To allow for low latency, edge caching ensures incoming data is saved quickly before sending it to the fog. If the EN is busy processing other IDS requests, subsequent requests are batched to be processed by the IDS.

Moreover, the system uses an ML-based SC-audit system to take care of the risks SCs propose in the BC. Multiple eligible nodes vote on an SC, and if a $\%$ of the chosen nodes has assessed the SC, the SC is added to the BC. This uses a reputation-based system: the nodes get discounted points if attacks are discovered in one of those SCs. In case of an active or a passive zero-day attack, a security mechanism that temporarily switches the network off allows IDS models to update. On a global notification through a zero-day attack alert SC, ENs can temporarily halt operations, enabling the edge IDS models to get updated and detect the new attack. In the SC, instructions can be given depending on the type of attack to varying ENs.

All attacks are analyzed in Table 6; for each attack, the figure mentions a proposed prevention or mitigation. In future work, these solutions can be further analyzed and tested. The main point of improvement would be to have proof running the ML model and scaling the network to enable many ENs to participate in the network. This allows the system to skip the step where the fog needs to process the data.

4 Discussion and Future Work

The discussion of this paper presents the results and findings of a study on the security of different types of MLBC solutions for improving the safety of IoT networks. Then, some suggestions for future work in the field of IoT security are made, considering the reviews and the current state-of-the-art solutions.

Discussion

Many papers have room for improvement and miss out on critical aspects that ensure the trustworthiness of papers. From Table 5, it becomes clear not all attacks are analyzed, experiments differ, and many different datasets are used. Two surveyed articles do not address essential attack vectors. Also, GDPR is not discussed, even though it is critical when designing BCML solutions. Lastly, measuring the overall effectiveness of different ML types in real-life environments is complex. It would be beneficial to have a framework to compare the efficacy and security of many ML models in an identical simulated environment.

The proposed BCML integration considers the papers' advantages and limitations and combines them to protect IoT devices against attacks more confidently. It improves on cross-domain ML-model training, and making the system modular while guaranteeing security through the use of the DQNSB scheme with SC auditability. The model still has limitations, including experimental testing and elaboration of the design.

From Section 1, it is apparent that existing IoT networks do not guarantee data security. From [16], achieving security and scalability for IoT data management is complicated by using BC alone. From Section 2.3, it is clear that ML can provide enhanced security with many existing types of IDS systems. BCML integrations for IoT data management struggle to find an optimum between computation power, security, decentralization, and speed, the IoT quadrilemma Figure 3.

Future work

Multiple IDS ML models (NIDS, HIDS, NIPS, HIPS) can be made for different sectors (IIoT, healthcare, smart city, smart home) to enable widespread adoption. These ML models can be lightweight for small ENs or big for more advanced analysis. Also, more research can be conducted to allow for cross-domain fused ML-based IDSs, ensuring a competent model. As seen in Section 3.1, DTL is a fusion strategy allowing for reusing models. Future research can focus on the optimal use of IDSs for different domains.

The next step is to improve scalability when the system is highly secure. Current research is focused on creating a way to enable off-chain transactions, and the study of zero-knowledge rollups is pacing fast. When off-chain transactions become possible, the throughput increases by a significant factor. Another scalability concern and research gap is the processing time of the ML models for IoT data.

Another significant research gap is the verifiable model inference, enabling the safe use of an ML model in BC. For example, zero-knowledge ML inference ensures integrity and tamper-proof ML use. Adopting verifiable ML models heightens the security and scalability of the network. Scalability is improved when ENs are allowed to compute, significantly reducing computation overhead.

Quantum computers can break current cryptographic algorithms, such as elliptic curve cryptography, widely used in BC protocols [33]. With the current rate of development, it is essential to have this in mind when developing new systems for IoT security.

5 Conclusions

The research aims to analyze and compare the latest research on securing the IoT with BC and ML and provide a proposal for a secure BCML integration.

