





Article

Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities

Burhan Ul Islam Khan ^{1,*}, Khang Wen Goh ², Abdul Raouf Khan ^{3,*}, Megat F. Zuhairi ^{4,*}
and Mesith Chaimanee ⁵

¹ Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia

² Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Malaysia; khangwen.goh@newinti.edu.my

³ Department of Computer Sciences, King Faisal University, Al-Ahsa 31982, Saudi Arabia

⁴ Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur 50250, Malaysia

⁵ Faculty of Engineering and Technology, Shinawatra University, Pathum Thani 12160, Thailand

* Correspondence: burhankhan@um.edu.my (B.U.I.K.); raoufkhank@kfu.edu.sa (A.R.K.); megatfarez@unikl.edu.my (M.F.Z.)

Abstract: Blockchain is recognized for its robust security features, and its integration with Internet of Things (IoT) systems presents scalability and operational challenges. Deploying Artificial Intelligence (AI) within blockchain environments raises concerns about balancing rigorous security requirements with computational efficiency. The prime motivation resides in integrating AI with blockchain to strengthen IoT security and withstand multiple variants of lethal threats. With the increasing number of IoT devices, there has also been a spontaneous increase in security vulnerabilities. While conventional security methods are inadequate for the diversification of IoT devices, adopting AI can assist in identifying and mitigating such threats in real time, whereas integrating AI with blockchain can offer more intelligent decentralized security measures. The paper contributes to a three-layered architecture encompassing the device/sensory, edge, and cloud layers. This structure supports a novel method for assessing legitimacy scores and serves as an initial security measure. The proposed scheme also enhances the architecture by introducing an Ethereum-based data repositioning framework as a potential trapdoor function, ensuring maximal secrecy. To complement this, a simplified consensus module generates a conclusive evidence matrix, bolstering accountability. The model also incorporates an innovative AI-based security optimization utilizing an unconventional neural network model that operates faster and is enhanced with metaheuristic algorithms. Comparative benchmarks demonstrate that our approach results in a 48.5% improvement in threat detection accuracy and a 23.5% reduction in processing time relative to existing systems, marking significant advancements in IoT security for smart cities.

Keywords: IoT security; data confidentiality; smart cities; neural network optimization; Ethereum blockchain; artificial intelligence (AI); cybersecurity



Citation: Khan, B.U.I.; Goh, K.W.; Khan, A.R.; Zuhairi, M.F.; Chaimanee, M. Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities. *Processes* **2024**, *12*, 1825. <https://doi.org/10.3390/pr12091825>

Academic Editor: Chunhui Zhao

Received: 25 July 2024

Revised: 19 August 2024

Accepted: 23 August 2024

Published: 27 August 2024



Copyright: © 2024 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

Blockchain plays an integral role in securing data within the Internet of Things (IoT) ecosystem owing to its unique characteristics, such as immutability, decentralization, and cryptographic security mechanisms [1]. With massively generated data in IoT, blockchain can maintain the ledger for data exchanges or transactions in an immutable form [2]. This means that, with a higher consensus among users, it is possible to amend the structure of the data recorded within the blockchain; thus, a higher degree of data integrity is facilitated [3]. Blockchain offers a decentralized network system with multiple nodes, where data are managed in a distributed manner [4]. Such a decentralized blockchain offers a potential impediment to attackers by closing all single control points to carry out intrusion. Currently,

several approaches are aimed at enhancing the security performance of blockchains [5–10]; however, to date, an entirely foolproof and robust model capable of effectively resisting cyber-attacks in the context of IoT has not been observed.

It has been noted that Artificial Intelligence (AI) can significantly enhance the performance of blockchain in IoT by providing advanced analytics, optimization, and automation capabilities [11]. AI algorithms can analyze large volumes of IoT data collected from sensors and devices in real time. By extracting valuable insights and patterns from these data, AI can optimize blockchain operations, such as transaction validation and consensus mechanisms, while helping to identify anomalies in the blockchain network and enhancing security and integrity [12]. By analyzing the historical performance data stored in the blockchain, AI models can predict when devices will likely require maintenance or replacement, enabling proactive interventions to prevent costly downtime and disruptions [13]. AI algorithms can optimize resource utilization in blockchain networks by dynamically adjusting parameters such as block size, transaction fees, and network bandwidth based on real-time demand and network conditions. This optimization ensures efficient use of computing resources and enhances the scalability and performance of blockchains in IoT environments [14]. AI-powered smart contract platforms can automate complex business logic and decision-making processes within the IoT ecosystems. IoT devices can autonomously execute transactions, negotiate terms, and enforce agreements using real-time data and contextual information by integrating AI algorithms into smart contracts. This automation streamlines processes, reduces latency, and improves efficiency [15].

However, there are also challenges in applying AI-based approaches to address security concerns in IoT using blockchains. (i) Both AI and blockchain require significant computational resources, which can be challenging to scale to the maximum elements of smart cities (e.g., the infrastructure of Information and Communication Technology (ICT), smart mobility, smart governance, healthcare, etc.) in large-scale IoT deployments that demand the processing power needed for AI algorithms and blockchain transactions may strain existing infrastructure and lead to performance bottlenecks. (ii) Achieving interoperability between AI algorithms and blockchain platforms can be complex, particularly when multiple heterogeneous IoT devices and systems are integrated. Ensuring seamless communication and data exchange between AI-enabled devices and blockchain networks requires standardized protocols and interfaces that are still evolving in the IoT ecosystem. (iii) AI algorithms often require access to large datasets for training and inference, raising concerns regarding data privacy and confidentiality, particularly in sensitive IoT applications. Integrating AI with blockchain introduces additional challenges in managing data privacy because blockchain's transparent and immutable nature may expose sensitive information to unauthorized parties if not properly encrypted or anonymized. (iv) While AI and blockchain technologies offer enhanced security features individually, their integration introduces new security risks and attack vectors in IoT deployment. Adversaries may exploit vulnerabilities in AI models or blockchain protocols to manipulate data linked to elements of smart cities in IoT, compromise device integrity, or launch sophisticated attacks such as adversarial examples or blockchain-based attacks.

The primary contributions of the proposed study model are as follows:

- Development of a three-layer operational framework within the IoT comprising sensor, edge, and cloud layers. This structure facilitates precise cyber-threat detection by identifying the transaction abnormalities. The intention is to provide a more accountable and interconnected model of each involved actor during their respective interaction, which needs to be added to the existing modeling approaches;
- Introducing a simplified yet highly robust mechanism for computing the legitimacy score enhances accountability among nodes participating in blockchain transactions. This step addresses issues of a higher degree of complexity involved in trust computation in blockchain operation, yet it cannot offer optimal data privacy;
- Innovation in decentralized Ethereum blockchain operations, integrating AI to optimize data confidentiality, is particularly tailored for smart city applications in the

IoT. This approach is intended to mitigate issues about off-chain data storage with increased operational costs;

- Introduction of a simplified consensus-based method and an analytical approach utilizing a decentralized evidence matrix to ensure maximum data integrity, non-repudiation, and confidentiality in large-scale IoT environments. This contributory step is meant to mitigate the possibility of introducing any new attack vector where an attacker can create a fork from a previous block to lower the strength of network security;
- Implementation of a novel metaheuristic optimization-based neural network predictive operation to dynamically identify and classify cyber threats, thereby enhancing system resilience and security. This step addresses the association of the computational burden with most AI-based methods in network security.

2. Related Work

This section discusses the evolution of distinct blockchain-based studies in existing systems.

It was noted that using pseudonyms can facilitate a better degree of anonymity in the blockchain, provided that robust unlinkability is maintained. This characteristic offers the first layer of defense by preventing the intruder from accessing sensitive information associated with the pseudonym user. This challenge was addressed in the work of Gutierrez-Aguero et al. [16], where a blockchain model was designed to offer unlinked interactions between the model and the user concerning their identity. This is accomplished by assigning a dynamic pseudo-identity to the user without any link to its original identity. However, this study introduces this model using a sophisticated key derivation framework, eventually introducing a significant degradation in transaction throughput for large networks. Javed et al. [17] carried out a similar modeling pattern to mitigate the issues of conventional anonymization approaches, leading to data quality degradation. The authors used smart contracts and blockchains, in which distributed user data can be used by service providers with a higher degree of privacy preservation. A smart contract is deployed by a user endowed with the privilege to custom configure it. However, this study is expected to offer higher propagational delay and dependency on authorized nodes for validating transactions.

Not all blockchain-based studies were meant to emphasize privacy; one example is the healthcare sector's exchange of information. This challenge was mitigated by the unique blockchain model presented by Lee and Song [18] by adopting ring signatures. The model can identify sensitive information, followed by obscuring it, whereas a smart contract is designed using a ring signature. The primary limitation of this study is that it is specific to the use-case, and the same model cannot be applied to different domain use cases. Furthermore, the model includes excessive variables while developing smart contract management, which can eventually pile up the heap of saturated memory over time. A similar study on adopting healthcare-based use cases was also presented by Omar et al. [19], who stated that healthcare-based information must be accessed by a health insurance company, which raises further data privacy concerns. An interoperable service for accessibility to policy information and concurrent storage of healthcare data is permitted in this blockchain design. However, the blockchain structure is retained externally to the system, which induces time for fetching and yielding the outcome.

Existing studies on data confidentiality are witnessing challenges in securing location-dependent services that are often associated with poor service quality. This problem was addressed by Qiu et al. [20], who designed a unique model that does not require any form of anonymizing server to perform validation. The model adopts the k-anonymity method to secure the user's location information, and incentives are introduced to promote user participation. The model requires substantial benchmarking of its outcome, and its applicability needs to be improved for continuous query systems in a blockchain.

The vulnerability associated with the conventional design of smart contracts in blockchain was addressed in the work of Albyaflah et al. [21], where data confidentiality was enhanced by developing a unique access control system based on user roles. The

system also developed a secure data store system represented in a smart contract capable of controlling gas consumption. However, the performance of the calling mechanism for a smart contract depends on the indexed array followed by updating processing, where there is a higher possibility of redundant information. Hence, the model can introduce latency while processing concurrent users requesting the same data or services.

Elisa et al. [22] introduced a different method of blockchain security in which the complexity associated with securing vastly interconnected services is addressed. The study model introduced an anomaly detection system for large-scale sophisticated applications, incorporating an artificial immune system and blockchain operation. Although the model facilitates highly decentralized operation, using the Merkle tree significantly reduces the storage overhead.

In addition to the above-mentioned research problems, the existing literature has also addressed scalability issues in blockchain implementation for large-scale applications. This issue was addressed by Khor et al. [23], who used bitwise logical operators to develop a scalable blockchain for securing batch ownership during data transmission. The study also uses the InterPlanetary File System, which permits the full-fledged accessibility of transactions to legitimate owners. In contrast, only the public can view transaction records to offer interoperability. Although the model is claimed to resist multiple attacks on the supply chain network, it has an extensive key management approach that introduces a computational burden for heavy traffic conditions. The adoption of the InterPlanetary File System was also witnessed in the work of Ugochukwu et al. [24] to securely store logistic information in a decentralized manner, followed by using a secure hash algorithm to protect data anonymity. This study model also resisted multiple lethal threats with satisfactory throughput. However, the model demands the generation of operational certificates for every legitimate access, progressively increasing the oversaturation of the resources of other nodes.

A security model was presented by Ullah et al. [25], in which a secure performance trade-off between regulatory and deregulated electricity markets was addressed. The authors used decentralized Ethereum, specifically for a regulated market in which data security is enhanced. However, more evidence is needed to prove the resistance of this model to extensive threat exposure. Viswanadham and Jayavel [26] used a nature-inspired algorithm to generate optimal security keys to secure and store data. However, the model is quite iterative in its operation upon exposure to various research environments in IoT. The blockchain model presented by Yousra et al. [27] addressed the challenges associated with security loopholes using conventional authentication protocols, where third parties use and access varied sensitive information. The essential parameters were identified using NFT, whereas the traditional authentication protocol was amended for more efficient monitoring of activities, and the study outcome was found to be cost-effective. However, the main pitfall of this model is its a priori attack definition, without which threats are difficult to identify and mitigate.

