mathematics

MDPI

Article

Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques

Ajmeera Kiran [1], Prasad Mathivanan [2], Miroslav Mahdal [3,*], Kanduri Sairam [4], Deepak Chauhan [5,6] and Vamsidhar Talasila [7]

[1] Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad 500043, India; ajmeerakiran@mlrinstitutions.ac.in
[2] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India; prasad.m@vit.ac.in
[3] Department of Control Systems and Instrumentation, Faculty of Mechanical Engineering, VSB-Technical University of Ostrava, 17. Listopadu 2172/15, 70800 Ostrava, Czech Republic
[4] Department of Electronics and Communication Engineering, NITTE Deemed to Be University, Udupi 574110, India; drsairam@nitte.edu.in
[5] School of Computing, Graphic Era Hill University, Dehradun 248002, India; dchauhan@gehu.ac.in
[6] Graphic Era Deemed to Be University, Dehradun 248002, India
[7] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur 522502, India; talasila.vamsi@kluniversity.in
* Correspondence: miroslav.mahdal@vsb.cz

Abstract: The rapid proliferation of smart devices in Internet of Things (IoT) networks has amplified the security challenges associated with device communications. To address these challenges in 5G-enabled IoT networks, this paper proposes a multi-level blockchain security architecture that simplifies implementation while bolstering network security. The architecture leverages an adaptive clustering approach based on Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) for efficient organization of heterogeneous IoT networks. Cluster heads (CH) are selected to manage local authentication and permissions, reducing overhead and latency by minimizing communication distances between CHs and IoT devices. To implement network changes such as node addition, relocation, and deletion, the Network Efficient Whale Optimization (NEWO) algorithm is employed. A localized private blockchain structure facilitates communication between CHs and base stations, providing an authentication mechanism that enhances security and trustworthiness. Simulation results demonstrate the effectiveness of the proposed clustering algorithm compared to existing methodologies. Overall, the lightweight blockchain approach presented in this study strikes a superior balance between network latency and throughput when compared to conventional global blockchain systems. Further analysis of system under test (SUT) behavior was accomplished by running many benchmark rounds at varying transaction sending speeds. Maximum, median, and lowest transaction delays and throughput were measured by generating 1000 transactions for each benchmark. Transactions per second (TPS) rates varied between 20 and 500. Maximum delay rose when throughput reached 100 TPS, while minimum latency maintained a value below 1 s.

Keywords: blockchain; Internet of Things (IoT); Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS); Network Efficient Whale Optimization (NEWO); data security; clustering techniques

MSC: 90C27; 68T07

Citation: Kiran, A.; Mathivanan, P.; Mahdal, M.; Sairam, K.; Chauhan, D.; Talasila, V. Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques. *Mathematics* **2023**, *11*, 2073. https://doi.org/10.3390/math11092073

Academic Editors: Gang Hu, Lan Cheng and Guanqiu Qi

Received: 23 March 2023
Revised: 11 April 2023
Accepted: 25 April 2023
Published: 27 April 2023

1. Introduction

The Internet of Things (IoT) architecture can be employed to install pervasive, interconnected devices utilizing cloud platforms in a centralized network. The predicted heterogeneity of IoT network devices is yet constrained by factors including scalability, scarce resources, throughput, centralized control, overhead, and latency [1]. The devices are controlled and managed by the server using a centralized network architecture. Centralized systems, however, have several shortcomings [2]. When several smart devices are connected to a network, it is not uncommon for a great deal of data to be produced. A large amount of network bandwidth is required, as well as excellent effectiveness and memory, for a cloud software network operator. Additionally, there is always a chance that the failure of the critical components of the centralized network would result in a catastrophic (or total) failure of the system [3]. A third party is frequently needed to perform additional manipulation on the data that the central cloud storage has acquired. The privacy of the end user could be jeopardized as a result of data leaks. Coordination of external computer resources presents an additional difficulty in demonstrating IoT performance and security in centralized systems [4]. Because of this, the majority of centralized systems in use today are unable to provide organizations with a guarantee of confidentiality and security of data [5]. Most IoT devices can only transmit over limited distances due to their low-power wireless receivers and transmitters [6]. The Multihop Cellular Network (MCN) idea, which enables a large reduction in signal coverage, can be used to benefit IoT networks [7]. Creating a large-scale network with diverse nodes is more challenging since typical blockchain implementations require high-performance nodes [8]. The dispersed nature of IoT networks and the sheer volume of connected things mean that some kind of autonomous defense mechanism is also required [9].

The primary challenges in the new IoT era powered by 5G include an ever-increasing variety of devices that are connected, the heterogeneous nature of gadgets and automakers, interconnection, an enormous amount of gathered data and network traffic, the need for a great deal of bandwidth, communication latency, and trust. In most cases, their technical worth has been acknowledged. Unfortunately, at the moment, they simply provide the ability to store transactional data. To address difficulties with complexity and expand the approach for securing IoT connections, this research analyzes a multi-level structure according to a special clustering method appropriate for the blockchain system. To accommodate blockchain integration in IoT systems, a modified clustering technique was developed by factoring in network performance measurements in predetermined cost functions [10,11]. This means that hacked nodes cannot insert invalid blocks onto the public ledger without being discovered. Hence, the multi-level blockchain prevents compromised entities from accessing it. Hence, the validity of data stored on a blockchain cannot be disputed [12]. Furthermore, crucial is the fact that the new multi-level architecture makes it possible to update the existing primary cloud server. This allows for widespread rollouts to become a reality. In addition, smart contracts guarantee that only authorized users have access to network resources by implementing a lightweight authorization and authentication method that operates locally inside each cluster [13].

Several systems for maintaining security and privacy have been created using tools like public key infrastructure, blockchains, smart cards, and passwords. Although some of these protocols are too sophisticated to be used with IoT devices, many of them have severe privacy and security flaws. This study suggests numerous contributions to overcome these problems.

