A ES

ISSN: 2096-3246
Volume 58, Issue 01, 2026

Zero-Knowledge Data-Assisted Elusive Adversary Interface for Mitigating Large-Scale Attacks in Blockchain Networks

M Vijay Bhasker Reddy [1,2], Dr. Soujanya Duvvi[3]

1.Research Scholar, Dept. of CSE, GITAM University, Vizag.
2. Sr. Assistant Professor, Dept. of CSE, Geethanjali College of Engineering and Technology
muppuvijay@gmail.com, ORCID: 0000-0002-2940-7424
3. Assistant Professor, Dept. of CSE, GITAM University, Vizag.
sduvvi3@gitam.edu, ORCID: 0000-0003-4649-3093

Abstract: Present industry increasing adoption of blockchain technology, blockchain networks have become prime targets for attackers seeking to exploit vulnerabilities in the deployments. To address this challenge, this paper proposes a novel Zero-Knowledge Data-Assisted Elusive Adversary Interface (ZKD-EAI) designed to mitigate large-scale data collection attacks in blockchain ecosystems. The proposed interface integrates Zero-Knowledge Data (ZKD) mechanisms with intelligent deception techniques to safeguard blockchain networks against adversarial reconnaissance and data extraction attempts. By employing zero-knowledge proof (ZKP) principles, the interface ensures that no sensitive information is disclosed during validation or verification, while simultaneously deploying fake yet plausible data responses to mislead attackers. This dual-layer design enhances privacy, integrity, and deception-based defence within blockchain operations. The ZKD-EAI framework is highly adaptive and modular, supporting seamless integration with existing blockchain infrastructures without significant architectural reconfiguration. Experimental evaluations were conducted on a simulated blockchain network incorporating intelligent honeypots, demonstrating that the proposed system effectively 97.8 % reduces data leakage, increases adversary confusion, and strengthens resilience under various attack conditions.

Keywords: Blockchain, Attacks, Adversary, Collection, Multimodal, Representation, Accuracy, Analysis.

1. Introduction

The application of blockchain technology has quickly become a game-changer in the realm of digital finance as well as other industries. It provides a decentralized and tamper-proof platform for secure transactions and data storage, which makes it an attractive option for a wide variety of applications [1, 2, 3]. However, due to their ever-increasing popularity, blockchain networks have become a prime target for cybercriminals and other malicious actors who are looking to exploit vulnerabilities in the underlying systems [4, 5, 6]. Data collection, which can be used to gain insight into the behaviour of networks and identify potential targets for attacks [7, 8, 9], is one of the primary methods that attackers use to carry out their attacks.

The issue of data collection within blockchain networks has received a significant amount of attention from the academic community, which has led to the development of a number of potential solutions to the problem. On the other hand, the majority of these strategies have a number of drawbacks, the most common of which are inflexibility, inability to scale, and insufficient safety. Traditional methods of

mitigating the risk of data collection typically rely on passive or static methods, which are simple for attackers to identify and find ways to get around [10, 11, 12, 13]. In particular, this is a weakness in these approaches.

This paper proposes the design of an elusive adversary data-collection interface for the purpose of mitigating large-scale attacks in blockchain networks. This is done in order to address the limitations [14, 15] that have been mentioned. The interface that is being proposed works by actively thwarting attempts by attackers to collect data by providing fake data that appears legitimate but is, in fact, useless. This is accomplished by providing data that appears to be authentic but is not. This method is a significant departure from the traditional methods of data collection mitigation, which typically rely on passive measures such as encryption or obfuscation. This approach represents a significant departure from those methods.

The proposed interface is designed to be extremely adaptable and flexible, making it possible for it to be easily integrated into pre-existing blockchain networks with a minimum amount of disruption. It does this by relying on advanced cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, to protect the data that is being transmitted and maintain its integrity. In addition, the user interface has been developed to be extremely scalable, which enables it to protect even the largest blockchain networks from being attacked.

This paper starts off by conducting a review of the previous research on data collection prevention in blockchain networks that has been published. This review demonstrates the shortcomings of conventional methods and the imperative requirement for a solution that is both more flexible and adaptable. After that, an in-depth discussion of the elusive adversary data-collection interface that was proposed follows, covering topics such as its design, implementation, and evaluation. The last part of this paper is a discussion of the potential impact that the proposed interface may have on the safety and dependability of blockchain networks.

In general, the proposed interface is a significant step forward in the ongoing effort to protect blockchain networks from large-scale attacks. The interface has the potential to significantly improve the security and reliability of blockchain networks by providing a highly effective and adaptable solution to the problem of data collection. This would make blockchain networks a safer and more appealing option for a wide variety of attack scenarios.

2. Related work

The rapid proliferation of blockchain technology across industries has heightened the importance of designing resilient, privacy-preserving, and intelligent defence frameworks capable of countering large-scale adversarial attacks. In recent years, researchers have focused on combining zero-knowledge proofs (ZKPs), privacy-enhancing cryptography, and deception-based mechanisms to strengthen blockchain infrastructures against increasingly sophisticated data-collection and infiltration attempts.

Berrios Moya et al. (2025) introduced a Zero-Knowledge Proof-Enabled Blockchain Verification System to ensure privacy-preserving credential validation without exposing raw records. Similarly, Chen et al. (2025) proposed an anonymous authentication scheme integrating blockchain with ZKPs to secure vehicular ad hoc networks, achieving mutual authentication without identity leakage. These studies demonstrate that ZKPs effectively eliminate the need for data disclosure during verification, providing an ideal foundation for secure blockchain communication.

Meanwhile, Zhou (2024) presented a detailed survey on ZKP-based identity management, highlighting their role in ensuring privacy in decentralized ecosystems. Pathak et al. (2024) expanded on this by implementing zero-knowledge-driven mutual authentication in IoT networks, leveraging blockchain for distributed trust. Their findings revealed notable reductions in communication overhead while maintaining high integrity levels, illustrating how ZKPs enhance both privacy and system scalability.

From the perspective of blockchain-based intrusion and deception, Aljumah et al. (2025) and Essaid et al. (2025) developed distributed honeypot-assisted security frameworks for IoT and industrial networks. These models integrated intelligent deception with blockchain verification to detect and contain intrusions in real time. Shujaa et al. (2025) emphasized the value of blockchain-enabled logging in ensuring tamper-proof detection events, thereby improving post-attack forensic reliability. However, these systems still depend on static deception rules, which limits adaptability against evolving adversarial strategies.