Recently, it was also noted that various AI-based security modeling had evolved in IoT: Decision Tree (Stefanescu et al. [28], Fu et al. [29]), Support Vector Machine (Salb et al. [30], Monteiro et al. [31]), Random Forest (Inder and Sharma [32]), Logistic Regression (Ivaninskiy and Ivashkovskaya [33]), conventional deep learning approaches (Lawrence and Zhang [34], Uppala et al. [35]), Artificial Neural Network (Kim et al. [36]), Recurrent Neural Network (HaddadPajourh et al. [37]), Long Short-Term Memory (Alamro et al. [38]), Auto Encoder (Arifeen et al. [39], Alaghbari et al. [40]), and nature-inspired algorithm (Taher et al. [41], Singh and Ujjwal [42]).

Adopting AI models in security IoT often requires extensive data for training and other associated operations. As these data contain highly sensitive information, offering optimal data confidentiality is challenging. It was also noted that AI-based security approaches are more complex than the reviewed blockchain-based solutions [16–27]. Such forms of complexity lead to unintended consequences that are computationally challenging to

correctly identify and stop. Existing AI models in blockchain approaches address resource constraints, scalability, and complexity issues.

A closer look at the above-mentioned security approaches shows that there are claimed benefits associated with all approaches. It is believed that the integrity of AI-specific models can be verified by blockchain. However, it is yet to be seen that if the blockchain's records are tampered with or compromised, they could eventually lead to outliers by AI models. Moreover, existing Ethereum blockchain-related approaches are case-specific, whereas existing AI-based solutions have complexity issues. The problems identified are discussed next.

3. Problem Description

In reviewing related work on the Ethereum blockchain, it is evident that prevailing methodologies primarily focus on introducing unlinkability between data and potential attackers [16,17,20]. Such approaches typically rely on cryptographic addresses to identify users and minimize the utilization of personal information. However, although these schemes provide pseudonymity, they fail to ensure comprehensive data confidentiality. Notably, existing implementations often employ techniques, such as ring signatures [18] and artificial immune systems [22], to bolster encryption methods to safeguard data stored within the blockchain. Despite claims of secure management of encryption keys [19], these schemes face challenges in maintaining data privacy under dynamic cyber threats. Additionally, some studies have explored off-chain storage solutions, such as centralized databases or the InterPlanetary File System, to preserve blockchain data [23,24]. However, these approaches compromise the optimal decentralization for improved data confidentiality, resulting in elevated operational and maintenance costs in large-scale IoT scenarios.

Conversely, specific investigations assert superior decentralization and enhanced data security in diverse test cases [25–27]. However, a notable drawback lies in potentially revealing sensitive information through linked metadata, including transaction addresses, timestamps, and amounts [25–27]. Protecting the confidentiality and anonymity of such metadata requires strategic planning to mitigate the risk of leakage.

Furthermore, although AI models have exhibited progress in augmenting the security performance of the Ethereum blockchain, there remains a need to integrate robust yet lightweight encryption approaches into Ethereum smart contracts and IoT devices [28–42]. Additionally, efforts to minimize data stored in the blockchain and strengthen communication security between IoT devices, AI models, and the Ethereum blockchain are warranted. It should be noted that an AI model has a higher degree of vulnerability toward adversarial attacks, where the model can be corrupted by malicious input itself. In reality, a valid and benchmarked blockchain model for verifying the integrity of the AI model remains to be reported in the literature. Addressing the computational complexities associated with AI model variants is imperative to optimize the performance while mitigating the inherent weaknesses in conventional schemes.

To address these challenges, our research endeavors to pioneer a novel computational framework that harmonizes AI and blockchain technologies. Our objectives are to mitigate the scalability challenges inherent in blockchain-based security frameworks, augment real-time threat detection through advanced AI algorithms, and fortify data confidentiality via encryption techniques and privacy-enhancing protocols. Additionally, we aim to address the specific security needs of smart cities by emphasizing seamless communication and instantaneous responsiveness within IoT ecosystems. The following section discusses the solutions to address these research problems.

4. Methodology

The primary purpose of the proposed study is to develop a novel and unique form of an intelligent computational framework for optimizing the data confidentiality associated with smart cities in the IoT. A smart city comprises various elements, such as ICT, IoT sensors, data analytics, smart mobility, energy management, sustainable infrastructure,

healthcare, and transportation. Unlike the approaches in the previous section, the proposed system develops a generalized framework that emphasizes the data and mechanisms for secure services using a blockchain-based IoT cloud. This will assist in offering maximum applicability to various smart city elements through cost-effective solutions. Hence, the proposed study does not emphasize any particular element of smart cities in IoT; instead, it builds an innovative framework that maximizes the supportability of most smart city applications' aspects. The proposed study model uses the Ethereum blockchain integrated with AI in a unique order to accomplish this study objective for large-scale IoT applications deployed over a cloud ecosystem. The architecture of the proposed framework is as follows.

The architecture in Figure 1 shows that various sensors deployed in discrete regions of smart cities perform sensing, and this sensed information is subjected to security assessment in dual stages. In the first stage of security assessment, the extracted sensory information is forwarded to the edge nodes. In contrast, the second stage facilitates analyzing and storing information acquired from the edge nodes.

- *Edge Layer Operation:* This is the first stage of operation in which raw sensory information from smart cities is extracted via multiple gateways and subjected to data confidentiality analysis. The stream of raw sensory information is analyzed to identify the usual traffic patterns with the possibility of a cyber breach. In addition, this monitoring of sensory data also assists in analyzing traffic data to evaluate the management of smart traffic and its responsiveness to malicious activities. This raw sensory data extraction process is carried out within the edge layer to acquire the legitimacy score, where the Ethereum blockchain further initiates validation. The term *legitimacy score* can be defined as a qualitative measure representing an IoT device's credibility, integrity, and reliability within a network. It should be noted that this operation stage also involves verifying the legitimacy of all sensing devices. The proposed scheme uses a unique consensus method for preserving privacy by confirming the regular or malicious state of data obtained from various sensors. The edge layer also authenticates the blockchain to safeguard data from multiple cyber threats. The novelty of the proposed architecture lies in its two levels of security approaches associated with data privacy. In the first layer, a newly constructed consensus is used to safeguard the data, whereas the transformation operation is carried out to obtain encoded data from the extracted features. This operation is intended to resist any form of illegal extraction of inference toward attack detection by any malicious adversary. In contrast to conventional blockchain models discussed in the literature, the outcome of blockchain validation is further subjected to transformation using AI, which results in the detection of abnormalities. The analyzed security information is stored in blockchain storage units and forwarded to the next cloud layer via multiple gateway nodes;
- *Cloud Layer Operation:* Upon arriving at cloud layers via gateway nodes, the data associated with the analyzed security information from the previous layer are initially stored in interconnected and decentralized cluster units of the cloud, where they are further cross-checked for their match with the predefined historical transactional data. This results in malicious/normal activity. It should be noted that two storage mechanisms are involved in the proposed scheme. The first form of storage mechanism is in the edge layer operation, which stores all monitored traffic information and legitimacy scores evaluated on the monitored traffic. The second form of storage mechanism occurs when the outcome of the edge layer detects abnormalities, and this information is stored in various connected storage units involved in the cloud layer operation. The result of this operation is the detection of suspicious activities;
- *AI Model:* The proposed schemes amend the conventional design of neural networks to address the issues about computational burden reported in the identified research problems in Section 3. The revised version of this neural network model in the proposed AI solution aims to achieve optimized performance in a dynamic environment with faster responsiveness while classifying regular and malicious nodes and traffic. The implemented AI model performs its classification task using the extracted features

within the edge layer operation. Finally, the information on analytical operations related to suspicious activity in both the edge and cloud layers is harnessed to confirm the presence of malicious activities. Finally, the operation results in identifying intruders and all patterns of intrusive activities linked to compromising the legitimacy score in the system. The framework offers data confidentiality and results in a highly intellectual system capable of determining any abnormalities within the transactional operation carried out by the blockchain network and cloud environment. Therefore, a two-way security assessment framework was used to validate IoT transactions.

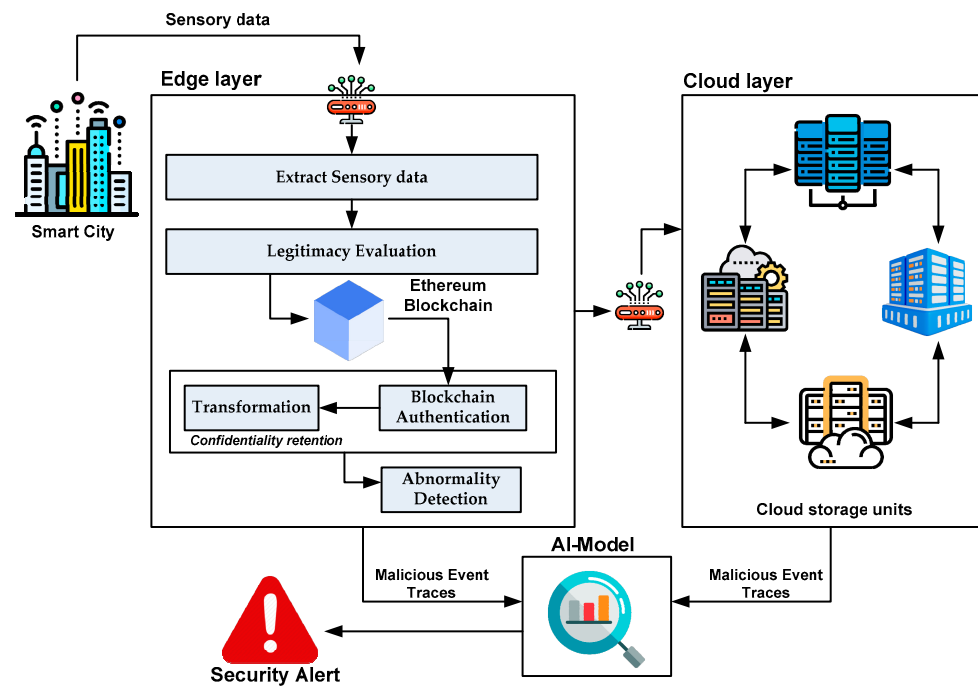


Figure 1. Architecture of proposed framework.

The complete operation of the proposed framework is classified into various essential tasks related to evaluating and managing the legitimacy score, offering data confidentiality using the Ethereum blockchain, and optimizing the security features using the AI model. The primary mechanism for assessing the legitimacy score is to authenticate the reliability of the IoT devices. The secondary mechanism for validating the sensory data and resisting cyber threats uses the simplified Ethereum blockchain technique. In contrast, AI modeling has been used to classify cyber threats. The proposed framework utilizes a consensus-based approach to determine the degree of tampering performed on the IoT devices. This technique also ensures a higher degree of data confidentiality in the IoT. The framework also presents an analytical method for minimizing the influence of cyber threats by obtaining an encoded object from extracted features. Further elaboration of the essential operations is as follows.

4.1. Evaluation of Legitimacy Score

This algorithm is responsible for computing the outcome of the legitimacy score, where the term *legitimacy score* can be defined as a probability value assigned by the parent IoT device (transmitting) to the selected IoT device to assist in forwarding data to the destination node. For every successful transaction, the parent IoT device assigns the highest probability value of one; otherwise, zero is assigned to the selected IoT node. However, this policy of assigning legitimacy scores must be flexible with dynamic IoT traffic to form a foundation for secure communication and collaboration in a networked environment. The operational steps of Algorithm 1 are as follows.

Algorithm 1. For Evaluating Legitimacy Score.