Several state-of-the-art research works have been considered in this review. Different types of BC and ML integrations

have been compared with each other. Then, the proposed design implements the DQNSB scheme to train a decentralized global model that distributes computing power with a focus on speed and, most importantly, security. Some limitations of this work include the thorough security and performance analysis of the proposed design.

The zero-knowledge rollups and quantum-proof encryption for improved scalability and security are still in development. Then lastly, the future challenges include multi-domain ML, focusing on scalability, verifying ML model outputs, and securing against quantum attacks.

Centralized IoT solutions will face significant challenges in dynamically changing environments, and there are often security concerns from centralized systems. Fully public decentralized solutions still face extreme data breaches, mainly from newly created software. In this paper, it has been shown that an integration of machine learning and blockchain can enhance IoT security. If the scalability problems are solved, this integration can be accessible to any individual or organization.

6 Responsible Research

The most crucial aspect of research is that the paper assesses all ethical concerns and risks for all technologies, and the work is reproducible. This does not only mean guaranteeing the use of technologies that will benefit affected people in a good way, but it also means the work is valuable for future researchers in the field.

Integrity The writing has included the works of different authors, and reviewed papers have been published in journals of good research quality: ACM and IEEE. They each have been assessed on their relevance and integrity. The design, conduct, reporting of results, and assessment of the paper must adhere sufficiently to the Netherlands code of conduct and the T.U. Delft Strategic framework [34]. From those ethical concerns, looking at the environment is vital. Moreover, the system has to be effective; a system that could be more effective at mitigating attacks will raise issues when the plans are implemented.

Moreover, a hard requirement from the General Data Protection Regulation (GDPR) is that all data needs to be stored within Europe [35]. Hosting data in the E.U. using a public B.C. is practically impossible because data is distributed over many nodes. Recent studies done by the European Union show that private and permissioned B.C.s partially comply, but many uncertainties remain [35].

Reproducibility This assessment is done by thoroughly understanding all frameworks used, evaluating the report's weaknesses, and conducting a security analysis for each proposal. Using this transparent framework and commenting on other works' transparency ensures the work is honest and responsible.

The work consists of a detailed methodology section and includes how the figures and tables are made. This ensures reliable communication with researchers in the field, allowing others to assess and reuse the methods.

References

[1] Statista, "Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030," 2022. [Online]. Available: https://www-statista-com.tudelft.idm.oclc.org/statistics/1183457/iot-connected-devices-worldwide/ (Accessed 2022-11-20).

[2] M. S. Ali, M. Vecchio, M. R. Pincheira Caro, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. Pp, pp. 1–1, 11 2018.

[3] G. Kambourakis, C. Kolias, and A. Stavrou, "The mirai botnet and the iot zombie armies," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, 2017, pp. 267–272.

[4] C. Page, "Amazon's ring quietly fixed security flaw that put users' camera recordings at risk of exposure," Aug 2022. [Online]. Available: https://techcrunch.com/2022/08/18/amazon-ring-security-risk/ (Accessed 2022-12-20).

[5] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in iot using machine learning and blockchain: Threats and countermeasures," vol. 53, no. 6, dec 2020.

[6] E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, R. Parizi, and G. Srivastava, "Secure ai and blockchain-enabled framework in smart vehicular networks," 12 2021, pp. 1–6.

[7] J. Yun, Y. Goh, and J.-M. Chung, "Dqn-based optimization framework for secure sharded blockchain systems," *IEEE Internet of Things Journal*, vol. Pp, pp. 1–1, 07 2020.

[8] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2021.

[9] K. Wang, J. Dong, Y. Wang, and H. Yin, "Securing data with blockchain and ai," *IEEE Access*, vol. 7, pp. 77 981–77 989, 2019.

[10] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[11] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, "Deep reinforcement learning for blockchain in industrial iot: A survey," *Computer Networks*, vol. 191, p. 108004, 2021.

[12] O. Fadi, Z. Karim, E. G. Abdellatif, and B. Mohammed, "A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments," *IEEE Access*, vol. 10, pp. 93 168–93 186, 2022.