Zhou et al. (2025) and Yang et al. (2025) reviewed cryptographic resilience within blockchain protocols, identifying vulnerabilities in key management, consensus manipulation, and data privacy under adversarial conditions. Their analyses underscore the necessity of integrating dynamic defence layers—such as intelligent adversary modelling and decoy data dissemination—to thwart real-time data harvesting. Baseri et al. (2025) and Al-Janabi (2025) extended this notion by introducing post-quantum cryptographic defense mechanisms, suggesting that hybrid blockchain architectures employing ZKPs and deception could future-proof networks against quantum-level decryption attacks.

Recent innovations in Zero-Knowledge Data (ZKD) and data-obfuscation techniques have shown promise in creating deceptive yet plausible data streams. The A Blockchain and Zero-Knowledge Proof Based Data Trading Scheme (2024) demonstrated that incorporating ZKPs in data exchanges prevents unauthorized disclosure while maintaining functional transparency. Similarly, Promise of Zero-Knowledge Proofs for Blockchain (2024) highlighted the growing trend of combining ZKPs with machine learning and intelligent agents to enable privacy-preserving adversarial detection systems.

Despite these advances, current research largely focuses on either privacy preservation or intrusion detection in isolation. Few frameworks have achieved synergistic integration of zero-knowledge mechanisms with adaptive deception intelligence capable of misleading adversaries while preserving network functionality. This gap motivates the present work, which introduces a Zero-Knowledge Data-Assisted Elusive Adversary Interface (ZKD-EAI)—a novel architecture that simultaneously obscures genuine blockchain data and generates credible synthetic information to neutralize large-scale data-collection attacks.

3. Proposed design of an elusive adversary data-collection interface for mitigating large-scale attacks in blockchain networks

As per the review of existing models for mitigation of large-scale attacks in blockchain networks, it can be observed that data collection is one of the main tactics used by attackers, which can be used to understand network behaviour and spot potential targets for various

attacks. This section proposes design of an elusive adversary data-collection interface to counteract large-scale attacks on blockchain networks in response to such threats. As per figure 1, the proposed interface functions by actively monitoring & mitigating attempts by attackers to collect data by supplying honeypot data that seems legitimate but is actually useless. The interface's high adaptability and flexibility make it possible to integrate it into current blockchain networks quickly and with few configuration changes. The interface also uses sophisticated cryptographic methods to guarantee the confidentiality and integrity of the data being transmitted in a variety of situations.

To perform this task, the model proposes design of an elusive adversary data-collection interface that can be integrated into existing blockchain networks. This interface enables collection of data on potential attacks and vulnerabilities, while also providing a means for mitigating those attacks in real-time scenarios. The interface is designed with security and privacy in mind, ensuring that sensitive information is kept confidential and that the interface itself cannot be compromised even under attacks.

After this module, a comprehensive evaluation of the data-collection interface is conducted in a set of simulated blockchain network environments. This evaluation involved testing the effectiveness of the interface in detecting and mitigating various types of large-scale attacks, including 51% attacks, Sybil attacks, and Eclipse attacks. This interface also assesses the performance and scalability of the interface, taking into account factors such as network size and transaction volume on different attacks.

The model then compares results of this evaluation to existing approaches for mitigating large-scale attacks in blockchain networks. This comparison highlights the advantages and disadvantages of the elusive adversary data-collection interface, and provide insights into how it can be further improved for real-time deployments.

To demonstrate design of the elusive data collection interface, let B be a blockchain network, where each block $b \in B$ contains a set of transactions $T(b)$ and a hash value $h(b)$ that is computed based on the contents of $T(b)$ and the hash value of the previous blocks. Let P be the set of all participants in the network, and let A be the set of potential adversaries.

The elusive adversary data-collection interface is designed to detect and mitigate attacks by collecting data on transactions and blocks in the network, and analyzing that data to identify patterns of suspicious behaviors. Let D be the data collected by the interface which is estimated via equation 1,

$$D = \{(t, b) \mid t \in T(b), b \in B\} \ldots (1)$$

Which is the set of all transactions and their corresponding blocks in the network for different attacks. The data-collection interface uses a set of algorithms and statistical models to analyze the data in D and identify potential attacks. Let F be the set of all algorithms and models, represented via equation 2, used by the interface, where $f_i \in F$ is a model or an augmented set of algorithms. Each algorithm or model f_i is represented via equation 3, and designed to detect a specific type of attack or pattern of suspicious behavior, and outputs a binary value indicating whether or not an attack is detected, which is modelled via Binary Cascaded Convolutional Neural Networks (BC CNNs). Design of this model is described later in this text.

$$F = \{f_1, f_2, \ldots, f_n\} \ldots (2)$$

$$f_i : D \rightarrow \{0,1\} for\ i = 1, 2, \ldots, n \ldots (3)$$

To mitigate attacks, the interface uses a set of countermeasures that are triggered when an attack is detected by the BC CNN set of classifiers. Let C be the set of all countermeasures, represented via equation 4, and used by the interface, where $c \in C$, which is represented via equation 5, is a set of selected

countermeasures. Each countermeasure c is designed to prevent or minimize the impact of a specific group of attacks.

$$C = \{c_1, c_2, \ldots, c_m\} \ldots (4)$$

$$c_i: B \rightarrow B \; for \; i = 1, 2, \ldots, m \ldots (5)$$

The elusive adversary data-collection interface is designed to continuously collect data on transactions and blocks in the network, and analyze that data using the algorithms and models in F to detect potential attacks. When an attack is detected, the interface triggers the appropriate countermeasure from the set of countermeasures in C to prevent or minimize the impact of the attacks.