- First, we present a novel method for direct, non-centralized authentication of communicating entities using biometrics and elliptic curve cryptography. By doing this, any possible single-point of failure problems are resolved;
- In order to prevent user cooperation and privileged insider assaults, we also design an authorization framework employing security tokens for access and membership validation as well as admittance rights groups;
- Additionally, we do formal security analysis utilizing the well-known BAN logic, which verifies the existence of a session key between interacting entities. To show that the suggested system is secure under all of the threat model assumptions, informal security analysis is also carried out;

- To show how effective the suggested protocol is, we conducted a comparative performance study. The results reveal that it has the fewest computing and communication difficulties when compared to other protocols.

The rest of the paper is organized as follows: Section 2 describes the literature review; Section 3 provides the proposed methodology; Section 4 details the result and discussion; and Section 5 illustrates the conclusion.

2. Literature Review

The study [14] suggests a different strategy for building trust in supply chains that contain a variety of IoT components. By employing simulations, we assess the proposed model and demonstrate its applicability. The goal of the research [15] was to investigate the use of blockchain technology to protect a loT-enabled WBMS's communication and data against harmful cyberattacks [16]. Experimental experiments provide proof of concept for the proposed blockchain-based IoT network for WBMSs. The cloud storage option for sensors is taken into consideration in the paper [17]. A unique group signature system that has minimal computational and communication costs is created to first establish anonymous authentication and then provide secure and effective data storage and sharing. Then, based on the suggested group signature scheme, a unique blockchain-based cloud storage protocol for sensors in the IIoT is built. This protocol makes use of smart contracts and proxy re-encryption to enable safe data transfer with minimal computational overhead [18]. The intent of this research [19] was to suggest Edge Share, a blockchain-based data-sharing structure for edge data-sharing offerings across heterogeneous network contexts. This is achieved by implementing a two-level overlay network architecture and an edge computing concept, which can substantially alleviate scheme stress and decrease transmission delay to improve information effectiveness. The suggested framework [20] has been carefully evaluated against several security criteria in comparison to conventional mechanisms. With the use of a multi-level authorization hub and a hierarchical attribute structure, the paper [21] suggests a novel attribute-based encryption method. By spreading different user attributes to distinct authorization centers, the technique enables flexible and fine-grained access control. It was then integrated with the Fabric blockchain technology to address the issue of high decryption costs for Internet of Things consumers [22]. To reduce consumers' decryption overhead, smart contracts on blockchain use high-complexity partial decryption algorithms. These methods use a blockchain-based dynamic secret-sharing mechanism. The power blockchain sharing approach, which can additionally share power trading books, is used to create a dependable trading center. The power data consensus technique and dynamically linked memory are intended to enable secure power data transport matching [23]. Secure SVM, a privacy-preserving SVM training scheme over blockchain-based encrypted IoT data, was used in this study [24]. Blockchain technology creates a secure and dependable data-sharing platform for numerous data sources, in which IoT data is encrypted and then stored on a distributed ledger [25]. The study [26] offers a unique Decentralized Blockchain-based Security (DeBlock-Sec) solution to address the security challenge in resource-constrained IoT environments. The limitation of the proposed model is the decentralized nature of blockchain can make it difficult to manage and update security protocols across a large number of devices. Finally, the integration of blockchain with existing IoT networks and protocols may require significant changes to the underlying infrastructure, which can be costly and time-consuming.

Motivation of the Research

In order to improve message relay between devices, many are turning to 5G networks as the demand for higher quality of service (QoS) and security in IoT networks develops. However, there are difficulties specific to this adoption. High-capacity 5G networks also enable extensive private data exchanges between 5G-IoT devices. In the event that malevolent actors compromised this data, serious consequences could result.

Furthermore, devices typically need to authenticate themselves during handovers in order to stop assaults due to the ultra-densification of base stations in 5G networks. Conventional security mechanisms, however, with their high processing, communication, and storage needs, are not appropriate for this context due to the resource-constrained nature of IoT devices.

In 5G-IoT networks, device heterogeneity poses additional difficulties because different device architectures for communication and security may exist. More effective key exchange and authentication techniques are required in order to guarantee the highest levels of security and privacy protection while preserving the best QoS. Overall, it is important but challenging to strike a balance between security, privacy, and QoS in 5G-IoT networks.

3. Proposed Methodology

The proposed network architecture is meant to make use of the cellular systems' capabilities and performance while providing an efficient and reliable security feature for IoT networks. To encrypt the multi-level structure, Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) is used. This research offers a framework to make it easier for IoT networked devices (objects and nodes) to be authenticated and authorized in a lightweight manner using blockchain technology. The entire cellular-enabled IoT network is divided into several levels by the suggested multi-level network paradigm. IoT nodes and diverse clusters make up Level 1. Sink nodes and controlling elements like cluster heads are included in level 2. Cellular network base stations are located at Level 3. The decentralized blockchain mechanism can be implemented at Level 3 by the BSs with the necessary servers and CPUs. The total system model is depicted in Figure 1.

The introduction of blockchain technology may result in more work and scalability problems. Figure 2 depicts the multi-level network concept that may be used to cut down on redundancy, speed up responses, better organize data, keep conversations private, and accommodate future growth.

Several modules and nodes with varying computational and resource needs are found on the first level. For the IoT system's regional authorization program, the cluster heads offer authentication and authorization functions for regionally embedded systems. In a blockchain setting, CH nodes may safely connect because of a thin consensus. On this level, the permission-based local HLF blockchain is implemented. Cellular network BSs make up the top level. At this level, reliable asymmetric cryptography method deployment is possible. The use of the global system and cutting-edge security measures at the highest levels ensures privacy and security (Level 3).