[13] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[14] J. Santos, T. Wauters, B. Volckaert, and F. De Turck, "Towards low-latency service delivery in a continuum

of virtual resources: State-of-the-art and research directions," *IEEE Communications Surveys Tutorials*, vol. 23, no. 4, pp. 2557–2589, 2021.

[15] K. Salah and M. Khan, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, 11 2017.

[16] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100067, 2022.

[17] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[18] J. J. Zhang, K. Liu, F. Khalid, M. A. Hanif, S. Rehman, T. Theocharides, A. Artussi, M. Shafique, and S. Garg, "Invited: Building robust machine learning systems: Current progress, research challenges, and opportunities," in *2019 56th ACM/IEEE Design Automation Conference (DAC)*, 2019, pp. 1–4.

[19] I. Ilahi, M. Usama, J. Qadir, M. U. Janjua, A. Al-Fuqaha, D. T. Hoang, and D. Niyato, "Challenges and countermeasures for adversarial attacks on deep reinforcement learning," *IEEE Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 90–109, 2022.

[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," May 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[21] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[22] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, "Towards a green blockchain: A review of consensus mechanisms and their energy consumption," in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2021, pp. 503–511.

[23] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3559–3570, 2019.

[24] S. Richards, "Sidechains." [Online]. Available: https://ethereum.org/en/developers/docs/scaling/sidechains (Accessed 2023-01-07).

[25] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 93 039–93 054, 2022.

[26] D. Trautwein, A. Raman, G. Tyson, I. Castro, W. Scott, M. Schubotz, B. Gipp, and Y. Psaras, "Design and evaluation of ipfs: A storage layer for the decentralized web," in *Proceedings of the ACM SIGCOMM 2022 Conference*, ser. Sigcomm '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 739–752.

[27] Z. Rahman, X. Yi, and I. Khalil, "Blockchain based ai-enabled industry 4.0 cps protection against advanced persistent threat," *IEEE Internet of Things Journal*, pp. 1–1, 01 2022.

[28] W. Zhang, X. Zhang, L. Lan, and Z. Luo, "Maximum mean and covariance discrepancy for unsupervised domain adaptation," *Neural Processing Letters*, vol. 51, 02 2020.

[29] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 17–30.

[30] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, ser. OSDI '99. USA: USENIX Association, 1999, p. 173–186.

[31] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3559–3570, 2019.

[32] S. Rathore and J. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. Pp, pp. 1–1, 11 2020.

[33] A. Mashatan and D. Heintzman, "The complex path to quantum resistance," *Commun. ACM*, vol. 64, no. 9, p. 46–53, aug 2021.

[34] A. Hol, "De nederlandse gedragscode wetenschappelijke integriteit 2018," *Justitiële verkenningen*, vol. 45.

[35] M. Finck, "Blockchain and the general data protection regulation," jul 2019. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS%5FSTU(2019)634445%5FEN.pdf

[36] J. M. Peterson, J. L. Leevy, and T. M. Khoshgoftaar, "A review and analysis of the bot-iot dataset," in *2021 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 2021, pp. 20–27.

[37] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.

[38] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "Ton_iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165 130–165 150, 2020.

[39] A. Sarwar, S. Hasan, W. U. Khan, S. Ahmed, and S. N. K. Marwat, "Design of an advance intrusion detection system for iot networks," in *2022 2nd International Conference on Artificial Intelligence (ICAI)*, 2022, pp. 46–51.

A Supporting figures

Name	Dataset use for attack prevention	Contents of dataset
BOT-IOT [36]	IoT botnet traffic	DDoS, DoS, OS and Service Scan, Keylogging and Data exfiltration attacks
UNSW-NB15 [37]	Contemporary network traffic attacks	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms
TON-IoT [38]	(I)IoT sensor, operating systems, and network traffic attacks	DoS, DDoS, ransomware, IoT gateways, and computer systems across the IoT/IIoT network
IoTID20 [39]	IoT intrusion	DoS, Mirai, MiTM, Scan attacks

Table 4: Different datasets for attack detection used in surveyed papers to analyze attack vectors.