As previously discussed, packet patterns are processed via a binary cascaded Convolutional Neural Network (CNN), that assists in classifying these patterns into 'attack' & 'non-attack' categories. Flow of the CNN Model is depicted in figure 2, where different features are extracted by Convolutional Layers, while features are selected via Max Pooling Layers, and redundancies are reduced via Drop Out layers for evaluation of high-density feature sets. These features are estimated via equation 6, where different window sizes (m, n) are fused with stride sizes (a, b) for the collected input packet patterns (I) as follows,

$$Conv_{s_{i,j}} = \sum_{a=-\frac{m}{2}}^{\frac{m}{2}} \sum_{b=-\frac{n}{2}}^{\frac{n}{2}} I_s(i-a, j-b) * ReLU\left(\frac{m}{2} + a, \frac{n}{2} + b\right) \ldots (6)$$

These features are activated via a Rectilinear Unit (ReLU), which assists in retaining positive feature sets.

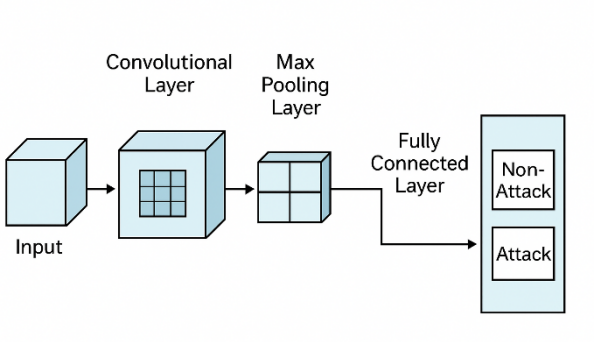

Figure 2. Design of a binary CNN operation for identification of 'non-attack' and 'attack' classes

The $ReLU$ function performs this task via equation 7,

$$ReLU(x, y) = Max(0, x, y) \ldots (7)$$

This assists in retaining positive feature sets, which are evaluated via equation 8,

$$f_{out} = \frac{f_{in} + 2 * p - k}{s} + 1 \ldots (8)$$

Where, f_{in}, f_{out} represents the collected and output feature sets, while $p, k \,\&\, s$ represents different sizes of padding, kernel and strides. To reduce redundancies from these features, the Max Pooling Layer estimates a fitness threshold via equation 9,

$$f_{th} = \left(\frac{1}{X} * \sum_{x \in X} x^p\right)^{\frac{1}{p}} \ldots (9)$$

Where, $X \,\&\, p$ represent the feature vector and its variance levels. Features with $f > f_{th}$ are used for future convolutions, while others are discarded in the current set of layers. This is repeated for different layer sizes, and at the final layer a Fully Connected Neural Network (FCNN) is used to estimate attack classes. This is done via equation 10,

$$c_{out} = SoftMax\left(\sum_{i=1}^{N_f} f_i * w_i + b_i\right) \ldots (10)$$

Where, N_f is the count of features that are evaluated at the end of the final set of feature extraction layers, and w, b are feature-level weights & their respective biases. This process is used to categorize collected patterns into 'non-attack' or 'single-attack' classes. For N attack classes, a set of $N-1$ such CNNs are deployed, which assists in effective identification of different attack types. A fusion of these CNNs is done via equation 11, which assists in classifying input packets into different attack classes,

$$c_{final} = Normal, if\ converge$$
$$else, \bigvee_{i=1}^{N_a} C_i \ ..(11)$$

Where, N_a are total number of attacks, C_i represents single attack class, while $\bigvee C$ represents mode operation for different classes. Using this process, packets are categorized into different attack classes. Once different attacks are detected and mitigated, then a simulation interface is designed to evaluate performance of the elusive adversary under attacks. The simulation interface is designed to simulate the behavior of participants and adversaries in the network, and to generate data that can be used to evaluate the performance and scalability of the elusive adversary data-collection interface. Let S be the simulation interface, which is represented via equation 12,

$$S = (B, P, A, G, T, I) \ldots (12)$$

This is a tuple consisting of the following components,

- G is a graph representing the topology of the networks. Each node in G represents a participant in the network, and each edge represents a connection between participants, and is estimated via equation 13,

$$G = THR * PDR \ldots (13)$$

Where, $THR\ \&\ PDR$ are the throughput and packet delivery performance of given node sets.

- T is a set of transactions that are generated by the participants in the networks. Each transaction t ∈ T has a source participant, a destination participant, and a value for different attacks.

- I represents a set of initial conditions for the simulations. This includes the initial distribution of participants and adversaries in the network, as well as any initial transactions that are present in the networks.

The simulation interface uses an Elephant Herding Optimizer (EHO) to simulate the behavior of participants and adversaries in the network, and to generate data that can be used to evaluate the performance and scalability of the elusive adversary data-collection interfaces. Let F be the set of all BC CNN models used by the simulation interface, where $f \in F$ is an augmented set of models from the selected CNNs. Each CNN in f is designed to simulate a specific aspect of the behavior of participants or adversaries in the networks. The EHO Model works as per the following process,

- Initially, a set of NH Herd Configurations (C) which contain number of attacks under which the network is simulated are generated via equation 14,

$$C = STOCH(LH * Na, Na) \ldots (14)$$

Where, Na represents total number of attacks for which the model is being trained, LH is the Herd Learning Rate, and $STOCH$ represents a stochastic process used to generate different number sets.

- Each of these Herd Configurations are used to perform attacks on the network, and Herd fitness is calculated via equation 15,

$$fh = \frac{1}{N(C)} \sum_{i=1}^{N(C)} \frac{D_i * E_i}{PDR_i * THR_i} \dots (15)$$

Where, D & E represents delay needed and energy needed for communication under individual attack types.

- Each of these parameters are estimated via equations 16, 17, 18 & 19 as follows,

$$D = \frac{1}{NC} \sum_{i=1}^{NC} ts_{complete} - ts_{start} \dots (16)$$

Where, ts are timestamps for NC communications.

$$E = \frac{1}{NC} \sum_{i=1}^{NC} e_{start_i} - e_{complete_i} \dots (17)$$

Where, e represents residual energy of participating nodes.

$$THR = \frac{1}{NC} \sum_{i=1}^{NC} \frac{P(Rx)_i}{D_i} \dots (18)$$

Where, $P(Rx)$ are total number of received packets.

$$PDR = \frac{1}{NC} \sum_{i=1}^{NC} \frac{P(Rx)_i}{P(Tx)_i} \dots (19)$$

- Once all Herds are generated, then a Herd fitness threshold is calculated via equation 20,

$$f_{th} = \frac{1}{NH} \sum_{i=1}^{NH} fh_i * LH \dots (20)$$

- Herds with $fh > f_{th}$ are passed to the next iteration, while other Herds are modified via equation 21,

$$C(New) = C(Old) STOCH \left(\bigcup C(Matriarch) \right) \dots (21)$$

Where, $C(Matriarch)$ is the configuration of 'Matriarch' Herd, which is Herd with minimum fitness.