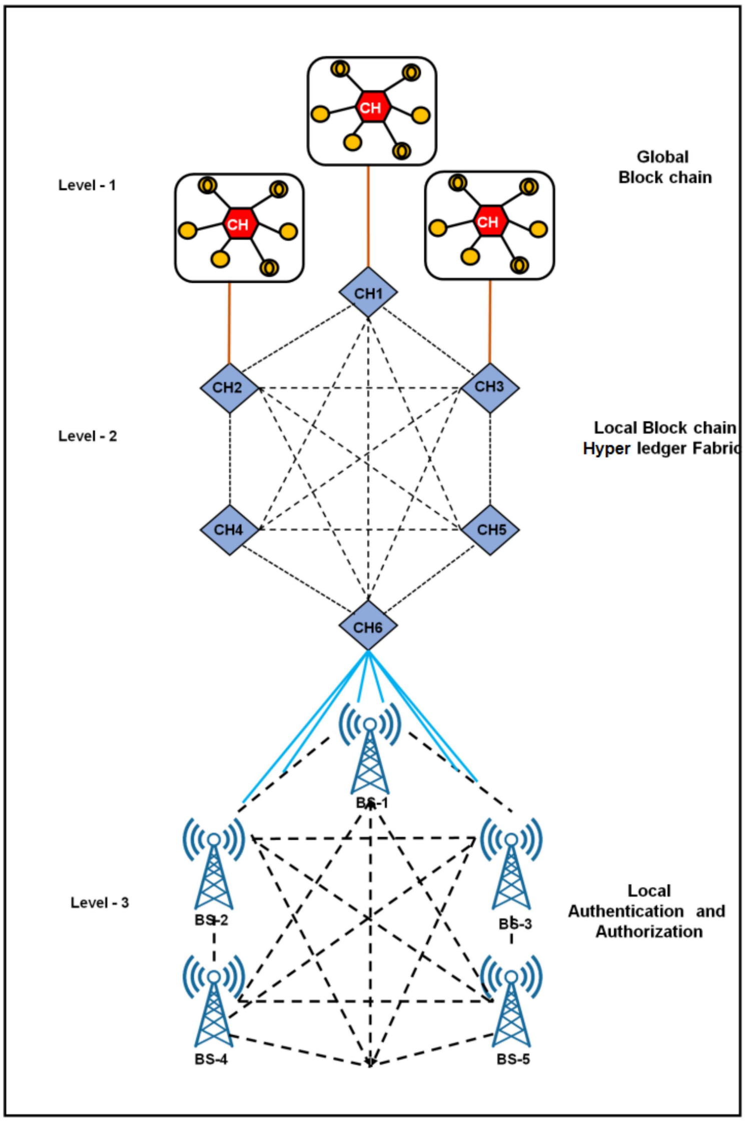

Figure 1. IoT network multi-level model.

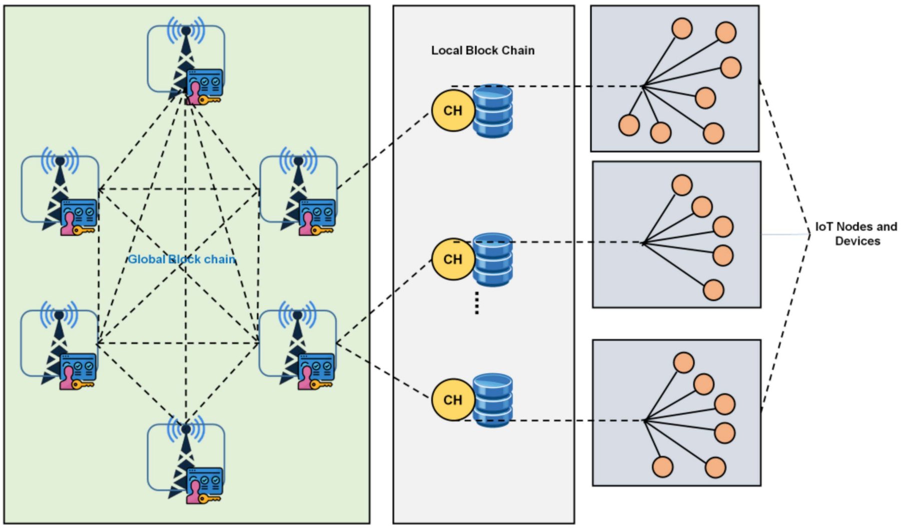

Figure 2. The network concept has three levels: an infrastructure level with a local authorization service, a local blockchain, and a public chain.

3.1. Implementation of the Framework

3.1.1. Network Self-Clustering

The foundation of metaheuristic algorithms is the intimate relationship between computational techniques and optimization. These techniques' main benefit is their freedom from local optimum spots. As a result, these methods search everywhere in the search space. Additionally, the metaheuristic algorithms' entire distribution of individual control (network nodes and participants). Localized communication is how these people interact with one another. The system responds strongly, and the application is quick to adapt to environmental changes. The IoT network's clustering strategy is seen in Figure 3.