Scheme		Rahman et al. [27]	Yun et al. [7]	Rabienejad et al. [6]	Rathore et al. [32]	Alkadi et al. [8]
Security	**Confidentiality**	◑	●	○	◕	○
	Integrity	◑	◕	○	◕	○
	Availability	●	●	◕	◕	○
BC features	**Consensus mechanism**	E	pBFT	Upgraded-DPoS	PoW	PoW
	Node scalability	◔	◑, E	◕, E	●	◔, E
	Decentralized	○	●	◕	○	E
ML Model	**Cross-domain**	◑	○	○	○	○
	Activation function	ReLU	M	ReLU	Nonlinear, M	ReLU
	Dynamically shared ML model(s)	◑	○	◑	●	●
	Type of ML	Static	Hybrid	Static	Dynamic	Hybrid
Experiment	**BC consensus, type**	HLF, pBFT	M	Upgraded DPoS	Ethereum, PoW	Ethereum, PoW
	Amount of nodes	2 - 500	200	16 - 128	E	E
	Block Size (KB)	M	0.2	1000	E	E
	Latency (s)	5 - 60	< 96, E	M	57	E
	TPS	1325 - 64	$6 * 10^5$	66 - 47	◔, E	E
	Energy Efficiency	M	M	◑, M	◔	E
	No. Epochs run	200	10000	100	N.A.	200
	ML Accuracy (%)	0.87	E	0.9982	79	95–99
	Train/Test dataset	BoT-IoT, TON_IoT	N.A.	IoTID20	MS COCO	BoT-IoT, UNSW-NB15
Attacks Resistance	**Majority Attack (%)**	33	> 25, M	51	51	E
	Quantum Attack	M	M	○	◔	○
	(D)DoS Attack	●	●, E	●	◕, E	◕
	Injection Attack	◔	M	○	◕	◔
	Routing Attack	○	M	○	◕	◔
	MiTM Attack	◑	M	◕	◕, E	◑
	Malware Attack	◔	M	○	◕	○
	Extraction Attack	◑	M	○	◕	◔
	Software Attack	◔	M	○	◑	◔

Table 5: Assessment of security, BC, ML, the experiment in the paper, and the attack resistance. M = **Missing**, not included. E = Depends on another input, requires **Extra** research.

Category	Attack Name	Potential attack vectors	Solution against attack	Extra resistance against attack	Future solution
Adversarial Training	Adversarial Training	ML	ML careful training		
Cryptography	Quantum	IoT, BC	By design		Quantum resistant cryptography
DoS	Jamming Attack	IoT, BC	HIDS		
DoS	Exhaustion Attack	IoT, BC	NIDS	HIDS	
DoS	DDos	IoT, BC	NIDS		
DoS	Sponge attack	ML	NIDS		
Extraction	Private Key Compromise	IoT	ID-based encryption		
Extraction	Storage Data Extraction	IoT	HIDS		
Extraction	Model Stealing	ML	ML careful training		zk-ML proof
Extraction	Training data extraction	ML	ML careful training		
Initialization	0 Day	IoT, BC, ML	NIDS	ML careful training	Security Mechanism Oracle
Injection	Exploit	IoT, BC	HIDS	SC audit	
Injection	Injection	IoT	SC audit		
Injection	Malware attack	IoT	HIDS	SC audit	
Injection	Adversarial Pertubation	ML	NIDS	ML perturbation resistance	
Injection	Smart Contract attack	BC	SC audit		
Malware	Malicious Model	ML	ML audit	ML careful training	
MiTM	Spoofing, Node Replication	IoT, BC	HIDS	By design	
MiTM	Insider attack	IoT	By design		
MiTM	Eavesdropping	IoT	NIDS	By design	
Network	Collusion	IoT, BC, ML	By design		
Network	Sybil attack	IoT, BC	By design		
Network	Hole (worm/black/gray)	IoT	By design		
Network	51% attack	BC	By design		
Physical	Node Tampering	IoT	HIDS		

Table 6: Assessment of the proposed design with the initial attack vectors.