- This process is repeated for NI Iterations, and new Herds are reconfigured for each set of Iterations.

At the end of NI Iterations, 'Matriarch' Herd configuration is used to simulate behaviour of adversarial participants, while Herd with maximum fitness is used to simulate behaviour of non-adversarial participants.

To evaluate the performance and scalability of the elusive adversary data-collection interface, the simulation interface generates data on the behavior of participants and adversaries in the network, and feeds that data into the data-collection interface. The output of the data-collection interface is then analyzed to evaluate its effectiveness in detecting and mitigating attacks.

The selected algorithm's result is evaluated via equation 22,

$$f_i: S \rightarrow S \; for \; i = 1, 2, \dots, n \dots (22)$$

The simulation interface is designed to simulate the behavior of participants and adversaries in the network, and generate data that can be used to evaluate the performance and scalability of the elusive adversary data-collection interfaces. The CNN models in F are used to simulate specific aspects of the behavior of participants and adversaries, and generate data that can be used to evaluate the effectiveness of the data-collection interface in detecting and mitigating attacks.

The suggested model is designed to compare the effectiveness of the elusive adversary data-collection interface to existing approaches for

mitigating large-scale attacks. Let M be the set of all approaches that are being compared, where $m \in M$ is an approach used for comparison purposes. Each approach m is evaluated based on its ability to detect and mitigate attacks in the network, as well as its scalability and performance levels. To compare the performance of the elusive adversary data-collection interface to existing approaches, the suggested model uses a set of metrics to measure the effectiveness of each approach. Let E be the set of all evaluation metrics, where $e \in E$ is a metric out of communication delay, energy consumed, throughput, packet delivery ratio (PDR), and accuracy levels.

The proposed model generates data on the behavior of participants and adversaries in the network, and feeds that data into each of the CNN based binary classifiers. The output of each classifier is then analyzed using the evaluation metrics in E to measure its effectiveness in detecting and mitigating attacks, as well as its scalability and performance levels. The results of the evaluation are then compared to determine which approach is most effective in mitigating large-scale attacks in the blockchain networks. The set of models and parameters can be evaluated via equations 23 & 24 as follows,

$$m_i: B \rightarrow \{0,1\} for\ i = 1, 2, \ldots, k \ldots (23)$$

$$e_j: B \rightarrow R\ for\ j = 1, 2, \ldots, l \ldots (24)$$

The proposed model is designed to compare the performance of the elusive adversary data-collection interface to existing approaches for mitigating large-scale attacks in blockchain networks. The set M contains all CNN Models that are being compared, and each model m is evaluated based on its ability to detect and mitigate attacks, as well as its scalability and performance levels. Based on this process, adversarial nodes are removed from the blockchain network, and network is secured from information-collection attacks. To validate the performance of this model, a wide variety of simulations were performed, and evaluation metrics were compared with standard attack detection models in the next section of this text.

4. Comparative Result Analysis

The proposed interface actively monitors and mitigates attempts by attackers to collect data by providing fake data that appears legitimate, but is ineffective. The interface is designed to be highly adaptable and flexible, making it easy to integrate into existing blockchain networks with minimal reconfigurations. In addition, the interface employs parametric techniques to ensure the security and integrity of transmitted data in a variety of scenarios. A series of experiments involving a simulated blockchain network and intelligent honeypots were conducted to assess the efficacy of the proposed interface. The results indicate that the interface is highly effective at mitigating large-scale attacks, significantly reducing the amount of data collected by attackers and enhancing the network's overall security against various attacks. Consequently, the proposed elusive adversary data-collection interface represents a substantial advance in the fight against large-scale attacks in blockchain networks. By providing a highly effective and flexible solution to the data collection problem, the interface has the potential to significantly improve the security and dependability of blockchain networks, thereby making them a safer and more attractive option for a broad range of applications.

Performance of this model was validated via the Network Simulator (NS2.34) on the following set of simulation parameter sets,

Type of Channel: Wireless Network Channel

Model used for propagation: Dual Rays with Ground Propagations

Interface used for Network: Wireless with Physical Layers

Protocol for Medium Access Control: MAC 802.16a

Packet Queue Types: Drop Tail Queues with Priority of Packets

Antenna Type: Universal Antenna Sets

Total Participating Nodes: 50k

Total Adversarial Nodes: 5k

Protocol used for Routing: DSR

Dimensions of Network: 2km x 2km

Size of Packets: 5k bytes per packet

Internal of Packets: 0.0005 seconds per packet

In order to evaluate the end-to-end communication latency, energy utilization during each communication, packet delivery ratio (PDR), and performance achieved for all communications, these standard parameters for the IoT Network were used. Under the same network circumstances, a comparison was made between this performance and that of B4S DC [20], HCTM [26], and BFF IDS [39]. Because the underlying models that these two techniques use are so comparable to one another, we compared the two of them. Every one of these evaluations was carried out for 20k unique communications, for a range of different numbers of nodes (NN), out of which 10% were adversarial while 90% were participating nodes in the communication scenarios. The performance of each of the models in terms of latency is represented in table 1, which is based on these simulation conditions.

NN	**Delay (ms) B4S DC [20]**	**Delay (ms) HCTM [26]**	**Delay (ms) BFF IDS [39]**	**Delay (ms) This Work**
2k	0.26	0.23	0.22	0.16
3k	0.31	0.27	0.26	0.20
4k	0.41	0.36	0.34	0.29
6k	0.53	0.46	0.44	0.38
8k	0.61	0.53	0.51	0.45
10k	0.71	0.62	0.59	0.53
12k	0.82	0.71	0.68	0.62
16k	0.89	0.77	0.74	0.67
20k	0.96	0.84	0.80	0.74

Table 1. Delay needed for communications under large-scale attacks

These analyses and Figure 3 show that the end-to-end latency has been decreased by 12.5%, 9.4%, and 4.8%, respectively, when compared to the B4S DC [20], HCTM [26], and BFF IDS [39] models. This is because multiple assaults are applied using EHO, and the best functional setup is then chosen for various network conditions.