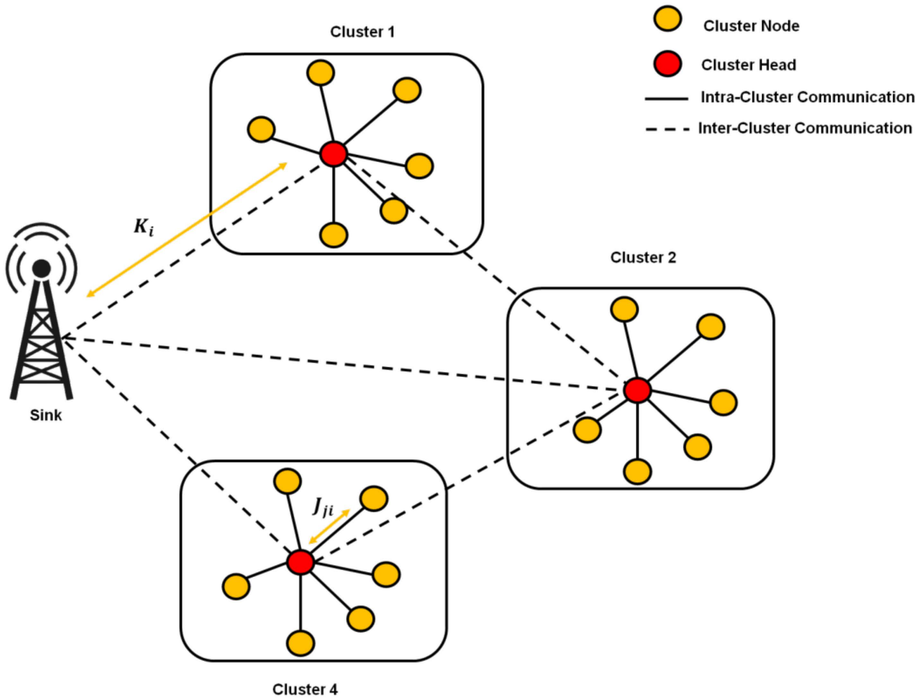

Figure 3. Scheme for cellular IoT network clustering.

Therefore, Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) is presented herein for the clustering of heterogeneous IoT networks. In this study, NEWO is used to improve the clustering of the proposed IoT network since it shows extremely strong performance in this regard. By reducing the average distance that data must travel between IoT devices and the selected cluster heads, the clustering method helps keep IoT systems as efficient as possible. By grouping, just a fraction of the nodes will need to make far-reaching connections to the Base Station (BS). As a result, the system's overall energy usage drops while the network's reach expands. By streamlining the deployment process, the clustering-based method improves the effectiveness of blockchain applications. The CH nodes are in charge of organizing the whole network into functionally independent clusters. To exchange information, other nodes in the cluster have to talk to the CH nodes. Clustering is the goal, and the idea is to get there by using evolutionary computing techniques to run on the network itself. This is done to simulate the disparate components that make up the IoT infrastructure. There is no hard-and-fast rule for how many clusters there should be or how many nodes there should be in each cluster. Moreover, the suggested clustering improves the adaptability of the IoT network's node placement. Taking into account the fact that nodes aren't evenly dispersed within clusters is a major factor.

3.1.2. CH Selection with Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS)

Satisfying energy restrictions is the most important aspect of the IoT network architecture. To extend network operation, communications, and transmission links can be made shorter, and power consumption can be decreased. By arranging nodes into autonomous clusters, shorter communication linkages can be achieved. Due to the necessity of each cluster member exchanging information with the associated CH, such an approach makes data aggregation and forwarding easier. EASISS is used in our suggested paradigm to represent vector data. The placements of the sparrow are determined at random inside the limits and are shown in a linear system in the form of Equation (1). Rand [0, 1], a randomly generated distribution number, makes up the beginning vector. For the optimization problem, each row represents a fitness function solution.

$$f(x) = \begin{bmatrix} f(SP_{1,1}, & SP_{1,2} & \cdots & SP_{1,d}) \\ f([SP_{2,1} & SP_{2,2} & \cdots & SP_{2,d}]) \\ \vdots & \vdots & \vdots & \vdots \\ f([SP_{n,1} & SP_{n,2} & \cdots & SP_{n(k),d}\Big]\Big) \end{bmatrix} \begin{bmatrix} f_{obj_1} \\ f_{obj_2} \\ \vdots \\ f_{obj_n} \end{bmatrix} \tag{1}$$

The mutation operator uses the Mutation Rate (MR) to help choose the best vector TaV from the population. The new progeny is displayed in Equation (2). The likelihood that $SP_{(g+1)}$ would produce two unique vectors is random, and it is also modified according to three random values. The vectors $\in [0, 1]$ differences in the mutation operation $r_1, r_2,$ and r_3 may be the conscious cause of the resultant's unfavorable outcome. Because of this, the method has to generate the difference in the vector's components in a manner that satisfies the range. Every single sparrow goes through a population-wide evolution of every single process until the optimal solution is identified.

$$SP_{g+1} = SP_{r1} + MR * (SP_{r_2} - SP_{r_3}) \tag{2}$$

Equation (3) calculates the Euclidean distance between the best-chosen sparrow and each sparrow.

$$dist = \sqrt{\sum_{i=1}^{N} \left(SP_{i.j} - SPbest_{i,j}\right)^2} \tag{3}$$

Similar to Equation (4) and undergoes recombination to create a new generation of children is known as $DV\ TaV$ a trial vector. In this case, a preset Crossover Probability Rate (CPR) is employed with binomial cross-over. If ($r \leq CPR\ BestDV$), the donor vector is chosen; if not, the target vector is.

$$SP_{i,j,g+1} = \left\{ \begin{array}{c} BestDV_j\ if\ (r \leq CPR) \\ BestTaV_j\ if\ (r > CPR) \end{array} \right\} \tag{4}$$

When $AV < ST$ indicates that there are no predators, producers move into a wider search mode, as shown in Equation (5). When the $AV \geq ST$ predator is present, which is rare, sparrows must defend themselves by fleeing to safer areas. Only infrequent scavengers follow producers significantly.

$$SP_{i,j}^{(t+1)} = \begin{cases} SP_{i,j}^{t}.\exp\left(\frac{-1}{a.I_{max}}\right) & if\ AV < ST \\ SPTV_{i,j}^{t} + Q.L & if\ AV \geq ST \end{cases} \tag{5}$$