Input: α_s, d, η_{tr}
Output: l_o
Start
1. **init** α_s
2. $\theta = f_1(d_i)$
3. $r_1 \rightarrow read(\alpha_s)$
4. $r_2 \rightarrow (l_s, \theta)$
5. **If** $\alpha_s = \theta$
6. $\alpha_s = \alpha_s + 1$
7. **Else**
8. $\alpha_s = 0$
9. **End**
10. $l_s = f_2(l_s, \eta_{tr})$
11. **arrange** $(l_s)^\gamma$
12. **If** $l_s > A_1 \&\& l_s < A_2$
13. $l_o = flag(valid)$
14. **Else**
15. $l_o = flag(malicious)$
16. **End**
End

The algorithm mentioned above contributes to safeguarding IoT networks from cyber threats that could either be an adaptive form of threat or induce potential physical damage to IoT devices. Such an adversary usually introduces itself into a secure network system via IoT devices with a weaker authentication framework. The proposed algorithm is intended for active and resisting passive attacks, where the adversary captures confidential information via various malicious activities. Irrespective of the varied strategies adopted by the adversary, the expected consequences of all these attack strategies lead to the compromisation of the actual data structure. Hence, the proposed algorithm aims to strengthen data confidentiality and integrity. The operational steps of the proposed algorithm are as follows: The algorithm takes the input of α_s (transaction score), d (data), and η_{tr} (cardinality of the transaction), which, after processing, yields an outcome of l_o (legitimacy outcome). The algorithm initializes the α_s (transaction score) preliminarily (Line 1), followed by evaluating the threshold value of θ where an explicit function $f_1(x)$ considers an input argument of data d_i (Line 2). Function $f_1(x)$ extracts the range of the minimum and maximum values of data d_i such that $d_i \in D$, where D represents the overall dataset. The following line of operation is associated with applying a $read()$ method that reads all the α_s (transaction scores) within the raw sensory data from IoT devices that are extracted from the D dataset and stored in the r_1 matrix (Line 3). The framework further estimates l_s (legitimacy score) and θ threshold values based on α_s (transaction score) (Line 4).

Conditional logic is framed, where the equivalency of α_s (transaction score) and θ threshold value is assessed (Line 5). Under favorable conditions, the value of α_s (transaction score) is incremented (Line 6); otherwise, the value of α_s (transaction score) is assigned to 0 (Line 8). After assessing the conditional logic associated with the transactional score, the system further estimated the global legitimacy score. This is accomplished by constructing another function, $f_2(x)$, considering the input argument of l_s (legitimacy score) and η_{tr} (cardinality of the transaction) (Line 10). The legitimacy score is computed by deploying function $f_2(x)$ to perform the following computations:

$$f_2(x) = \frac{\Delta l_s}{\eta_{tr}} \quad (1)$$

In Equation (1), the computation of function $f_2(x)$ is performed by considering Δl_s representing the l_s/c and η_{tr} (cardinality of the transaction), where variable c represents the network coefficient. It should be noted that the difference between variables l_s and

Δl_s is that the former is used for initialization based on probability assigned values in transaction scores, while the latter is used by considering the former along with including the network coefficient to make it practically applicable for blockchain networks. The study then organizes the transactions into a proper arrangement considering l_s (legitimacy score) and γ (extracted features) (Line 11). The algorithm then formulates the second conditional logic to determine the final range of the value of l_s (legitimacy score), with A_1 and A_2 as the minimum and maximum current values, respectively (Line 12). Attribute A_1 represents $(\tau - 2)/c$, A_2 represents τ/c , and a score of 2 represents the involvement of only two observational datasets. Upon finding the favorable condition stated in Line 12, the algorithm generates the flagging message of the validated legitimacy outcome l_o (Line 13); otherwise, it generates the malicious legitimacy outcome l_o (Line 15). Therefore, it can be seen that Equation (1) is used for the calculation of the legitimacy score considering the dependable attributes of l_s and η_{tr} , whereas probability is only used to assign in Line 6 and Line 8 toward transaction score α_s on the basis of the condition specified in Line 5. Hence, probability is used as a starting point of initialization for the transaction score, which is one of the dependable parameters in calculating the legitimacy score. Furthermore, the algorithm performs grouping based on the total features and computed legitimacy scores.

A closer look at this algorithm shows that initialization has been performed for local parameters such as the score of transactions, value of threshold, and score of legitimacy. This is followed by estimating the global parameters of the legitimacy score per the total frequency of accomplished transactions based on the computed score of legitimacy and cumulative extracted features. This means that the proposed framework computes the legitimacy score. However, it was initialized first, which offers potential adaptability to the algorithm to fine-tune itself to various dynamic conditions of cyber threats. Designated flagging of the message to be regular and threatening is performed based on this computation. Therefore, this algorithm contributes to a simplified and novel approach for computing the eligibility of an IoT node to be considered secure and reliable using the new concept of legitimacy score.

Further, back-tracing the steps of this algorithm will be challenging for any adversary if they attempt to disclose the data. The second conditional statement poses the first impediment to an adversary, where it is infeasible for an adversary to compute the A_1 and A_2 attributes that consist of private information depending on the network coefficient and the currently extracted feature. The next impediment is the computation of the legitimacy score (Line 10), as an attacker cannot gain information associated with the cardinality of transactions related to the blockchain, which repositions a massive amount of transactional information. Hence, extracting one set of specific transaction information without timestamp information from a voluminous transaction requires extensive computational resources from any form of adversary. Therefore, this algorithm introduces a robust first line of defense and legitimacy computation.

This study addresses the security issues of data vulnerabilities in smart cities by introducing a decentralized system to manage IoT devices. Further, the scheme uses a lightweight consensus method for minimizing resource requirements. In contrast, the presented blockchain scheme offloads specific computational demands to an explicit edge layer to reduce the associated cost and blockchain usage. This significantly increased the capability of the proposed model to handle large-scale IoT deployment.

4.2. Ethereum Data Reposition

Once the legitimacy score is estimated in the previous algorithm, the communication and data exchange are initiated within the IoT cloud environment. This will eventually mean that safeguarding the data exchanged among IoT devices is the most critical task. The proposed framework utilizes an Ethereum blockchain with a more robust trapdoor function to ensure both forward and backward secrecy. The term *trapdoor function* represents an operation that is simpler to compute in one direction but challenging to compute in the reverse direction without secret dependable data. Simultaneously, the algorithm emphasizes

retaining the maximum data integrity, confidentiality, and non-repudiation. In contrast, the exchanged data are subjected to repositioning within the Ethereum blockchain network.

Various operational steps are involved in the proposed framework for storing sensory data. The initial step toward storing sensory data is understanding the necessary data format. To format the data originating from the IoT device, encoding generates the binary format required for smart contract management in the Ethereum blockchain [43]. Furthermore, the smart contract used in our prior model was deployed to handle the data type for information generated by IoT devices [44]. Moreover, the encryption algorithm utilized in our previous model was deployed to cipher the information before storing the data in the blockchain [44]. The benefit of this approach is that it allows only legitimate members to have permitted access to and decrypt the exchanged information. Another significant advantage of this framework is that the proposed Ethereum blockchain can facilitate the storage of voluminous sensory data directly on the blockchain, unlike conventional Ethereum, which suffers from scalability issues. In the proposed framework, the facilitation of voluminous storage is ensured by storing the reference to the data in the form of hashtags. In contrast, actual data are stored in distributed clusters of cloud storage units. The operational steps of this algorithm (Algorithm 2) are as follows.

Algorithm 2. For Ethereum Data Reposition.

Input: η_{tr} , n
Output: ψ
Start
 1. init $\eta_{tr} = 0$, $\psi = 0$
 2. **For** $i = 1 : n$
 3. $\eta_{tr} \rightarrow$ extract scores from IoT devices
 4. **If** $\eta_{tr} = T$
 5. $\psi \rightarrow$ Evaluate data linked to η_{tr}
 6. store $\psi \rightarrow n(H_i)$
 7. $\psi \rightarrow$ forward(edge, cloud)
 8. **End**
 9. **End**
End

The discussion of the above-mentioned algorithmic steps is as follows. The algorithm takes the input of η_{tr} (cardinality of the transaction) and n (number of IoT devices), which, after processing, yields an outcome of ψ (reposited Ethereum data). The first steps of the algorithmic implementation are associated with initializing specific arguments. The algorithm initializes η_{tr} (cardinality of the transaction) and the hash value of the message exchanged by sensory device ψ as zero (Line 1). Considering all the n IoT devices (Line 2), the algorithm evaluates the content of the IoT devices. All scores associated with the IoT devices from the prior algorithm were obtained and stored in the same attribute as η_{tr} (Line 3).

Furthermore, the algorithm checks whether η_{tr} is true T (i.e., valid) (Line 4). Upon confirming the validity η_{tr} , the data are evaluated, which acts as a reference to the original data in the form of a hash score ψ (Line 5). The acquired information of the hashed scores is updated back to the file-sharing system within IoT devices. This is followed by storing the exchanged information in a hashed tree H_i and stored in the same matrix of ψ (hash value of the message exchanged) (Line 6). Finally, this information is forwarded to the edge and cloud nodes (storage units), completing the algorithm's operation (Line 7). The outcome of this algorithm is matrix ψ , now termed the reposited Ethereum data. A critical insight into the steps of algorithmic formulation shows that the proposed scheme offers a higher degree of security for data stored in hashed trees maintained in edge and cloud layer operations. This will eventually mean the algorithm assures a highly secure communication system, even if any private key is likely compromised. This phenomenon complies with forward secrecy. At the same time, this algorithm also offers higher security for keys

and all prior communications, even if any potential attacker compromises the current key. This phenomenon complies with backward secrecy. Hence, the proposed scheme exhibits forward and backward secrecy characteristics, which are the prime elements for designing any trapdoor function. Furthermore, it should be noted that the trapdoor function is one of the foundations of different variants of security protocols in cryptography. It offers a one-way function that is easier to evaluate in one direction. Still, reversing them without using an explicit token called trapdoor is impossible. In its distinct way, the hashing operation acts as that trapdoor function.

A closer look at this algorithmic implementation shows that the reference-based hash score of the original sensory data is stored in a distributed cloud environment. The input of essential sensory information associated with transactions is considered, leading to generating a hash score in a distributed form maintained in a tree as an outcome. The benefit of this approach is that no adversary can possess actual data, even if this algorithm attempts to be maliciously accessed. The distributed hashed information is computationally intensive to disclose by an adversary owing to multiple dependencies that require extensive resources. Hence, this algorithm can introduce data integrity. In addition, essential dependable attributes (e.g., transactional scores) are obtained from all individual IoT devices, whose legitimacy scores are assessed using a prior algorithm. Upon determining the legitimacy of these devices, the algorithm estimates the hash scores of the data carried by each IoT device. To ensure higher scalability in the proposed Ethereum data repositioning, the proposed framework considers that all cloud servers use a protocol for sharing exchanged sensory data maintained as a distributed file system to leverage higher and concurrent storage [43]. The value-added advantage of adopting this storage framework is that the conventional Ethereum blockchain facilitates a decentralized way to store data and provides a highly transparent mechanism to validate data/transactions; however, it must enable a robust distribution strategy. The proposed framework uses this protocol within a blockchain to offer decentralized storage and a faster and more effective distribution system. Thus, robust scalability was introduced by the proposed framework. The second benefit of this framework is that the generated hashed score is forwarded to the edge and cloud nodes for further assessment of any abnormality. It should be noted that the hosting of edge nodes is performed within the network layer, where the block nodes are maintained in distributed cloud storage units. Hence, all block nodes within a cloud correlate with the original data nodes and are kept as a decentralized hashed tree. This indicates that no member apart from IoT devices with higher legitimacy scores can access these block nodes. Hence, a higher degree of data confidentiality was incorporated into this framework.

This algorithm estimates the global legitimacy score in the prior algorithm, where the authenticated user/node is determined. Only in the case of a validated transaction (indicating a higher legitimacy score) will it be considered a criterion for storing data in the proposed Ethereum blockchain. Hence, the proposed algorithm offers non-repudiation of services in addition to data integrity and confidentiality. This can be stated based on the fact that for any attempt of a regular or illegitimate access request when forwarded to the application, the request message is subjected to verification by referring to the metadata stored within the block nodes in a cloud environment. Additionally, all transactional records are maintained and seamlessly updated over the decentralized hash tree. Hence, a higher degree of accountability for all nodes and transactions was retained within the proposed framework. The next part of the algorithm implementation further extends this operation to incorporate and emphasize the confidentiality perspective.

4.3. Ethereum-Based Confidentiality

This is the next module of implementation that emphasizes retaining the maximal level of data confidentiality in the Ethereum blockchain to ensure more secure internal communication in the IoT cloud environment. The proposed framework uses a consensus-based approach, leveraging the Proof-of-Work technique to validate the data for resisting

lethal cyber threats in the IoT. It should be noted that the proposed framework also uses an analytical approach to resist threats by subjecting data to the encoding mechanism. This helps safeguard the data from various types of attacks. This algorithm offers optimal data confidentiality for transforming the data into block structures in Ethereum. Under this framework, a public key is used to encrypt the data, whereas decryption is performed using a private key. The overall steps of this algorithm (Algorithm 3) implementation are as follows.

Algorithm 3. For Ethereum-based Confidentiality.