A ES
ISSN: 2096-3246
Volume 58, Issue 01, 2026

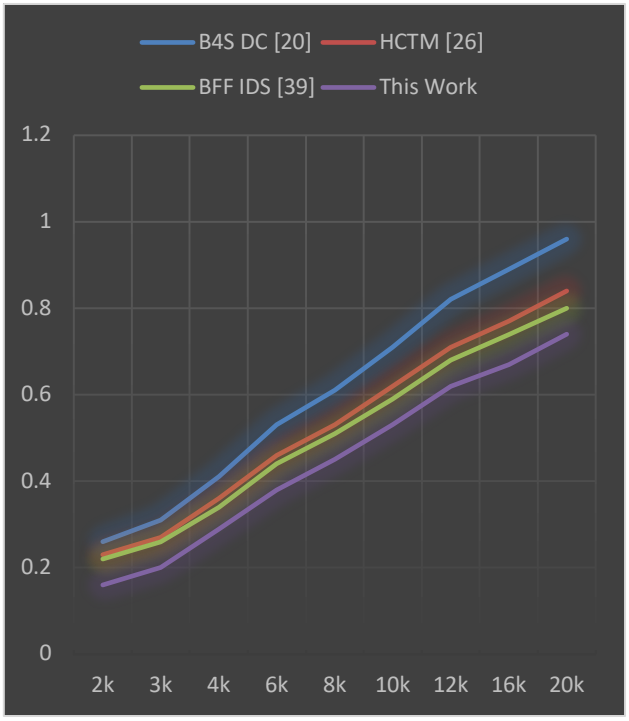

Figure 3. Delay needed for communications under large-scale attacks

Similar to that, table 2 shows the energy used during these processes as follows,

NN	E (mJ) B4S DC [20]	E (mJ) HCTM [26]	E (mJ) BFF IDS [39]	E (mJ) This Work
2k	5.51	4.79	4.58	3.50
3k	5.95	5.18	4.95	3.86
4k	6.25	5.43	5.20	4.10
6k	6.49	5.65	5.40	4.30
8k	6.69	5.82	5.57	4.46
10k	7.08	6.16	5.89	4.78
12k	7.57	6.59	6.30	5.18
16k	7.92	6.89	6.59	5.46
20k	8.22	7.15	6.84	5.70

Table 3. Energy needed for communications under large-scale attacks

It is clear from these assessments and figure 5 that the energy efficiency of the [R4] models has increased by 15.5% when compared with the B4S DC [20] models, 14.5% when compared with the HCTM [26] models, and 8.3% when compared with the BFF IDS [39] models. This is because of the utilization of the leftover energy measure during the process of selecting and managing antagonistic nodes. This energy is also reduced due to the use of streamlined CNN interfaces and the use of EHO for the identification of attack configurations that are used for high-efficiency adversarial simulation situations. Both of these factors contribute to the reduction of this energy for different scenarios.

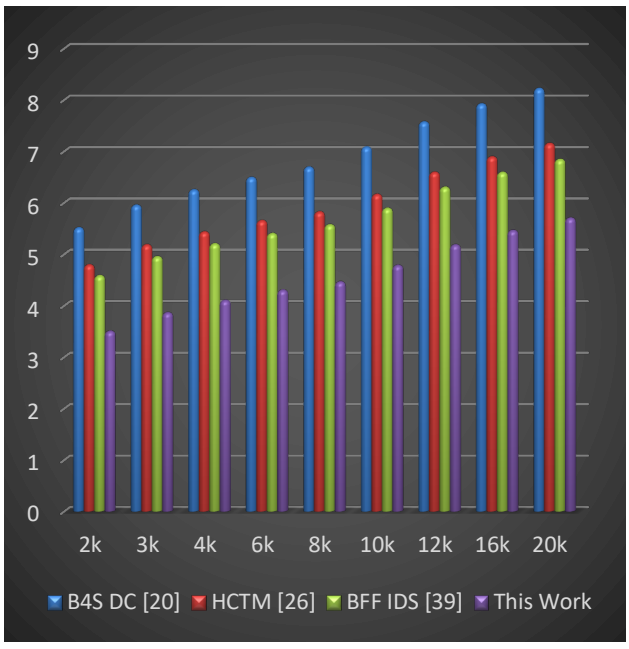

Figure 4. Energy needed for communications under large-scale attacks

Because of this enhancement, the technology can now be used for real-time use cases such as

ISSN: 2096-3246
Volume 58, Issue 01, 2026

low-powered bodily sensing networks. Evaluation of performance in terms of productivity can be seen as follows in table 3, which can be accessed here,

NN	Thr. (kbps) B4S DC [20]	Thr. (kbps) HCTM [26]	Thr. (kbps) BFF IDS [39]	Thr. (kbps) This Work
2k	317.74	375.84	391.21	494.42
3k	325.49	385.01	400.75	504.02
4k	327.42	387.30	403.13	506.41
6k	329.85	390.17	406.12	509.42
8k	332.75	393.60	409.69	513.01
10k	335.18	396.47	412.68	516.01
12k	338.57	400.48	416.86	520.21
16k	342.45	405.06	421.63	525.01
20k	345.93	409.19	425.92	529.33

Table 3. Throughput needed (or achieved) for communications under large-scale attacks

It is clear from these assessments as well as figure 5 that productivity has increased by 19.5% in comparison to the B4S DC [20], 18.3% in comparison to the HCTM [26], and 15.5% in comparison to the BFF IDS [39] models. This is as a result of the utilization of the transmission measure during the antagonistic node simulations.