For a fixed number of iterations, the location of the scavenger may be found in Equation (6), where I max β mean is the variable step controlling the parameter's average value and variation is 1. Algorithm 1 is EASISS. The equation combines the current position of the particle with the difference between the global best and personal best positions, scaled by β. The goal is to update the particle's position towards the global best position, while taking into account its own personal best position. This helps the particle swarm algorithm to explore the search space efficiently and converge to a good solution.

$$SP_{i,j}^{(t+1)} = SP_{GBest}^{t} + \beta \cdot \left[SP_{i,j}^{t} - SP_{GBest}^{t} \right]^{(t+1)} \tag{6}$$

Algorithm 1: EASISS

```
Create nodes at random in 2D space,
Initialize population $G$ at random
Evaluate each (node) sparrow's objective function
While (not utilizing the most iteration)
  Use every node $i$ in a cluster $k$
  Do with $i = 1$ to $N$ nodes
      Choose three nodes at random from the population
      Use the Euclidean distance to calculate the distance between nodes
      Observe the mutant sparrow population
      Produce a new population
      Perform the recombination process
      If ($r < CPR$) then
          Do a selection operation
      Else
          Optimal fitness should replace the sparrow population G.
          For each sparrow, reevaluate the objective function.
          Update the population's $SP_{best}$ position and chose as $CH$
      End
      $t = t + 1$
  End Do
Stop while
Return Best solution
```

3.1.3. Network Changes Optimization Using Network Efficient Whale Optimization (NEWO)

The network modifications, such as node creation, movement into, and removal from the IoT network, are carried out using the meta-heuristic algorithm NEWO. NEWO is mathematically designed to encircle prey, assault with a bubble net, and seek prey, which is quite similar to the Whale Optimization Algorithm in terms of feeding behavior. The following steps are taken to adopt NEWO, as well as initializing the whale's population:

$$X = \begin{bmatrix} X_1 \\ X_2 \\ \cdots \\ X_3 \end{bmatrix} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,d} \\ x_{2,1} & \cdots & x_{2,d} \\ \vdots & \cdots & \vdots \\ x_{n,1} & \cdots & x_{n,d} \end{bmatrix} \tag{7}$$

where n is the number of whales and d is the dimension. Calculating and assessing the whale population's fitness value. There will be at least two fitness values for each whale to consider depending on the issue. This evaluation is formulated as follows for problems with two objectives, such as F_1 and F_2:

$$FX = \begin{bmatrix} F_1(X_1) & F_2(X_1) \\ F_1(X_2) & F_2(X_2) \\ \vdots & \vdots \\ F_1(X_n) & F_2(X_n) \end{bmatrix} \tag{8}$$

The search agent's initial spawn location is chosen at random, and when it does, the nearby node's information is cloned to that node's position. Calculating each search agent's fitness value and selecting the best for reference are the following steps. Afterward, NEWO's parameters are modified so that further search agents are generated based on the position of the best agent. A fitness function is used to determine which cluster head should be used. This function is essential to the exploring mechanism of NEWO (search for prey). The characteristics of the node, such as its energy level (Er) and the density of nodes nearby are the function's determining factors.

$$f(CH_i) = p_1[N(CH_i)] + p_2\sum(CH_E) \tag{9}$$

In Equation (9), the variables p_1 and p_2 are chosen at random between 0 and 1, and the variable (CH_i) is a list of all the nodes that are close to the CH. CH_i and CH_E are the remaining energies of the neighboring nodes. In this case, a node needs to have a lot of neighbors nearby in addition to enough remaining energy to become the CH; hence, the higher the fitness value, the better the solution. The base station transmits the cluster heads' IDs throughout the network after determining the best arrangement of cluster heads and the nodes they belong to. Each of these cluster heads transforms into a command center for its area, in charge of gathering and transmitting information. Algorithm 2 provides the pseudocode for the proposed approach.

Algorithm 2: NEWO

```
while ($r < r_{max}$)
  while ($t < t_{max}$)
     For every search agent's $CH_i$
        Clone the $CH_i$ node closest to it
        Calculate fitness
        Compute the coefficient vectors
        Select the whale's location
        Adjust the $X^*$ best position if $X$ is greater than $X^*$
        For all search agents, update the fitness function.
     End for
  End while
$CH$ = nearest node to the $X^*$ position
End while
```

4. Result and Discussion

An IoT network simulation was carried out to test the effectiveness of the proposed clustering techniques. In a 2-D network, there are 100 randomly chosen nodes. Since MATLAB 2018a provided a trustworthy environment for clustering algorithms and made it simple to simulate techniques, it was chosen so that the final results could be compared.

4.1. Clustering Results

To test the efficiency of the suggested clustering approach, it was compared to four other algorithms already reported in the literature: the cascading model [27], Low Energy Adaptive Clustering Hierarchy (LEACH) [28], Gateway Clustering Energy-Efficient Centroid (GCEEC) [29], and Black Hole and Ant Colony Optimization (BH-ACA) [30]. The same simulated network architecture was used to assess each protocol. The number of clusters and CHs produced by each method after its optimization varied. The simulation outcomes show that the proposed clustering model is effective and that the algorithm for minimizing distances and overall network energy is also effective. By reducing network load, decreasing distance, and increasing network coverage, as shown in Figures 4–6, the suggested EASISS-NEWO outperforms the existing algorithms.

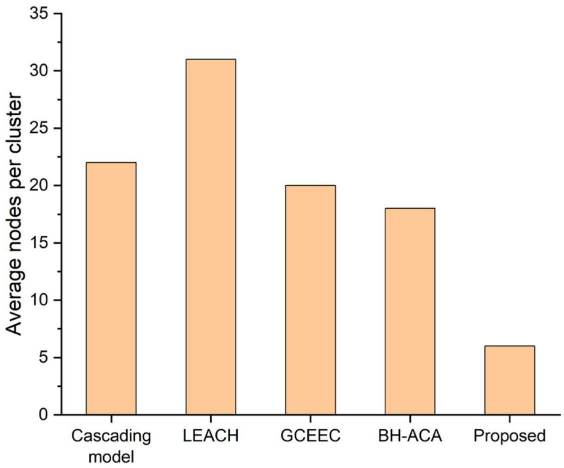

Figure 4. Comparison of average nodes per cluster of the proposed model with cascading model [27], LEACH [28], GCEEC [29], and BH-ACA [30].