Input: I_b (indexed identity of Ethereum block), h_p (prior hash score)

Output: β_f (final evidence matrix), b_a (block added)

Start

1. **init** $I_b = 0, h_p = 0$
2. **constructBlock**(β)
3. **If** $\eta_{tr} = T$
4. evaluate $hash(b_h)$
5. **End**
6. **If** $I_b > 0$
7. $b_h = f_3(b_{arg})$
8. **End**
9. **EvaluateMiner**($F_e(\beta)$)
10. **While** ($A_3 == 0$)
11. **do** compute $\beta = \beta + 1$
12. **End**
13. **If** ($i == 1$)
14. $\beta = 1;$
15. $b_a = \text{constructBlock}(\beta)$
16. **Else**
17. $F_e = i$
18. $\beta_f = \text{EvaluateMiner}(\beta_f)$
19. $b_a = \text{constructBlock}(\beta)$
20. **End**

End

The illustration of the algorithm mentioned above for Ethereum-based confidentiality is as follows. The algorithm takes the input of I_b (indexed identity of the Ethereum block) and h_p (prior hash score), which, upon execution, results in an outcome of β_f (final evidence matrix) and b_a (block added). In the preliminary step, both input arguments are initialized to 0 (Line 1). An explicit function $\text{constructBlock}()$ is constructed considering the β evidence matrix to construct individual blocks using a precise hash score associated with the data (Line 2). After constructing a respective block, the algorithm checks for the condition to check if the η_{tr} cardinality of the transaction is true (T representing valid) (Line 3). The favorable case of this condition results in the evaluation of hash scores associated with block b_h (Line 4). Furthermore, the algorithm checks whether the value of the indexed identity of block I_b is greater than 0, representing the presence of at least one block (Line 6). If the indexed identity of the block is found to be valid, then the hashed block score is estimated using an explicit function $f_3(x)$ considering the input argument of blocks, that is, b_{arg} (Line 7). This function $f_3(x)$ extracts the digest score associated with the attribute b_{arg} , which further consists of hashed-based encryption SHA3, the current score of hash h_c , evidence matrix β , the indexed identity of block I_b , transaction λ , prior hash score h_p , and timestamp t . This operation returns the current value of the block b_h . The next step of implementation is associated with the execution of miners using a consensus approach with Proof-of-Work. For this purpose, another explicit function, $\text{EvaluateMiner}()$, was constructed, which considers its argument to be the final evidence F_e concerning β evidence matrix (Line 9). The β evidence matrix is empirically represented as $(F_e + 1)$. The algorithm constructs a new attribute, A_3 , which is checked for equivalence with 0 (Line 10). The

new attribute A_3 represents the logical AND operations between $(\beta + F_e)$ and $(2^n - 1)$. Simultaneously, if the condition formed by A_3 is equivalent to 0, the algorithm increases the value of the β evidence matrix (Line 11). The outcome of this operation results in potential evidence adhering to the consensus protocol, followed by the addition of novel blocks to the existing Ethereum blockchain network. A conditional logic to check for at least one block i is carried out (Line 13), and then the β evidence matrix is assigned as the highest probability score of 1 (Line 14). The function *constructBlock()* is the currently updated β evidence matrix in the prior step to generate a new block b_a to be added to the existing Ethereum blockchain (Line 15). However, suppose that the conditional logic is found to violate (Line 13). In this case, the algorithm assigns the current block I to the final evidence F_e (Line 17), followed by updating the β_f final evidence matrix and newly added block b_a (Line 18 and Line 19), thereby completing the final steps of this algorithmic implementation.

A closer look at the implementation of this algorithm will show that it offers a higher range of data confidentiality by leveraging the integrity of transactional records. This is achieved by implementing SHA3 encryption, which efficiently computes the digest's record. It should be noted that this operation generates a hash score adhering to one-way encryption, acting as a unique signature with a uniform-sized outcome. Such one-way hashing operations safeguard the data against malware, and botnets may be present deep within the network and often go undetected in conventional encryption frameworks. A better form of accountability and reliability of this algorithm can be ensured because if an adversary or any illegitimate node attempts to alter even one bit of data within the block, the complete digest structure will change, resulting in a potential trapdoor function. In addition, constructing a block in the Ethereum blockchain involves various forms of digest integration; hence, a minor change in one block will alter the hash scores even to a smaller extent. Furthermore, the integrity of this chain network of hash scores can be validated by using the consensus protocol in the Ethereum blockchain. However, the proposed framework uses a different consensus mechanism that requires extensive computational resources to mitigate the complexities of simplifying hash scores. This problem is addressed in the proposed algorithm by deploying a quantifiable evidence matrix, thereby securing the forwarding of the digest information to the Ethereum blockchain network. This operation requires little computational effort while maintaining higher hash chain integrity. This algorithm generates block hash scores by using multiple inputs: h_c , β , I_b , λ , h_p , and t . The framework entitles a block to estimate its hash scores only under the condition of a validated transaction using the first and second algorithms. In the presence of a valid number of blocks, as per their indexed information, the hash scores of each block are generated using the digest.

The framework also performs mining operations of blocks by deploying the final evidence matrix, whereas the verified generated evidence acts as an accountable parameter for non-repudiation. It should be noted that once the algorithm verifies a block, it is not possible to perform any form of alteration to the block content. Hence, the proposed framework ensures higher sustainability toward data confidentiality and integrity, even in the presence of highly vulnerable and unreliable IoT and cloud networks intruded upon by lethal cyber-attacks. Therefore, the primary contribution of this algorithm is its cost-effective integrity checks for hash chains and the less computational effort required to generate evidence, unlike the conventional consensus method in blockchain. Furthermore, a hash tree is implemented to retain hash scores and sensory data from the IoT devices. This feature offers the immutability characteristics of the proposed Ethereum blockchain, which can secure sensory data in a distributed and decentralized manner in IoT cloud systems. The following algorithm performs further analytical operations to boost the security features.

4.4. Analytical Method for Resisting Threats

This implementation module is meant to complement prior algorithmic operations. From the previous algorithm, it is noted that the construction of a block is carried out after

the validation of the sensory data has been accomplished, followed by forwarding the evidence over the complete network structure of the Ethereum blockchain. This part of the implementation applies a simplified analytical approach to add a layer of data confidentiality apart from that obtained from prior Ethereum-based confidentiality algorithms. The first task toward accomplishing this target is to map the essential parameters for enhancing computational efficiency by transforming the categorical scores into a numerical structure. This operation is followed by the truncation of redundant and irrelevant features, resulting in the optimal selection of parameters. This module of implementation selects the optimal quantity of attributes using a similarity measure, which can be empirically represented as follows:

$$\mu = \frac{A_4}{A_5 \cdot A_6} \quad (2)$$

The above empirical expression (2) shows the formulation of similarity measures μ , which are used to determine the association of two arbitrary attributes, g_1 and g_2 . The dependent variables for Equation (2) are as follows.

$$A_4 = \sum_{i=1}^d \rho_1 \cdot \rho_2 \quad (3)$$

$$A_5 = \sqrt{\sum_{i=1}^d (\rho_1)^2} \quad (4)$$

$$A_6 = \sqrt{\sum_{i=1}^d (\rho_2)^2} \quad (5)$$

Equations (3)–(5) show the dependable variables A_4 , A_5 , and A_6 formulations, respectively. Furthermore, the formulations of these variables are carried out considering entities such as ρ_1 and ρ_2 representing $(u_1 - g_1)$ and $(u_2 - g_2)$, respectively. Simultaneously, the arbitrary inputs g_1 and g_2 are formed by extracting the mean value of the data points (u_1 and u_2) concerning the number of individual data d . The primary contribution of this similarity measure metric, μ , is to efficiently transform the attributes to generate novel dimensional data without eliminating or affecting the core information present within the sensory data. This module also generates a simplified statistical function for encoding f_{en} as follows:

$$f_{en} = (\beta_{up}(D), \delta(D)) \quad (6)$$

According to empirical expression (6), the computation of the statistical function for encoding f_{en} is dependent on two variables, β_{up} and δ , which represent novel samples of updated data within the evidence matrix and error-prone scores, respectively, considering dataset D . The system evaluates $\beta_{up}(D)$ by considering the mean of the feature γ within datasets D and data point u_1 . It should be noted that this function f_{en} is used to obtain the encoded feature from the dataset by transforming it, which acts as an additional layer of security toward the essential features of the data, thereby resisting potential threats.

4.5. AI-Based Security Optimization

The proposed framework includes a novel AI model that modifies conventional neural networks for faster inference, efficient training, and compact representation. For this purpose, the framework uses a neural network consisting of all interconnected nodes (neurons) organized in the form of layers to learn the patterns of the dataset. The first novelty of this AI model is the incorporation of a *unique optimization policy* designed to work well in dynamic and practical environments. The second novelty of this AI model is incorporating a mechanism to *speed the optimization* process, resulting in faster training and effective inference as an outcome. These two joint features of conventional neural networks in the proposed AI model are designed to be fast, efficient, and well suited for real-world

IoT applications, possibly with a focus on human interaction or social systems. It targets excelling tasks that require quick adaptation to changing conditions or in domains where speed is essential. The proposed AI model classifies classes corresponding to the normal and adversary. The idea is to maximize the detection of abnormalities and reduce the duration of training. The adversary’s detection and classification are based on the features acquired from the previously implemented algorithm to *evaluate the legitimacy score*. The AI model was designed by constructing three layers of neural networks: input, hidden, and output.

Figure 2 shows the solution representation of the proposed AI model, where the input layer is fed with m number of features γ obtained from dataset D. The process of abnormality detection in the transaction process is carried out by allocating weight scores ϕ , where the hidden layer further performs fine-tuning of the weight score. The hidden layer also computes the bias function with a target to generate a score of the resultant weight score $\phi^{\gamma+2}$ while the resultant bias function can be represented as $\phi^{\gamma+3}$. The framework proceeds further toward the computation of an activation function empirically defined as follows:

$$A_f = \phi_1 \cdot A_7 \cdot \phi_2 \tag{7}$$

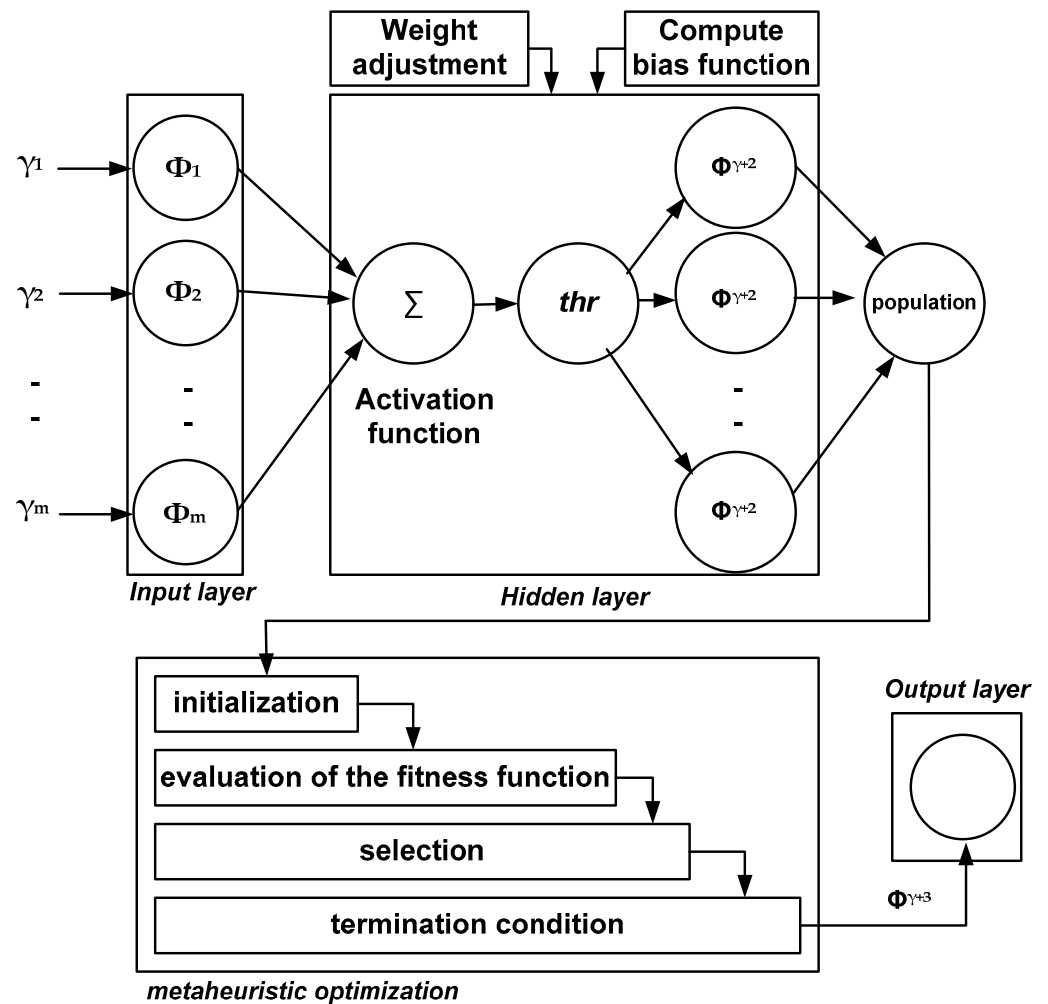


Figure 2. Proposed AI model.