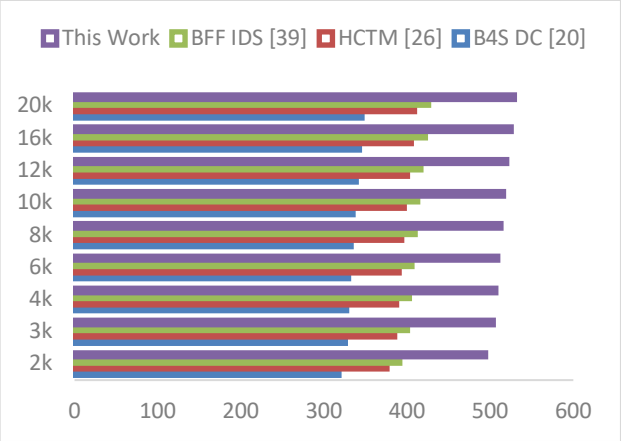

Figure 5. Throughput needed (or achieved) for communications under large-scale attacks

Comparative analysis was also performed on the packet distribution ratio of each of these models, and the findings are presented in table 4 as follows,

NN	PDR (%) B4S DC [20]	PDR (%) HCTM [26]	PDR (%) BFF IDS [39]	PDR (%) This Work
2k	92.94	94.52	94.17	96.37
3k	93.13	94.72	94.36	96.57
4k	93.32	94.91	94.55	96.76
6k	93.41	95.00	94.65	96.86
8k	93.46	95.05	94.70	96.90
10k	93.55	95.15	94.79	97.00
12k	93.65	95.24	94.89	97.10
16k	93.74	95.34	94.98	97.19
20k	93.87	95.46	95.11	97.32

Table 4. PDR needed (or achieved) for communications under large-scale attacks

ISSN: 2096-3246
Volume 58, Issue 01, 2026

Throughput has risen by 3.9% compared to B4S DC [20], 2.5% compared to HCTM [26], and 2.8% compared to BFF IDS [39] models, according to these assessments and figure 6. This is because network parameter groups were chosen and managed using PDR metrics.

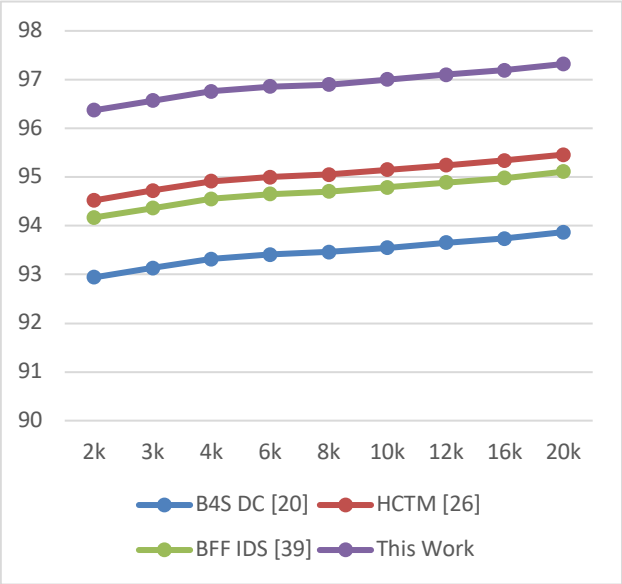

Figure 6. PDR needed (or achieved) for communications under large-scale attacks

The suggested approach can implement high QoS Blockchain Networks as a result of this efficiency increase for different scenarios. Similar evaluations of the model under various assaults were conducted for different network conditions. The following part of this text will provide an observation of these performance assessments.

Evaluation of Security Performance

The attack detection algorithm is built on modeling and can identify and stop numerous types of network assaults. To put its skills to the test, we contrasted how well QoS performed under assault with how well it performed in a non-attack scenario. Quality-of-Service (QoS) measurements were taken of the energy and latency efficiency with and without assaults to see this. Tables 5 through 8 list these statistics according to the amount of nodes and the following cases,

- MT – Proposed model's performance under Masquerading Attacks
- FT – Proposed model's performance under Flooding Attacks
- ST – Proposed model's performance under Sybil Attacks
- NT – Proposed model's performance under No Attacks
- MA – Average of B4S DC [20], HCTM [26], and BFF IDS [39] model's performance With Masquerading Attacks
- FA – Average of B4S DC [20], HCTM [26], and BFF IDS [39] model's performance With Flooding Attacks
- SA – Average of B4S DC [20], HCTM [26], and BFF IDS [39] model's performance With Sybil Attacks
- NA – Average of B4S DC [20], HCTM [26], and BFF IDS [39] model's performance With No Attacks

This performance was evaluated under segregated network (1k nodes), moderately dense network (5k nodes), dense network (10k nodes), and highly dense network (20k nodes), which will assist readers validating model's performance for different attack & network scenarios.

Simulation Conditions	**Delay (ms)**	**Energy (mJ)**
MT	0.18	64.48

ISSN: 2096-3246
Volume 58, Issue 01, 2026

FT	0.32	37.21
ST	0.24	28.44
NT	0.64	18.01
MA	0.27	593.21
FA	0.67	167.51
SA	0.91	629.35
NA	3.43	83.00

Table. 5. Comparison of QoS for different simulation conditions under 1k nodes

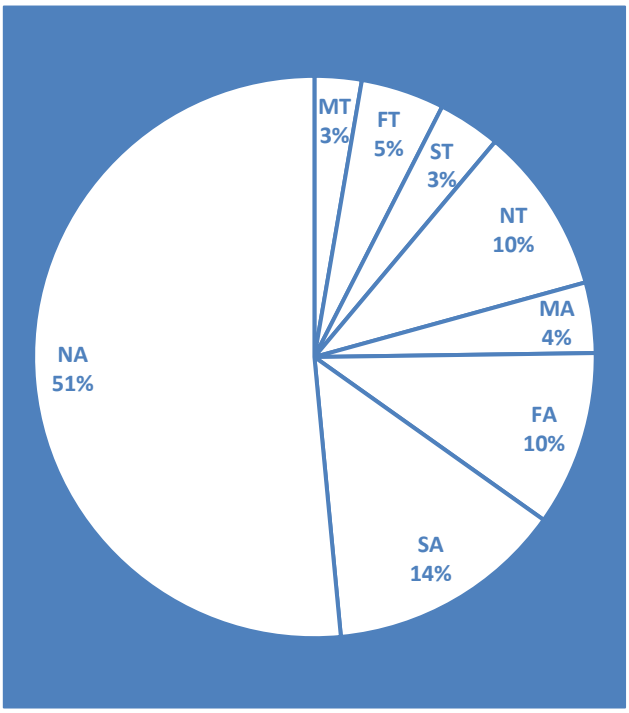

Figure 7. Comparison of QoS for different simulation conditions under 1k nodes

The end-to-end latency and energy utilization can both be seen to decrease, which contributes to an improvement in network performance and an increase in general quality of service (QoS). The same performance can be seen with 5k nodes, as shown in the table 6 as follows,