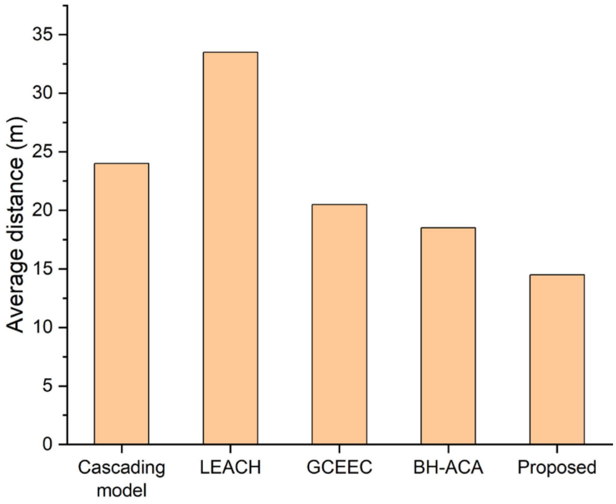

Figure 5. Comparison of average distance of the proposed model with cascading model [27], LEACH [28], GCEEC [29], and BH-ACA [30].

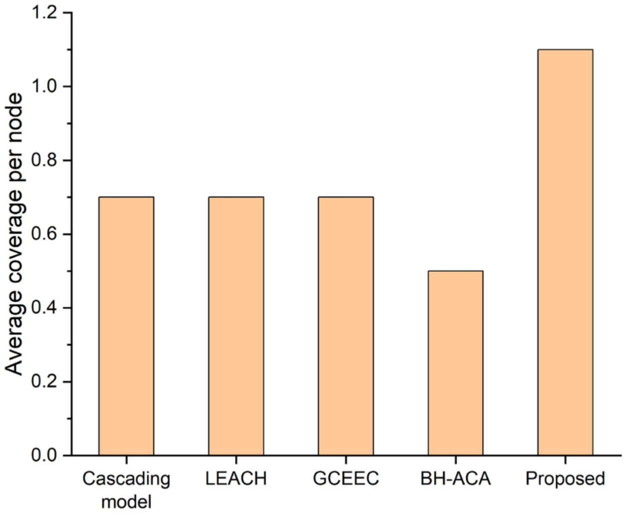

Figure 6. Comparison of average coverage per node of the proposed model with cascading model [27], LEACH [28], GCEEC [29], and BH-ACA [30].

As the blockchain applications' BS server, a workstation was used to build the Level-3 simulation model. Ethereum and Hyperledger private networks' throughput and latency characteristics might be easily assessed in this environment. All of the networks had the same physical infrastructure and were given the same virtual workload. For the experiment, it was planned to use a distributed ecosystem that would incorporate the aforementioned two blockchain networks. The basis for the simulation models was a workstation with an Intel Core i7-3770 processor running at 3.4 GHz and 16 GB of RAM. For simplicity, just one mining node was used to start the Ethereum network.

4.2. Performance Evaluation

A blockchain application's principal goal is to keep track of the many transactions that its users have submitted. A block is generated, and the transaction outcome is stored on the blockchain ledger as a result of the submitted transactions' subsequent processing through the verification and ordering procedures. The latency and throughput of the system were measured to evaluate the effectiveness of the proposed model. To demonstrate the value of the proposed framework, the results were compared to the parameters established in the literature. Hyperledger Caliper was used throughout the study to allow for the administrator's unique blockchain setup. Both node and network latency are significantly influenced by block size. The system's latency is determined by how long it takes to gain consensus when a node begins to notice fresh block validations. Several transactions, including Open, Transfer, and Query, were used to analyze the system. Results were reported for Ethereum and Hyperledger Fabric (level 2 suggested blockchain). Table 1 shows the performance of Hyperledger and Ethereum.

Table 1. Performance of Hyperledger and Ethereum.

Name	**Send Rate (TPS)**		**Max Latency (s)**		**Min Latency (s)**		**Avg Latency (s)**		**Throughput (TPS)**	
Blockchain	E	H	E	H	E	H	E	H	E	H
Transfer	10.7	10	7.13	0.38	2.07	0.06	4.63	0.19	6.7	10
Open	22.7	20.2	7.05	0.38	2.12	0.04	4.58	0.18	10	20.1
Query	10.2	10	0.02	0.07	0.01	0.01	0.01	0.01	10.2	10

E—Ethereum; H—Hyperledger Fabric.

By using a multi-level architecture, the average latency is reduced. Only some of the nodes (i.e., CHs) in this architecture contribute to the validation of new blocks. The outcomes of the Ethereum implementation are also shown in Table 1. As a worldwide blockchain technology, it is clear that the proposed lightweight HLF blockchain outperforms Ethereum.

When choosing a suitable blockchain platform for IoT applications, latency and throughput are crucial performance parameters, along with security and privacy. The latency goals can only be met if the blockchain network's distribution of resources is optimized for a given input load. Further analysis of System under Test (SUT) behavior was accomplished by running many benchmark rounds at varying transaction sending speeds. Maximum, median, and lowest transaction delays and throughput were measured by generating 1000 transactions for each benchmark. Transactions per second (TPS) rates varied between 20 and 500. In Figure 7, we can see the highest, median, and lowest transaction latencies that occurred throughout our experiment's many runs. Maximum delay rose when throughput reached 100 TPS, while minimum latency maintained a value below 1 s. The transaction throughput results for different transaction sending rates are shown in Figure 8.