Equation (7) represents the formulation of the adopted activation function, A_f , using three dependable variables ϕ_1, A_7 , and ϕ_2 . The first and third variables ϕ_1 and ϕ_2 represent the weight score and bias function, respectively, whereas the second variable A_7 , is computed as follows:

$$A_7 = A_{f1} \left[\sum_{i=\chi}^{\gamma} A_8 + A_9 \right] \quad (8)$$

In Equation (8), the computation of the second variable A_7 in the parent expression (7) considers A_{f1} a sigmoidal activation function. Variable A_8 represents the product of the features extracted from the dataset (D^γ) concerning neuron weight χ and primary weight score ϕ^γ , i.e., $A_8 = \chi \cdot \phi^\gamma$. The second variable, A_9 in Equation (8), represents the bias scores. Based on the activation function A_f in (7), the proposed AI model generates outcome labels to assist in tagging the analyzed feature as normal or adversary. There is a specific rationale behind adopting this specific activation function, viz., sigmoidal activation function, which offers a faster prediction response in the range of 0 and 1. At the same time, it can normalize the outcome of neurons. Furthermore, this AI algorithm maintains a higher degree of predictive accuracy by introducing nonlinearity through a sigmoidal activation function that allows the proposed AI model to approximate a complex relationship with the traffic information in IoT. This indirectly also contributes to optimizing smart contracts to predict the results of various conditions, thereby leveraging anomaly detection.

The next part of the proposed AI model is associated with implementing a *unique optimization policy* in which a metaheuristic optimization approach is adopted to find the optimal solution. The first step of this unique optimization policy is to perform *initialization*, in which the system starts with a population of candidate solutions that are usually arbitrarily generated. The population data are generated as $\sigma_\gamma(x, y)$ where the σ_γ represents the position of the population data y at a specific position of x , and the ranges of the values of x and y are $(1, \gamma)$ and $(1, D)$, respectively. The next part of the implementation is associated with *evaluating the fitness function* using a predefined objective function. This fitness function aims to identify the robustness of the solution to security problems related to optimizing an adversary's detection and classification. The proposed framework outperforms the estimation of the fitness function to explore the optimal result for determining abnormality patterns caused by cyber threats. Hence, the proposed framework empirically formulates the optimal solution as follows:

$$\Omega = S^{-1}[\Delta r] \quad (9)$$

Equation (9) shows the computation process of the fitness function to explore the optimal solution for determining any forms of abnormalities. The variable Ω represents the optimal solution, S represents the complete sample, and Δr represents the effective result r obtained by differentiating the target resultant T_r and classifying the resultant C_r . The prominent location of the sample was detected based on this fitness function, and the location of the sample was subjected to an updating process.

It should be noted that such location information can be constantly updated in a dynamic environment in IoT. This completes the *selection* process in which an individual from the population is selected for further processing based on their fitness. This step involves probabilistic selection mechanisms, in which solutions with higher fitness are more likely to be chosen. Based on the higher score of the optimal fitness function, the framework updates the operation of features mainly associated with anomalies. After meeting the maximum number of simulation iterations, the system executes the termination condition.

A closer look at the proposed AI scheme shows that it has used a revised neural network version. It is meant to eliminate complexities associated with iterative operation with suboptimal performances reported in existing learning-based models in Section 2. Furthermore, the model parameters are transferred to smaller, more efficient models (hidden layers), reducing computational demands. Moreover, the core architecture (Figure 1) consistently monitors the outcome of both the edge and cloud layers, which induces persistent monitoring of both the AI and blockchain systems, where inefficiencies can be identified and curtailed significantly. Hence, considerably less computational overhead is observed in the proposed system when AI is integrated into the blockchain. The contribution of the proposed AI model is that it effectively maintains a balance toward exploring novel regions

associated with the search space and utilizing the optimal solutions for accomplishing an optimal solution leading to the classification of the nodes. Furthermore, the proposed AI model contributes to effective classification performance with reduced issues of overfitting and minimal processing duration. The following section discusses the outcomes of the study.

5. Results

This section presents the results of the study. As the proposed study introduces a novel form of Ethereum blockchain design, it is necessary to develop an effective strategy to analyze its outcome, as it is meant to support the maximum number of elements of smart cities in the IoT, and its performance is not restricted to specific elements of smart cities. For this purpose, the model is primarily analyzed for its confidentiality in the IoT environment, where the requirements for strengthening the confidentiality of IoT applications are investigated. From the IoT application perspective, confidentiality concerns are assessed via generated voluminous sensory data that may consist of proprietary industrial data, personal information, and location data. The assessment also investigated potential threats associated with transaction linkability, data leakage, various attacks, and blockchain analysis.

Furthermore, a test environment is designed to simulate IoT transactions on the proposed Ethereum blockchain with confidentiality attributes. At the same time, a standard performance metric was used to monitor the effectiveness of the study model. The performances of the proposed Ethereum blockchain and AI model were validated and tested using various performance metrics.

5.1. Assessment Environment

The proposed study was performed on a standard 64-bit Windows machine with a core-i7 processor. The simulation parameters used to configure the proposed model are presented in Table 1. The initialized IoT devices were set to 200 for the preliminary part of the experimental analysis, which was later maximized to 500 to check the system's sustainability. The IoT devices involved in the assessment are allocated specific account information, a public/private key, and a blockchain wallet that can be used to access the user account and verify the transaction in the Python environment. The Ethereum nodes were initialized using go-Ethereum [45] and configured over a virtual machine. The framework also uses a public and private key pair to implement encryption in the proposed framework, thereby ensuring the presence of a minimally single account owned externally. The system generates 10-bit public addresses using public keys associated with an externally constructed user account in the blockchain network. This means that the public address can be utilized to deploy the user's smart contract, followed by forwarding transactions. A dedicated communication interface between the Ethereum blockchain and the application interface was established using NodeJS (latest v. 22.x). The duration of transactions is monitored using a decentralized smart contract known as Etherscan [46], whereas the initial blockchain network is designed using the Ganache tool.

Table 1. Simulation parameters.

Parameter	Values
Number of accounts	200
Number of transactions in 1 batch	20
Number of peers/devices	10
Type of genesis block	override
Generated transaction rate	0.01 s
Frequencies of transaction	40,000
IoT devices	200
Mode of smart contract	Independent execution

The proposed framework was implemented and analyzed using the CIC-IoT dataset, a benchmark real-time dataset encapsulating various forms of lethal cyber threats in the IoT [47]. The dataset was designed considering 105 IoT devices, with 33 reported lethal attacks categorized into seven classes. The captured traffic in its original form during reported attacks was maintained in the form of *.pcp* files, while *.csv* files were used to reposition the extracted features *.pcp* files using a machine-learning approach. Furthermore, multiple tools were used to organize the dataset suitable for analysis, which used feature extraction using *DPKT* and classification *.pcp* files were generated using *TCPDump* to generate smaller files of multiple numbers. PySpark handles the data, whereas *Mergecap* integrates all classified data *.pcp* files. The algorithms were extensively benchmarked after setting up the Python environment to obtain the final outcome.

5.2. Result Accomplishment

The numerical results are presented in Tables 2–4, where multiple performance metrics are used to assess the effectiveness of the proposed framework. The primary benchmarking of the proposed model was performed by comparing the proposed study model with existing AI models (Tables 2 and 3) and existing blockchain approaches (Table 4). The outcome in Table 3 was obtained by averaging all individual outcomes of the standalone AI models shown in the existing system. Secondary benchmarking of the proposed framework was carried out by comparing the proposed study with some recent literature, such as Aldyaflah et al. [21], Elisa et al. [22], Javed et al. [17], Khor et al. [23], Lee and Song [18], Omar et al. [19], Qiu et al. [20], Ugochukwu et al. [24], Ullah et al. [25], Viswanadham and Jayavel [26], Yousra et al. [27], and Agüero et al. [16]. The primary reason for considering the literature mentioned above as existing systems in comparative analysis is that they have innovative methods of blockchain design that have been reported to be much better than conventional blockchain design in the literature.

Table 2. Numerical outcomes for AI approaches.

Approaches	Accuracy (%)	Algorithm Processing Time (s)
Proposed	98.4	0.389
Decision Tree (DT)	85.2	0.687
Support Vector Machine (SVM)	87.5	0.509
Random Forest (RF)	90.5	0.299
Logistic Regression (LR)	88.7	0.898
K-Means Clustering (KMC)	82.3	1.207
Reinforcement Learning (RL)	92.2	0.908
Artificial Neural Network (ANN)	91.5	2.871
Convolution Neural Network (CNN)	93.7	3.803
Recurrent Neural Network (RNN)	85.4	2.596
Long Short-Term Memory (LSTM)	90.1	1.977
Auto Encoder (AE)	92.8	2.902

Table 3. Detection accuracy for multiple adversaries.

Classes of Adversary	Proposed	Existing System
DDoS	98.5	90.4
Brute-Force	99.5	89.6
Spoofing	99.8	87.8
Recon	98.9	87.9
Host Discovery	97.3	92.1
Web-based	97.1	92.3
Mirai	98.1	92.4

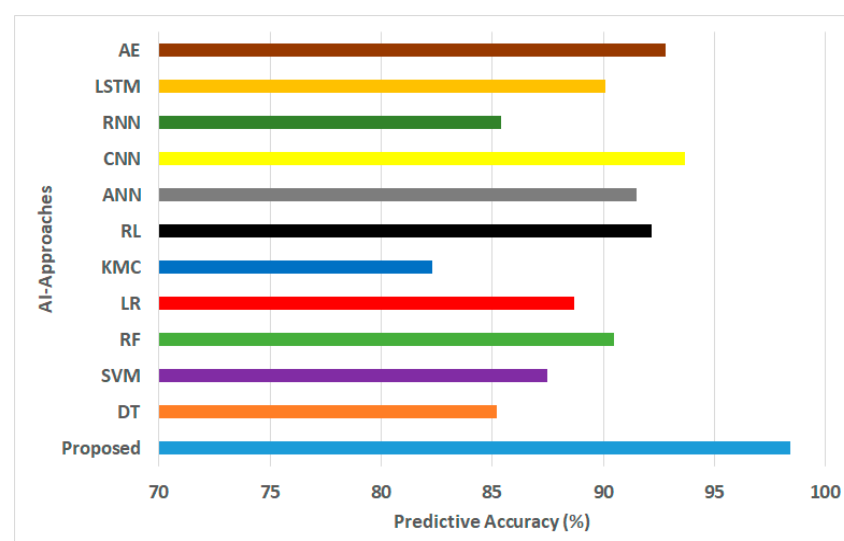
Table 4. Multi-metric performance outcome for blockchain approaches.