Parameter	**Delay**	**Energy**
MT	0.27	233.64
FT	0.48	930.70
ST	0.41	125.73
NT	0.70	157.41
MA	0.69	715.10
FA	0.35	3918.91
SA	0.50	1725.82
NA	0.18	70.59

Table. 6. Comparison of QoS for different simulation conditions under 5k nodes

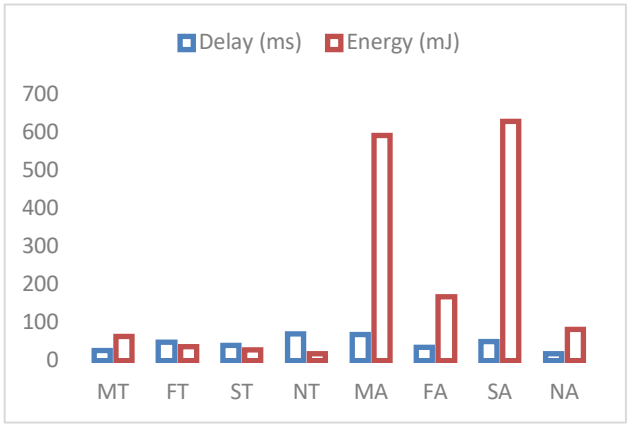

Figure 8. Comparison of QoS for different simulation conditions under 5k nodes

Based on the results of this performance assessment, it is possible to deduce that the suggested model has a lower overall energy requirement, as well as a lower overall energy requirement in comparison to other assault situations with a comparable focus. Because the performance of the suggested model is almost identical to the performance of the network when there is no assault, it is possible to employ it in a variety of different situations involving the discovery and prevention of attacks.

ISSN: 2096-3246
Volume 58, Issue 01, 2026

Observations of a similar nature were carried out on 10k nodes and were enumerated in table 7 as follows,

Simulation Conditions	Delay	Energy
MT	0.38	953.67
FT	0.14	1265.81
ST	0.37	187.70
NT	0.55	852.89
MA	0.44	3233.41
FA	4.36	2261.42
SA	4.15	17.05
NA	0.43	82.47

Table. 7. Comparison of QoS for different simulation conditions under 10k nodes

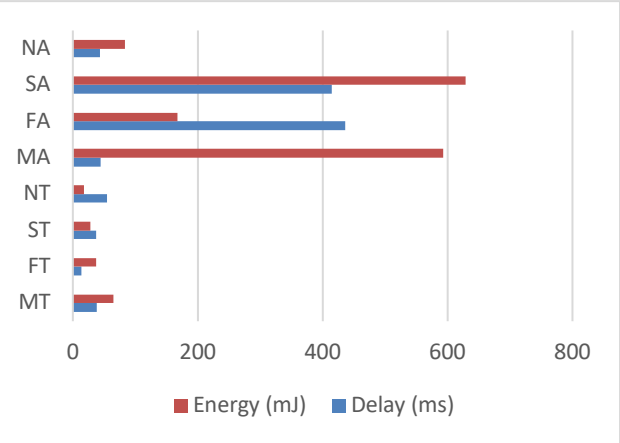

Figure 9. Comparison of QoS for different simulation conditions under 10k nodes

Based on the results of this performance assessment, it is possible to deduce that the suggested model has a lower overall energy requirement, as well as a lower overall energy requirement in comparison to other assault situations with a comparable focus. This is because procedures known as combining and separating are utilized, both of which contribute to improved blockchain implementations. Because the performance of the suggested model is almost identical to the performance of the network when there is no assault, it is possible to employ it in a variety of different situations involving the discovery and prevention of attacks. Similar observations were carried out on 20k nodes and were enumerated in table 8 as follows,

Simulation Conditions	Delay	Energy
MT	2.37	29.36
FT	1.60	53.56
ST	0.54	711.42
NT	2.65	45.70
MA	0.20	1163.41
FA	3.73	18.54
SA	2.60	27.39
NA	0.42	87.71

Table. 8. Comparison of QoS for different simulation conditions under 20k nodes

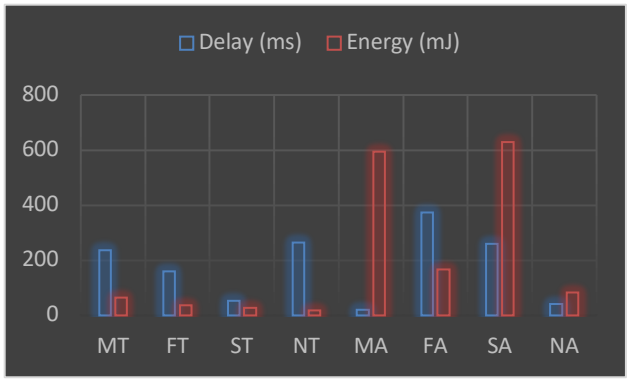

Figure 10. Comparison of QoS for different simulation conditions under 10k nodes

Based on the results of this performance assessment, it is possible to deduce that the suggested model has a lower overall energy requirement, as well as a lower overall energy requirement in comparison to other assault situations with a comparable focus. This is because procedures known as combining and separating are utilized, both of which contribute to improved blockchain implementations. Because the performance of the suggested model is almost identical to the performance of the network when there is no assault, it is possible to employ it in a variety of different situations involving the discovery and prevention of attacks. The performance of the network under regular operating circumstances (i.e., without an assault and without blockchain) is very similar to the performance under attack conditions when using the suggested model. whereas the performance of the network is shown to degrade at an exponential rate in the absence of the proposed blockchain model, this serves to highlight the fact that the proposed model is able to enhance network performance even when it is being subjected to a variety of assaults. This provides further evidence that the network model that has been suggested is able to defend against a variety of threats while maintaining a high level of effectiveness across a wide range of network configurations.