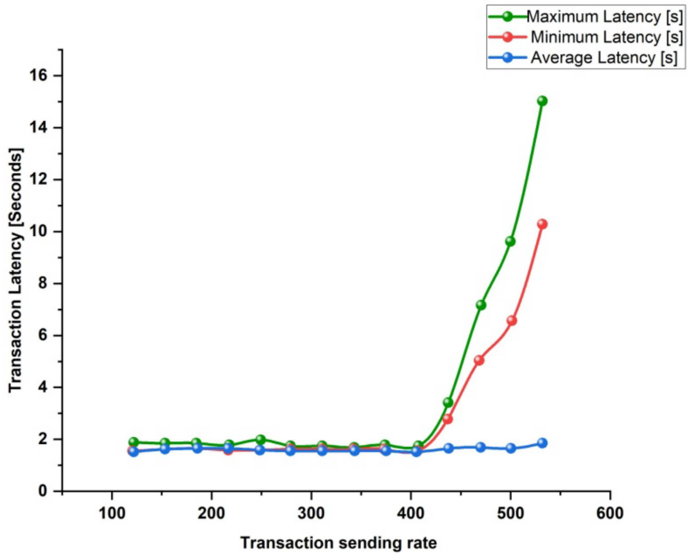

Figure 7. Latency vs. transaction sending rate.

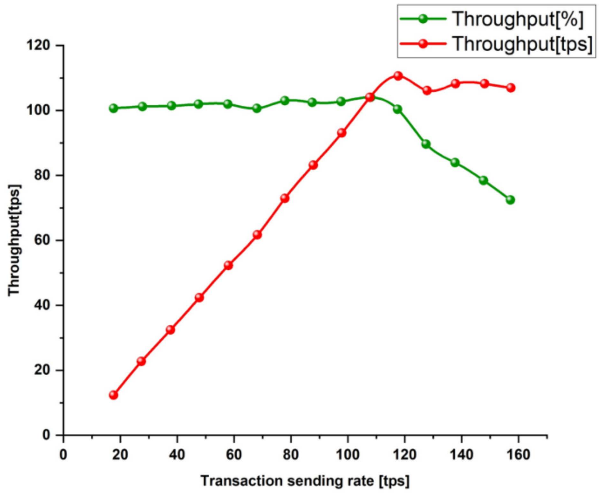

Figure 8. Throughput vs. transaction sending rate.

The throughput was consistent at roughly 100%, even though the sending rate peaked at 110 transactions per second. When the sending rate was raised to 110 TPS, the maximum acceptable sending rate for the SUT, a drastic decrease in throughput was noticed. For the sake of this experiment, every blockchain transaction was produced by a separate client. The HLF has a new three-step design called execute-order-validate, where each stage is dependent on the results of previous stages. As the real throughput is very close to 100%, a 100 TPS transmission rate is doable. Yet, there is only a marginal reduction in throughput when sending at 100 and 200 TPS. We calculated that this means our infrastructure can handle sending at a pace of roughly 110 TPS. Hence, our proposed architecture might allow for the real-time provisioning of a wide variety of 5G-enabled IoT applications with little additional delay. The maximum delay approaches 15 s as the number of input transactions rises. Because of limitations imposed by the containers' allocation to peer nodes, this is the scenario. Since the peer nodes are not initially subjected to heavy loads, the minimum latency almost always remains constant. The block size, channel count, ordering service, users, and endorsing nodes are just a few examples of how blockchain configuration can affect latency. It is evident that, in each case, every transaction is completed, i.e., no transaction loss takes place.

5. Conclusions

This research proposes a distributed security model for IoT devices communicating through cellular networks with multiple hops, using a blockchain-based approach with a multi-level architecture. The IoT network is divided into clusters using the self-clustering EC method, designed with the EASISS-NEWO technique to increase network lifespan and security and reduce processing burden, network load, and latency. The proposed solution addresses issues related to IoT security, such as framework privacy, authentication, heterogeneity, flexibility, and scalability. Four existing methods were compared with the suggested clustering method through simulation studies, and the proposed technique outperformed the alternatives in terms of network load, coverage, and distance. The proposed multi-level system was evaluated, and the results indicated the lightweight blockchain was preferable over Ethereum's global network. Future studies will focus on building a realistic, scalable testbed to investigate, assess, and compare the performance of IoT devices in a real-world environment. Blockchain technology is known to be energy-intensive, which can be a significant issue for IoT systems that rely on battery-powered devices. Future research could explore ways to optimize blockchain solutions for energy efficiency, such as by using lightweight consensus algorithms or off-chain processing.

Author Contributions: A.K.—Conceptualization, methodology, formal analysis, investigation, writing—original draft; P.M.—Conceptualization, methodology, formal analysis, investigation, writing—original draft; M.M.—Conceptualization, methodology, resources, writing—review and editing; K.S.—Conceptualization, formal analysis, investigation, writing—original draft; D.C.—methodology, validation, writing—original draft; V.T.—methodology, validation, writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the project SP2023/074 Application of Machine and Process Control Advanced Methods supported by the Ministry of Education, Youth and Sports, Czech Republic.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available through email upon request to the corresponding author.