Blockchain Approaches	Transaction Throughput	Resource Consumption	Confirmation Time	Detection Accuracy	Processing Time
Proposed	4500	29.87	0.2665	98.65	0.6766
Aldyafiah et al [21]	2765	49.89	2.544	91.45	5.9978
Elisa et al [22]	1988	47.83	1.006	89.03	1.1886
Javed et al. [17]	2296	42.11	2.313	89.57	5.872
Khor et al. [23]	2011	47.29	1.926	87.06	2.6088
Lee and Song [18]	2981	62.56	3.216	90.02	6.446
Omar et al. [19]	1989	51.99	1.132	85.11	3.897
Qiu et al. [20]	1303	51.05	0.997	87.11	2.651
Ugochukwu et al. [24]	3101	62.12	1.093	91.37	2.196
Ullah et al. [25]	3655	54.13	3.887	91.76	4.127
Viswanadham and Jayavel [26]	2199	55.36	2.187	90.1	4.302
Yousra et al. [27]	3211	43.87	2.876	92.67	4.968
Aguero et al. [16]	3266	65.02	3.107	91.52	5.302

The numerical evaluation shows that the proposed framework of the Ethereum blockchain uses a unique and novel AI model to perform better in terms of multiple performance parameters. The outcome shows that the proposed study model offers optimal confidentiality and cost-effective operation capable of resisting cyber threats without affecting the primary operation in IoT and cloud environments. The discussion of the results is as follows.

5.3. Result Discussion

The results are discussed with respect to the benchmarked outcome in the context of the AI (Figures 3–5) and blockchain models (Figures 6–10). The analysis considers the standard and most frequently adopted AI methods as conventional machine-learning approaches (Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), Logistic Regression (LR), K-Means Clustering (KMC), and Reinforcement Learning (RL)) and conventional deep learning approaches (Artificial Neural Network (ANN), Convolution Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Auto Encoder (AE)). The performance metrics considered were the predictive accuracy, processing time, and detection accuracy.

**Figure 3.** Predictive accuracy for AI approaches.

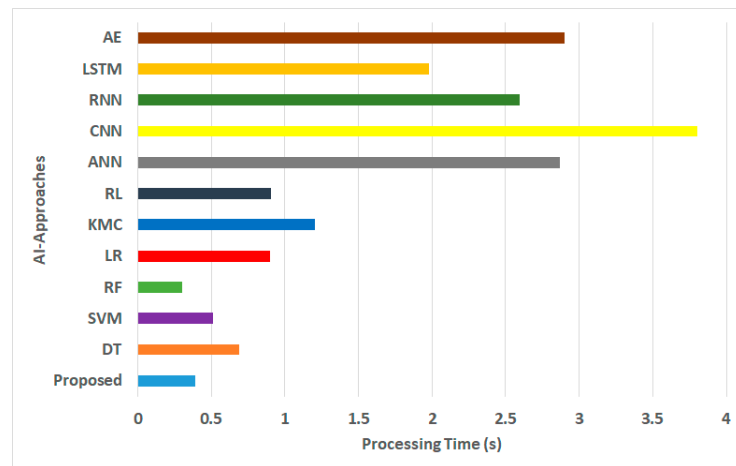


Figure 4. Processing time for AI approaches.

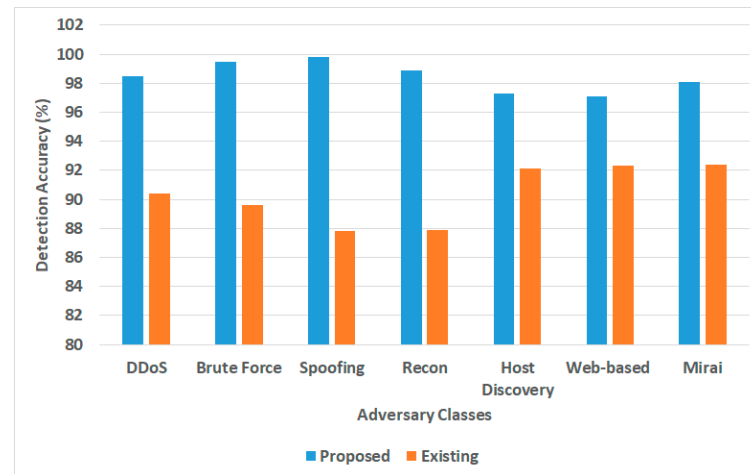


Figure 5. Detection accuracy for AI approaches.

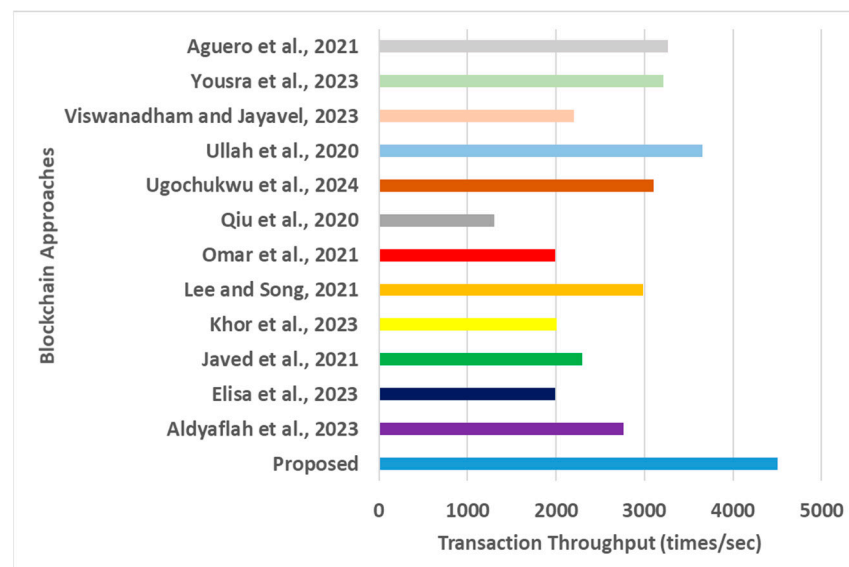


Figure 6. Transaction throughput for blockchain approaches [16–27].

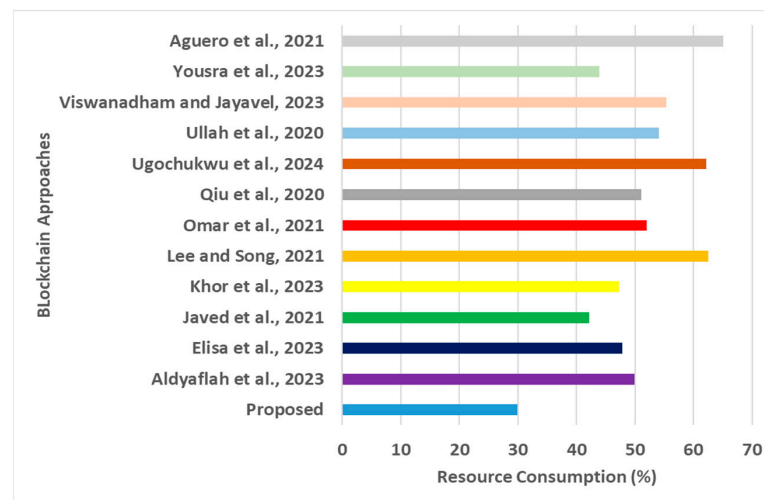


Figure 7. Resource consumption for blockchain approaches [16–27].

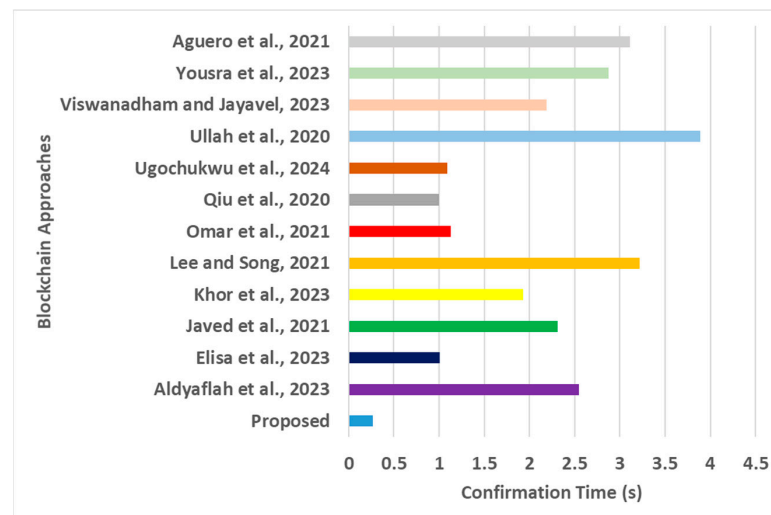


Figure 8. Confirmation time for blockchain approaches [16–27].

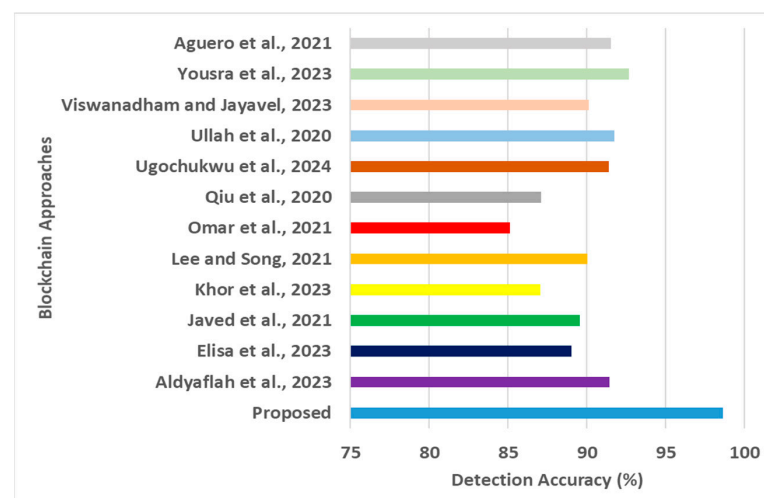


Figure 9. Detection accuracy for blockchain approaches [16–27].

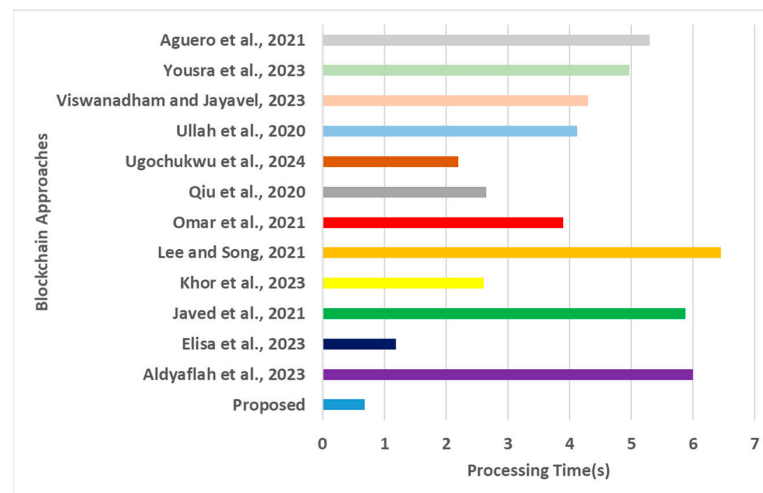


Figure 10. Processing time for blockchain approaches [16–27].