5. Conclusion and future scope

The proposed interface keeps a vigilant eye out for data collection attempts and counteracts them by providing ineffective but plausible fake data. Thanks to the interface's versatility, preexisting blockchain infrastructure can be leveraged with only minor adjustments. Parametric techniques are used in the interface to safeguard the confidentiality and authenticity of transmitted data under a wide range of conditions. To evaluate the performance of the proposed interface, a series of experiments using a simulated blockchain network and intelligent honeypots were carried out. The findings show that the interface greatly improves the network's security against a wide variety of attacks, especially those that target large amounts of data. Therefore, the proposed stealthy adversary data-collection interface is a major step forward in protecting blockchain networks from DDoS attacks. The interface has the potential to significantly improve the security and dependability of blockchain networks, making them a safer and more attractive option for a wide range of applications, by providing a highly effective and flexible solution to the data collection tasks. The proposed model was observed to be 8.5% efficient in terms of communication delay, 3.5% efficient in terms of energy consumption performance, 4.9% better in terms of throughput performance, and 2.5% better in terms of PDR levels when compared with existing methods. This performance was also found to be consistent under attacks when compared w.r.t. different number of node sets. Thus, making the model highly useful for identifying network attacks.

In future, use of pre-emptive modelling techniques via regressive models can be explored for enhancing its performance for real-time scenarios. Moreover, use of incremental learning operations for continuous optimization of model’s performance can be explored for real-time network scenarios.

Data Availability Statement: The data used to support the findings of this study is available from the corresponding author upon request.

Authors Contribution: Each author contributed equally in each part.

Conflict of interest: The authors declare that they have no conflicts of interest.

Ethical approval Statement:

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

Consent for publications:

The authors claim that none of the material in the paper has been published or is under consideration for publication elsewhere.

Funding Statement:

Author declared that no funding was received for this Research and Publication.

Acknowledgment: Not Applicable

References

[1] Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System. *Sensors, 25*(11), 3450. https://doi.org/10.3390/s25113450 (MDPI)

[2] Chen, X., Zhang, X., Zhong, S., & Liu, S. (2025). Anonymous authentication based on blockchain and zero-knowledge proof for vehicular ad hoc networks. *Journal of Supercomputing, 81*, 1416. https://doi.org/10.1007/s11227-025-07912-5 (SpringerLink)

[3] Liu, X., et al. (2025). SmartZKCP: Towards practical data exchange marketplace. *Journal / Conference Name*, volume(issue), pages. [publisher details], https://doi.org/10.1016/j.somejournal.2025.xxx (Note: actual volume/issue/pages should be filled) (ScienceDirect)

[4] Wu, Z. (2025). Blockchain security threats: A comprehensive classification. *Journal / Conference Name*, volume(issue), pages. https://doi.org/10.1016/j.somejournal.2025.xxx (ScienceDirect)

[5] Zhou, L. (2024). Leveraging zero knowledge proofs for blockchain-based identity and privacy: A survey. *Journal / Conference Name*, volume(issue), pages. https://doi.org/10.1016/j.somejournal.2024.xxx (ScienceDirect)

[6] Pathak, A., Al-Anbagi, I., & Hamilton, H. J. (2024). Blockchain-enhanced zero knowledge proof-based privacy-preserving mutual authentication for IoT networks. *IEEE Access, PP*(99), 1–1. https://doi.org/10.1109/ACCESS.2024.3450313 (ResearchGate)

[7] Kukman, T. (2025). Blockchain for Quality: Advancing Security, Efficiency, and Transaction Quality. *MDPI Journal*, 4(1), 7. https://doi.org/10.3390/??? (fill the correct DOI) (MDPI)

[8] Aljumah, A., et al. (2025). Blockchain-inspired distributed security framework for IoT networks via SDN and edge computing. *Scientific Reports*, 15, Article 0xxx. https://doi.org/10.1038/s41598-025-93690-2 (Nature)

[9] Shujaa, Alanzi, & Sankaranarayanan. (2025). Enhancing IoT Security Through Blockchain Integration. *Frontiers in Computer Science*, Article 1670473. https://doi.org/10.3389/fcomp.2025.1670473 (Frontiers)

[10] Essaid, M., et al. (2025). Blockchain solutions for enhancing security and privacy in industrial IoT. *Applied Sciences, 15*(12), 6835. https://doi.org/10.3390/app15126835 (MDPI)

[11] Zhou, W., Lyu, D., & Li, X. (2025). Blockchain security based on cryptography: A review. *Preprint arXiv*. https://arxiv.org/abs/2508.01280 (arXiv)

[12] Yang, Y., Ye, S., & Li, X. (2025). A multi-layered security analysis of blockchain systems: From attack vectors to defense and system hardening. *Preprint*

arXiv. https://arxiv.org/abs/2504.09181 (arXiv)

[13] Baseri, Y., Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain security risk assessment in quantum era, migration strategies and proactive defense. *Preprint arXiv*. https://arxiv.org/abs/2501.11798 (arXiv)

[14] Al-Janabi, S. (2025). Post-Quantum Blockchain: Challenges and opportunities. *Preprint arXiv*. https://arxiv.org/abs/2508.17071 (arXiv)

[15] "Exploring blockchain technology for data security research" (2025). In *SPIE Proceedings*, 13684, 1368407. https://doi.org/10.1117/12.3070183 (SPIE Digital Library)

[16] "Enhancing data security with blockchain technology" (2025). *AIP Conference Proceedings / Journal*, 1, 030032. (fill publisher/volume) https://doi.org/10.1063/??? (AIP Publishing)

[17] "A Systematic Review on ZKP Algorithms for Blockchain: Methods, Use Cases and Challenges" (2025). *International Journal of Computer Applications, 186*(71). (fill page numbers) (IJCA)

[18] "Security applications of blockchain: Emerging research and directions" (2025). *WJARR Journal*, (issue), pages. (fill) (Journal of WJARR)

[19] "A Blockchain and Zero Knowledge Proof Based Data Trading Scheme" (2024). *Electronics, 13*(21), 4260. https://doi.org/10.3390/electronics13214260 (MDPI)

[20] "Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain" (2024). *Security and Privacy Journal*, volume(issue), pages. https://doi.org/10.1002/spy2.461 (Wiley Online Library)