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

References

1. Pal, K. Privacy, security, and policies: A review of problems and solutions with blockchain-based internet of things applications in manufacturing industry. *Procedia Comput. Sci.* **2021**, *191*, 176–183. [CrossRef]
2. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [CrossRef]
3. Gong, S.; Tcydenova, E.; Jo, J.; Lee, Y.; Park, J.H. Blockchain-based secure device management framework for an internet of things network in a smart city. *Sustainability* **2019**, *11*, 3889. [CrossRef]
4. Firoozjaei, M.D.; Lu, R.; Ghorbani, A.A. An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Secur. Priv.* **2020**, *3*, e131. [CrossRef]
5. Lv, Z.; Qiao, L.; Li, J.; Song, H. Deep-learning-enabled security issues in the internet of things. *IEEE Internet Things J.* **2021**, *8*, 9531–9538. [CrossRef]
6. Yu, K.; Tan, L.; Yang, C.; Choo, K.-K.R.; Bashir, A.K.; Rodrigues, J.J.P.C.; Sato, T. A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings. *IEEE Internet Things J.* **2021**, *9*, 8154–8167. [CrossRef]
7. Ali, G.; Ahmad, N.; Cao, Y.; Asif, M.; Cruickshank, H.; Ali, Q.E. Blockchain based permission delegation and access control in Internet of Things (BACI). *Comput. Secur.* **2019**, *86*, 318–334. [CrossRef]
8. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhao, P.; Liu, S. A survey of blockchain and intelligent networking for the metaverse. *IEEE Internet Things J.* **2023**, *10*, 3587–3610. [CrossRef]
9. Yang, X.; Yang, X.; Yi, X.; Khalil, I.; Zhou, X.; He, D.; Huang, X.; Nepal, S. Blockchain-based secure and lightweight authentication for Internet of Things. *IEEE Internet Things J.* **2021**, *9*, 3321–3332. [CrossRef]
10. Lv, Z.; Qiao, L.; Hossain, M.S.; Choi, B.J. Analysis of using blockchain to protect the privacy of drone big data. *IEEE Netw.* **2021**, *35*, 44–49. [CrossRef]

11. Wang, S.; Sheng, H.; Zhang, Y.; Yang, D.; Shen, J.; Chen, R. Blockchain-empowered distributed multi-camera multi-target tracking in edge computing. In *IEEE Transactions on Industrial Informatics*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–10.
12. Yan, L.; Yin-He, S.; Qian, Y.; Zhi-Yu, S.; Chun-Zi, W.; Zi-Yun, L. Method of reaching consensus on probability of food safety based on the integration of finite credible data on block chain. *IEEE Access* **2021**, *9*, 123764–123776. [CrossRef]
13. Almakhour, M.; Sliman, L.; Samhat, A.E.; Mellouk, A. Verification of smart contracts: A survey. *Pervasive Mob. Comput.* **2020**, *67*, 101227. [CrossRef]
14. Al-Rakhami, M.S.; Al-Mashari, M. A blockchain-based trust model for the internet of things supply chain management. *Sensors* **2021**, *21*, 1759. [CrossRef]
15. Faika, T.; Kim, T.; Ochoa, J.; Khan, M.M.; Park, S.-W.; Leung, V.C.M. A blockchain-based Internet of Things (IoT) network for security-enhanced wireless battery management systems. In Proceedings of the 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 29 September–3 October 2019.
16. Li, B.; Zhou, X.; Ning, Z.; Guan, X.; Yiu, K.-F.C. Dynamic event-triggered security control for networked control systems with cyber-attacks: A model predictive control approach. *Inf. Sci.* **2022**, *612*, 384–398. [CrossRef]
17. Lu, J.; Shen, J.; Vijayakumar, P.; Gupta, B.B. Blockchain-based secure data storage protocol for sensors in the industrial internet of things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 5422–5431. [CrossRef]
18. Krichen, M.; Lahami, M.; Al-Haija, Q.A. Formal methods for the verification of smart contracts: A review. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022.
19. Yang, L.; Zou, W.; Wang, J.; Tang, Z. EdgeShare: A blockchain-based edge data-sharing framework for Industrial Internet of Things. *Neurocomputing* **2022**, *485*, 219–232. [CrossRef]
20. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [CrossRef]
21. Xu, H.; He, Q.; Li, X.; Jiang, B.; Qin, K. BDSS-FA: A blockchain-based data security sharing platform with fine-grained access control. *IEEE Access* **2020**, *8*, 87552–87561. [CrossRef]
22. Cao, K.; Ding, H.; Wang, B.; Lv, L.; Tian, J.; Wei, Q.; Gong, F. Enhancing physical-layer security for IoT with nonorthogonal multiple access assisted semi-grant-free transmission. *IEEE Internet Things J.* **2022**, *9*, 24669–24681. [CrossRef]
23. Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K.C. A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3582–3592. [CrossRef]
24. Shen, M.; Tang, X.; Zhu, L.; Du, X.; Guizani, M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet Things J.* **2019**, *6*, 7702–7712. [CrossRef]
25. Lekssays, A.; Landa, L.; Carminati, B.; Ferrari, E. PAutoBotCatcher: A blockchain-based privacy-preserving botnet detector for Internet of Things. *Comput. Netw.* **2021**, *200*, 108512. [CrossRef]
26. Narayanan, U.; Paul, V.; Joseph, S. Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *13*, 769–787. [CrossRef]
27. Fu, X.; Yao, H.; Yang, Y. Modeling and analyzing cascading dynamics of the clustered wireless sensor network. *Reliab. Eng. Syst. Saf.* **2019**, *186*, 1–10. [CrossRef]
28. Safaa, S.S.; Mabrouk, T.F.; Tarabishi, R.A. An improved energy-efficient head election protocol for clustering techniques of wireless sensor network (June 2020). *Egypt. Inform. J.* **2021**, *22*, 439–445.
29. Qureshi, K.N.; Bashir, M.U.; Lloret, J.; Leon, A. Optimized cluster-based dynamic energy-aware routing protocol for wireless sensor networks in agriculture precision. *J. Sens.* **2020**, *2020*, 1–19. [CrossRef]
30. Sefati, S.; Abdi, M.; Ghaffari, A. Cluster-based data transmission scheme in wireless sensor networks using black hole and ant colony algorithms. *Int. J. Commun. Syst.* **2021**, *34*, e4768. [CrossRef]

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.