The inference of the outcome accomplished is as follows:

- Predictive Accuracy:** Predictive accuracy is expressed as a percentile and is computed by dividing the number of correct predictions by the total number of predictions. The quantified outcome in Figure 3 shows that the proposed AI model offers approximately 9.3% increased predictive accuracy compared with the mean value of all existing AI models. Lower predictive accuracy scores were observed for KMC ($Acc = 82.3\%$), RNN ($Acc = 85.4\%$), and DT ($Acc = 85.2\%$). The primary reason for this is the unsuitability of these algorithms for capturing highly complex relationships associated with traffic data in a threat environment. However, approaches such as CNN ($Acc = 93.7\%$) and AE ($Acc = 92.8\%$) have better predictive accuracy after the proposed framework. However, the higher computational resource demands for CNN and AE reduce their applicability to yield fewer practical outcomes. The primary reason based on specific scenarios for the optimal predictive accuracy score ($Acc = 98.4\%$) can be explained by two main reasons: (i) the proposed framework performs the analytical operation in both the edge and cloud layers that maintain a higher degree of indexed transactional information to yield better accuracy even before subjecting it to the AI model; (ii) unlike any existing AI models used for secured blockchain operation, the proposed framework implements a neural network integrated with a metaheuristic optimization method acting as multiple levels of faster-operating filtering process to narrow down the predictive outcome to a highly accurate one;
- Processing Time:** This performance metric is responsible for computing the overall algorithm processing time for the proposed and conventional AI methods under consideration. Figure 4 shows that the proposed framework reduces the algorithmic processing time by approximately 13% in contrast to the mean values of existing AI models. The justification behind this outcome is as follows. Unlike the existing approaches discussed in Section 2, the proposed framework does not instantly convert the incoming data to the blockchain or directly apply its AI model. This is a particular scenario when the proposed scheme reduces the processing time while the existing system cannot. The proposed framework initially constructs a structure for repositing data over the Ethereum blockchain, followed by building blocks and evaluating the miners. Furthermore, it introduces an analytical method to thwart all possible dynamic threats and then implements the AI model. Hence, the input data to the AI model are characterized by higher-quality data and require a less iterative method for its AI model to generate its predictive outcome. However, this is not the case with conventional AI models, which otherwise apply a series of standalone iterative operations, resulting in a higher processing time. It should also be noted that deep learning-based approaches, such as AE ($proc_{time} = 2.9$ s), RNN ($proc_{time} = 2.5$ s), CNN ($proc_{time} = 3.8$ s),

and ANN ($proc_{time} = 2.8$ s), consume more processing time than conventional machine-learning approaches. It can also be noted that RF ($proc_{time} = 0.299$ s) offers reduced processing time in contrast to the proposed framework ($proc_{time} = 0.389$ s); however, it lacks interpretability, and the processing time is expected to increase when exposed to real-time streamed data. It should be noted that the proposed scheme emphasizes processing time (PT) during its final evaluation in contrast to the conventionally adopted metric of Computational Time Complexity (CTC) owing to the following reasons: (i) both PT and CTC are typically used for assessing algorithmic performance; however, CTC provides only a theoretical efficiency measure while PT provides empirical evidence of applying algorithms to practical world scenarios based on hardware; (ii) the CTC parameter emphasizes the asymptomatic behavior of an algorithm by offering high-level performance visualization; however, it abstracts away the inclusion of any implementation specifications while PT offers a concrete measure of the runtime of an algorithm considering extensive attributes, for example, environmental factors, software, hardware, etc.;

- *Detection Accuracy:* This performance metric was computed by dividing the number of attacks positively detected by the total number of attack test instances introduced. The outcome in Figure 5 shows that the proposed framework offers an improved detection accuracy of approximately 8.1% in contrast to the mean values of conventional AI models. The proposed AI models offer higher threat detection accuracy, specifically for DDoS attacks ($Det_{acc} = 98.5\%$), Brute-Force attacks ($Det_{acc} = 99.5\%$), spoofing attacks ($Det_{acc} = 99.8\%$), and Recon attacks, mainly concerning vulnerability scan and port scans ($Det_{acc} = 98.9\%$). The proposed framework also showed better threat detection accuracy for Mirai attacks ($Det_{acc} = 98.1\%$). At the same time, there is a less significant difference in detection accuracy performance for identifying host discovery attacks ($Det_{acc} = 97.3\%$) and web-based attacks ($Det_{acc} = 97.1\%$). On the other hand, the existing AI model shows effective threat detection for Mirai attacks ($Det_{acc} = 92.4\%$), Web-based attacks ($Det_{acc} = 92.3\%$), and host discovery attacks ($Det_{acc} = 92.1\%$). Other attacks, such as DDoS, brute-force attacks, spoofing attacks, and Recon attacks, must be more optimally detected by the existing system. It was noted that most of the existing AI models must undergo extensive operation, which is costly and time-consuming, with overfitting issues surfacing. The exact scenario of better performance of the proposed system for higher detection accuracy is noted because of the decentralized blockchain operation performed on multiple edge devices, whose interconnected network is further indexed and hosted in the cloud layer in its distributed storage units. Furthermore, the analytical method implemented in the proposed framework is meant to eliminate unnecessary data and features that reduce computational processing time and offer ample scope for both neural network and metaheuristic optimization. These integrated operations not only allow the system to operate faster to detect any form of abnormalities and inconsistencies but also offer reliable closure toward its inference.

The next part of the assessment is associated with benchmarking the proposed model based on the recent literature on various evolving blockchain frameworks in IoT. The evaluation was carried out using multiple performance metrics: (i) transaction throughput (Figure 6), which measures the number of transactions processed per second, as high throughput is essential for IoT applications with numerous devices generating transactions; (ii) resource consumption (Figure 7): this is evaluated as the computational resources (CPU, memory) and storage space required to execute privacy-preserving transactions on the Ethereum blockchain because high resource consumption can limit scalability and increase costs; (iii) confirmation time (Figure 8): this measures the time taken for a transaction to be included in a block and confirmed by the network, as short confirmation times are essential for IoT applications that require timely and reliable transaction processing—the detection accuracy (Figure 9) and processing time (Figure 10). The graphical outcomes are as follows.

The inference of outcomes (Figures 6–10) are as follows:

- *Transaction Throughput:* Higher transaction throughput is always anticipated for any blockchain operation concerning large-scale real-world IoT applications. A closer look at Figure 6 shows that the approaches of Elisa et al. [22], Omar et al. [19], and Qiu et al. [20] recorded the lowest transaction throughputs. Elisa et al. [22] introduced an authentication mechanism that considers multiple contents of blockchain addresses, such as user identity, transactions, and record numbers. At the same time, these values continue to escalate, demanding more computational effort toward iteratively reforming authentication. Hence, the throughput declines. Omar et al. [19] offered a segregated structure for system applications with intrinsic data, while the blockchain was kept as an external structure. Hence, fetching services and verifying many users are witnessed with a reduced throughput. Qiu et al. [20] introduced a private blockchain with sophisticated query request processing using dynamic location variables. The anonymizer module performs its task effectively to obfuscate the query for the server. However, when exposed to a dynamic threat environment, this approach demands a higher dependency on the blockchain network to undergo a re-analysis process concerning its query. Hence, the throughput drops significantly, even though it is one of the best static data/transaction approaches. However, the approaches of Ullah et al. [25], Yousra et al. [27], and Aguero et al. [16] have been shown to offer better throughput after the proposed framework. However, these frameworks are specifically designed for particular applications that need to be more flexible in supporting generalized IoT applications with a more significant stream of transactions. Two factors of the explicit scenario can justify the optimal throughput results for the proposed model: (i) the mechanism of evaluation and assessment of the legitimacy score offers more accountable nodes to participate in the transaction process, while the new Ethereum design generates a final evidence matrix that reduces the computational effort required by a system hosted in edge devices, and (ii) a novel neural network-based approach with the inclusion of dynamic weight and bias tuning with selection of optimal conditions leads to more accountable records needed to support a large number of transactions. The quantified outcome shows that the proposed framework offers an approximately 20% increase in throughput compared with the mean scores of the blockchain-based approaches;
- *Resource Consumption:* Almost every blockchain operation includes extensive computational resources, and consistency increases with more users joining the network. A closer look at Figure 7 shows that the proposed framework offers significantly lower resource consumption. In contrast, the approaches of Lee and Song [18], Ugochukwu et al. [24], and Aguero et al. [16] offer significantly higher resource consumption. The approach proposed by Lee and Song [18] was used to deploy ring signatures to develop a blockchain structure. Although this adoption offers better privacy preservation by hiding the sender's and receiver's addresses, its smart contract method extensively deploys symmetric key encryption, which increases the dependencies of secret key storage within the nodes. This architecture was initially designed for the healthcare sector in IoT; however, when exposed to a much larger-scale IoT environment with multiple constructed application domains, the resource dependencies significantly increase. The study model implemented by Ugochukwu et al. [24] suffered from similar challenges associated with smart contract operations between IoT devices and blockchain networks. The framework presented by Aguero et al. [16] involves many software components to manage node identification, including the cyclic process of managing and retaining identifiers. This cyclic task offers a significant hurdle to the intruder; however, it also impedes an average user, preventing them from undergoing similar authentication iteratively. Although this study model provides genuine resistance to multiple levels of security threats, there is a trade-off between data integrity and data non-repudiation when this model is exposed to a dynamic form of cyber threats in a large environment. The prime event when the proposed system is found to excel at optimal performance in contrast to the existing scheme can be

justified by three factors concerning the reduced score of resource consumption for the proposed framework: (i) the proposed framework progressively increases the data quality in every incremental step of operation, leading to less computational effort toward the minimized size of data; (ii) the encoding mechanism further complements this evaluation process during verification with much less computational effort and data dependencies; and (iii) the method of generating evidence in the consensus approach and hash-based integrity checks is carried out using extracted features and not raw data, leading to increasingly lower resource dependencies. The quantified outcome shows that the proposed framework offers approximately 22% reduced resource consumption compared to existing AI models;

- *Confirmation Time:* This performance parameter represents the system's response time toward validating transactions, which is essential for any blockchain-deployed IoT application that demands faster responsiveness. This responsiveness depends on the structure of the blockchain and its integration into the system. Figure 8 shows the existing approaches to encounter slightly longer confirmation times. Although this higher confirmation time score is no more than 4 s, they can go extensively with many transactions on streamed IoT applications. Ullah et al. [25] reported a higher confirmation time of 3.887 s when analyzed in a standard test environment in the proposed analysis. The Merkle root tree has been used to manage use-case data, increasing the computational overhead due to data block hashing and integration. This increased the confirmation time. The blockchain model presented by Aguero et al. [16] was also found to have a higher confirmation time of 3.107 s, which is mainly due to the involvement of an external transaction manager in validating the account. This mechanism includes extensive validation and unlocking of information using sophisticated passphrase management. Although this framework offers better data integrity and a higher degree of bidirectional secrecy in cryptography, its extensive operation requires more resources and validation time. The model presented by Aldyaflah et al. [21] also exhibited a slightly longer confirmation time of 2.544 s. This model introduced an access control system using the roles of users for better data confidentiality, whereas smart contracts were used as secured data stores. The data structure used involves extensive mapping of tag indexes with the database, offering better data secrecy; however, fetching and query management for concurrent clients on a large scale is challenging, apart from including a higher confirmation time. However, the reduced confirmation time for the proposed framework was mainly attributed to the inclusion of similarity measures for the optimal selection of features. Furthermore, the encoding process performed on features offers extensive resistance to dynamic cyber threats and a lightweight transformation process. This phenomenon within the proposed scheme is another specific scenario that reduces the dependency on iterative validation, even on a large scale, and for concurrent users, reducing confirmation time. Unlike existing blockchain models, the quantified outcome shows that the proposed model offers an approximately 19% reduced confirmation time.

Apart from the above results, it was found that the proposed framework offers 89% increased detection accuracy (Figure 9) and 34% reduced processing time in contrast to existing blockchain methods (Figure 10). Hence, from the perspective of the accomplished outcome, the proposed framework offers cost-effective data confidentiality when encountering dynamic cyber threats for the maximal elements of smart cities in an IoT environment. In addition, computational cost-effectiveness has been proven to support the newly introduced security features.

6. Conclusions

In conclusion, our innovative three-layered mechanism integrating a decentralized Ethereum blockchain with AI models significantly improves data confidentiality, particularly in IoT smart city applications. By distributing blockchain operations across edge devices and cloud environments, our framework enables multidimensional secure data

management within an IoT cloud ecosystem. By leveraging a unique legitimacy scoring system, our approach secures data stored within edge and cloud systems, ensuring transaction integrity and confidentiality. Upon identifying secure transaction conditions, the framework collects sensor data and stores them in a tamper-resistant format to mitigate cyber threats effectively. Our implementation includes a novel consensus method that significantly reduces the computational overhead while maintaining the integrity of the transaction hashes. By distributing the blockchain network with digests generated through algorithmic processes, we enhance the security of the original sensory data generated by IoT smart cities, thereby minimizing intrusion risks. The primary security stage verifies digests on distributed hashes generated across edge nodes, followed by a secondary security stage, where the AI model appends blocks to the proposed blockchain network after data verification. Utilizing a confidentiality method, we transformed raw sensory data into a distinct form to prevent data disclosure to potential attackers. Additionally, an analytical model encodes features to resist data disclosure, whereas a neural network-based approach predicts abnormalities in the IoT cloud environment. Our framework demonstrated approximately 9.3% increased predictive accuracy, 13% reduced processing time, and 8.1% increased detection accuracy compared to conventional AI models. Furthermore, it exhibits approximately 20% increased transaction throughput, 22% reduced resource consumption, 19% reduced confirmation time, 89% increased detection accuracy, and 34% reduced processing time compared with conventional blockchain-based approaches. Future work will explore scalability, enhance consensus methods, optimize resource consumption, integrate additional AI techniques, and conduct real-world deployments to advance further and validate our proposed solution in diverse smart city environments.

Author Contributions: Conceptualization, methodology, and validation: B.U.I.K., K.W.G., A.R.K. and M.F.Z.; formal analysis and investigation: K.W.G., M.F.Z. and M.C.; writing—original draft preparation: B.U.I.K., K.W.G., M.C. and A.R.K.; writing review and editing: B.U.I.K., M.C. and M.F.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Project Grant KFU241665.

Data Availability Statement: The data presented in this study are available on request from the corresponding author due to grant restrictions.

Acknowledgments: The authors express their appreciation for Bisma Rasool's effort in proofreading and editing the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Anwar, F.; Khan, B.U.I.; Kiah, M.L.B.M.; Abdullah, N.A.; Goh, K.W. A Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 878–907. [[CrossRef](#)]
2. Al Hwaitat, A.K.; Almaiah, M.A.; Ali, A.; Al-Otaibi, S.; Shishakly, R.; Lutfi, A.; Alrawad, M. A new blockchain-based authentication framework for secure IoT networks. *Electronics* **2023**, *12*, 3618. [[CrossRef](#)]
3. Khan, B.U.I.; Goh, K.W.; Mir, M.S.; Mohd Rosely, N.F.L.; Mir, A.A.; Chaimanee, M. Blockchain-Enhanced Sensor-as-a-Service (SEaaS) in IoT: Leveraging Blockchain for Efficient and Secure Sensing Data Transactions. *Information* **2024**, *15*, 212. [[CrossRef](#)]
4. Xu, D.; Gao, Y.; Xiao, X. Precision Poverty Alleviation Methods in the Agricultural Field Based Upon Wireless Communication Networks and Blockchain. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 2687445. [[CrossRef](#)]
5. Mathur, S.; Kalla, A.; Gür, G.; Bohra, M.K.; Liyanage, M. A Survey on Role of Blockchain for IoT: Applications and Technical Aspects. *Comput. Netw.* **2023**, *227*, 109726. [[CrossRef](#)]
6. Abubakar, M.; Jarocheh, Z.; Al-Dubai, A.; Liu, X. A Survey on the Integration of Blockchain and IoT: Challenges and Opportunities. In *Advanced Sciences and Technologies for Security Applications*; Springer International Publishing: Cham, Switzerland, 2022; pp. 197–221. ISBN 9783031044236.
7. Alam, T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. *Computers* **2022**, *12*, 6. [[CrossRef](#)]
8. Sathish, C.; Rubavathi, C.Y. A Survey on Blockchain Mechanisms (BCM) Based on Internet of Things (IoT) Applications. *Multimed. Tools Appl.* **2022**, *81*, 33419–33458. [[CrossRef](#)]

9. Imran, M.; Zaman, U.; Imran, M.; Imtiaz, J.; Fayaz, M.; Gwak, J. Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment for Pandemic Preparedness, Challenges, and Solutions. *Electronics* **2021**, *10*, 2501. [\[CrossRef\]](#)
10. Hariharan, R.; Tyagi, A.K.; Soni, G. A Survey on Blockchain-Internet of Things-Based Solutions. In *Privacy Preservation and Secured Data Storage in Cloud Computing*; IGI Global: Hershey, PA, USA, 2023; pp. 108–134. ISBN 9798369305935.
11. Alwi, S.; Salleh, M.M.; Abu, M.; Ismail, A.F.; Abbas, M.S.; Fadzilah, A.H.H. Concept of Integration of Blockchain and Artificial Intelligence. In Proceedings of the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 12–13 May 2023. [\[CrossRef\]](#)
12. Chithanuru, V.; Ramaiah, M. An Anomaly Detection on Blockchain Infrastructure Using Artificial Intelligence Techniques: Challenges and Future Directions—A Review. *Concurr. Comput.* **2023**, *35*, e7724. [\[CrossRef\]](#)
13. Soori, M.; Dastres, R.; Arezoo, B. AI-Powered Blockchain Technology in Industry 4.0, A Review. *J. Econ. Technol.* **2023**, *1*, 222–241. [\[CrossRef\]](#)
14. Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. *Big Data Cogn. Comput.* **2020**, *4*, 28. [\[CrossRef\]](#)
15. Ouyang, L.; Zhang, W.; Wang, F.-Y. Intelligent Contracts: Making Smart Contracts Smart for Blockchain Intelligence. *Comput. Electr. Eng.* **2022**, *104*, 108421. [\[CrossRef\]](#)
16. Gutierrez-Aguero, I.; Anguita, S.; Larrucea, X.; Gomez-Goiri, A.; Urquizu, B. Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum. *IEEE Access* **2021**, *9*, 108912–108923. [\[CrossRef\]](#)
17. Javed, I.T.; Alharbi, F.; Margaria, T.; Crespi, N.; Qureshi, K.N. PETchain: A Blockchain-Based Privacy Enhancing Technology. *IEEE Access* **2021**, *9*, 41129–41143. [\[CrossRef\]](#)
18. Lee, D.; Song, M. MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address. *IEEE Access* **2021**, *9*, 158122–158139. [\[CrossRef\]](#)
19. Omar, A.A.; Jamil, A.K.; Khandakar, A.; Uzzal, A.R.; Bosri, R.; Mansoor, N.; Rahman, M.S. A Transparent and Privacy-Preserving Healthcare Platform with Novel Smart Contract for Smart Cities. *IEEE Access* **2021**, *9*, 90738–90749. [\[CrossRef\]](#)
20. Qiu, Y.; Liu, Y.; Li, X.; Chen, J. A Novel Location Privacy-Preserving Approach Based on Blockchain. *Sensors* **2020**, *20*, 3519. [\[CrossRef\]](#)
21. Aldyafлах, I.M.; Zhao, W.; Upadhyay, H.; Lagos, L. The Design and Implementation of a Secure Datastore Based on Ethereum Smart Contract. *Appl. Sci.* **2023**, *13*, 5282. [\[CrossRef\]](#)
22. Elisa, N.; Yang, L.; Chao, F.; Naik, N.; Boongoen, T. A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity. *IEEE Access* **2023**, *11*, 8773–8789. [\[CrossRef\]](#)
23. Khor, J.H.; Sidorov, M.; Zulqarnain, S.A.B. Scalable Lightweight Protocol for Interoperable Public Blockchain-Based Supply Chain Ownership Management. *Sensors* **2023**, *23*, 3433. [\[CrossRef\]](#)
24. Ugochukwu, N.A.; Goyal, S.B.; Rajawat, A.S.; Verma, C.; Illés, Z. Enhancing Logistics with the Internet of Things: A Secured and Efficient Distribution and Storage Model Utilizing Blockchain Innovations and Interplanetary File System. *IEEE Access* **2024**, *12*, 4139–4152. [\[CrossRef\]](#)
25. Ullah, A.; Siddiquee, S.M.S.; Hossain, M.A.; Ray, S.K. An Ethereum Blockchain-Based Prototype for Data Security of Regulated Electricity Market. *Inventions* **2020**, *5*, 58. [\[CrossRef\]](#)
26. Viswanadham, Y.V.R.S.; Jayavel, K. A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology. *Electronics* **2023**, *12*, 1404. [\[CrossRef\]](#)
27. Yousra, B.; Yassine, S.; Yassine, M.; Said, S.; Lo'ai, T.; Salah, K. A Novel Secure and Privacy-Preserving Model for OpenID Connect Based on Blockchain. *IEEE Access* **2023**, *11*, 67660–67678. [\[CrossRef\]](#)
28. Stefanescu, D.; Montalvillo, L.; Galán-García, P.; Unzilla, J.; Urbieto, A. Industry 4.0 Business-Oriented Blockchain Design Decision Tree. In *Blockchain and Applications, 5th International Congress*; Springer Nature: Cham, Switzerland, 2023; pp. 113–123. ISBN 9783031451546.
29. Fu, M.; Zhang, C.; Hu, C.; Wu, T.; Dong, J.; Zhu, L. Achieving Verifiable Decision Tree Prediction on Hybrid Blockchains. *Entropy* **2023**, *25*, 1058. [\[CrossRef\]](#)
30. Salb, M.; Zivkovic, M.; Bacanin, N.; Chhabra, A.; Suresh, M. Support Vector Machine Performance Improvements for Cryptocurrency Value Forecasting by Enhanced Sine Cosine Algorithm. In *Computer Vision and Robotics*; Springer: Singapore, 2022; pp. 527–536. ISBN 9789811682247.
31. Monteiro, S.; Oliveira, D.; António, J.; Henriques, J.; Martins, P.; Wanzeller, C.; Caldeira, F. A Scalable Framework to Predict Bitcoin Price Using Support Vector Machine. In *Advances in Intelligent Systems and Computing*; Springer International Publishing: Cham, Switzerland, 2023; pp. 293–299. ISBN 9783031148583.
32. Inder, S.; Sharma, S. Predicting the Movement of Cryptocurrency “Bitcoin” Using Random Forest. In *Communications in Computer and Information Science*; Springer International Publishing: Cham, Switzerland, 2021; pp. 166–180. ISBN 9783030912437.
33. Ivaninskiy, I.; Ivashkovskaya, I. Are Blockchain-Based Digital Transformation and Ecosystem-Based Business Models Mutually Reinforcing? The Principal-Agent Conflict Perspective. *Eurasian Bus. Rev.* **2022**, *12*, 643–670. [\[CrossRef\]](#)
34. Lawrence, T.; Zhang, L. IoTNet: An Efficient and Accurate Convolutional Neural Network for IoT Devices. *Sensors* **2019**, *19*, 5541. [\[CrossRef\]](#)

35. Uppala, R.; Ramya, V.; Senthil, M.V. Develop a 7 Layers Convolution Neural Network and IoT-Based Garbage Classification System. *Int. J. Intell. Syst. Appl. Eng.* **2023**, *11*, 268–275.
36. Kim, S.-K.; Huh, J.-H. Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records. *Electronics* **2020**, *9*, 763. [[CrossRef](#)]
37. HaddadPajouh, H.; Dehghantanha, A.; Khayami, R.; Choo, K.-K.R. A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting. *Future Gener. Comput. Syst.* **2018**, *85*, 88–96. [[CrossRef](#)]
38. Alamro, H.; Marzouk, R.; Alruwais, N.; Negm, N.; Aljameel, S.S.; Khalid, M.; Hamza, M.A.; Alsaied, M.I. Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning. *IEEE Access* **2023**, *11*, 82199–82207. [[CrossRef](#)]
39. Arifeen, M.; Ghosh, T.; Islam, R.; Ashiquzzaman, A.; Yoon, J.; Kim, J. Autoencoder Based Consensus Mechanism for Blockchain-Enabled Industrial Internet of Things. *Internet Things* **2022**, *19*, 100575. [[CrossRef](#)]
40. Alaghbari, K.A.; Lim, H.-S.; Saad, M.H.M.; Yong, Y.S. Deep Autoencoder-Based Integrated Model for Anomaly Detection and Efficient Feature Extraction in IoT Networks. *IoT* **2023**, *4*, 345–365. [[CrossRef](#)]
41. Taher, S.S.H.; Ameen, S.Y.; Ahmed, J.A. Enhancing Blockchain Scalability with Snake Optimization Algorithm: A Novel Approach. *Front. Blockchain* **2024**, *7*. [[CrossRef](#)]
42. Singh, R.; Ujjwal, R.L. Hybridized Bio-Inspired Intrusion Detection System for Internet of Things. *Front. Big Data* **2023**, *6*, 1081466. [[CrossRef](#)]
43. Sangeeta, N.; Nam, S.Y. Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability. *Electronics* **2023**, *12*, 1545. [[CrossRef](#)]
44. Olanrewaju, R.F.; Khan, B.U.I.; Kiah, M.L.M.; Abdullah, N.A.; Goh, K.W. Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT. *Electronics* **2022**, *11*, 3982. [[CrossRef](#)]
45. Ethereum Ethereum/Go-Ethereum: Official GO Implementation of the Ethereum Protocol, GitHub. Available online: <https://github.com/ethereum/go-ethereum> (accessed on 3 February 2024).
46. Etherscan APIs-Ethereum (ETH) API Provider. Available online: <https://etherscan.io/apis> (accessed on 14 February 2024).
47. CIC IoT Dataset 2023. Available online: <https://www.unb.ca/cic/datasets/iotdataset-2023.html> (accessed on 8 February 2024).

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.