International Journal of Intelligent Communication and Computer Science
Vol. 3, No. 2, Pages 23-30.

A Blockchain-Enabled Architecture for Distributed and Immutable Honeypot Networks

Aparna Tiwari[1] and Dinesh Kumar[1]

Short Paper

[1]Research Scholar, Department of Computer Science and Engineering, Maharaja, Ranjit Singh Punjab Technical University, Bhatinda, INDIA

Email: aparnatiwariphd@gmail.com
Received: 02 Jan 2024 Revised: 11 Aug 2025 Accepted: 13 Sep 2025

Abstract:

In the rapidly evolving landscape of cybersecurity, traditional defense mechanisms often struggle to keep pace with the sophistication of modern cyberattacks. Distributed honeypot systems, designed to detect, analyze, and mitigate malicious activities by luring attackers into decoy environments, offer a promising solution. However, managing and securing these systems presents unique challenges, particularly in terms of data integrity, coordination, and scalability. This paper proposes a novel approach to enhancing distributed honeypots by leveraging blockchain technology and attack analysis techniques. Specifically, we integrate blockchain's decentralized ledger for secure, tamper-proof storage of honeypot data and attack logs, along with advanced attack analysis frameworks to gain deeper insights into adversary tactics. The proposed system enables real-time tracking of attack patterns, collaborative defense mechanisms, and a transparent audit trail for forensic analysis. We demonstrate the feasibility and effectiveness of this approach through simulations and real-world case studies, highlighting its potential to enhance the robustness and scalability of distributed honeypot networks.

Keywords: Honeypot, Blockchain, Attack

1. Introduction

Cybersecurity threats have become increasingly complex, with attackers adopting more sophisticated, distributed, and multi-vector strategies [1]. Today's adversaries often employ advanced techniques such as botnets, polymorphic malware, and distributed denial-of-service (DDoS) attacks, which can evade traditional security mechanisms. While firewalls, intrusion detection systems (IDS), and antivirus software are commonly used to defend against these threats, they are often reactive, designed to respond only after an attack has occurred. As a result, these tools frequently fail to protect against new or unknown attack vectors, leaving organizations vulnerable to emerging threats [2-5].

In response to these limitations, honeypots have emerged as a promising proactive defence strategy. A honeypot is a deliberately vulnerable or deceptive system designed to attract and engage attackers, diverting them from valuable assets while providing critical data for threat analysis and intelligence gathering. By observing how attackers interact with the honeypot, security teams can gain valuable insights into attack methods, tactics, and tools, which can be used to strengthen broader defence strategies. However, while effective, the traditional use of honeypots faces significant scalability and security challenges. For instance, when deployed in large, dynamic environments, maintaining a network of honeypots that is both secure and manageable becomes complex. Additionally, the data collected from honeypots may be susceptible to

tampering, making it difficult to trust the integrity of the information [6-9].
To address these challenges, this paper proposes the integration of blockchain technology with distributed honeypot systems. Blockchain, with its decentralized, transparent, and immutable nature, provides a solution to the inherent vulnerabilities of centralized honeypot systems. By leveraging the blockchain's tamper-proof ledger, honeypot data can be securely stored and shared across multiple nodes without fear of data corruption or manipulation. Moreover, the blockchain's distributed architecture allows for the creation of a robust, scalable network of honeypots that can operate collaboratively, sharing intelligence in real time. This not only improves the detection of cyber threats but also enhances the system's overall resiliency against attack [10].
Furthermore, we incorporate advanced attack analysis techniques, such as machine learning and anomaly detection, to process the attack data captured by the honeypots. These techniques help identify new attack patterns, correlate incidents across different honeypots, and automate responses to emerging threats. This combination of blockchain's security features and advanced analysis tools creates a more effective and intelligent defence system capable of responding proactively to cyber threats in real time.

2. Related Work

Honeypots have long been a valuable tool in the arsenal of cybersecurity professionals. By intentionally creating a decoy system that appears vulnerable, honeypots attract malicious actors who believe they are targeting a legitimate resource [6]. The advantage of this approach is that it allows defenders to observe attackers in a controlled environment, gathering crucial information about attack methodologies, tools, and techniques. This intelligence can then be used to improve detection systems, develop new countermeasures, and better understand emerging threats [7].
Despite their effectiveness, traditional honeypots have several limitations. First, scaling a honeypot network to cover large, distributed environments becomes increasingly difficult. Managing multiple honeypots spread across different geographic regions or systems requires significant coordination, and maintaining a high level of security in such a system becomes challenging. Furthermore, traditional honeypots are often isolated and lack the ability to share threat intelligence across multiple instances. This means that an attack detected by one honeypot may not be immediately shared with other parts of the system, slowing down the response time and leaving gaps in defence [8].
Another significant issue is the integrity of the data collected by honeypots. In traditional systems, it is possible for an attacker to manipulate or falsify the data captured by a honeypot, either by exploiting vulnerabilities in the honeypot itself or by gaining access to the server storing the data. This compromises the reliability of the information and undermines the trustworthiness of the threat intelligence gathered.
Blockchain technology, with its decentralized architecture, offers a promising solution to these problems. By utilizing blockchain's features of immutability and transparency, we can ensure that the data collected by honeypots is secure and tamper-proof. Once attack data is recorded on the blockchain, it cannot be altered or deleted without the consensus of the network, providing an additional layer of security and trustworthiness. Additionally, the blockchain enables honeypots to operate as part of a distributed network, where each honeypot node can share attack data in real time without relying on a central authority. This distributed approach allows for faster detection of emerging threats, more effective collaboration across different nodes, and better overall coordination.
Blockchain also provides an inherent audit trail, which can be used for forensic analysis and regulatory compliance. The immutable nature of blockchain means that every action, event, and decision made by the honeypot system is recorded, creating a comprehensive and tamper-proof log that can be reviewed if needed. This can be particularly valuable for incident response teams, law enforcement, or organizations seeking to trace the origins of an attack.

3. Methodology

A dynamic distributed honeypot system was proposed that utilizes a fixed number of hosts to form a secure private Blockchain network [25]. This network operates as a peer-to-peer (P2P) system, restricting access to only authorized entities and ensuring data security and integrity. The study introduces two types of honeypots—static and dynamic—each designed to improve network security by attracting and analyzing different kinds of cyberattacks. The combination of static and dynamic honeypots provides a more comprehensive defense strategy by enabling real-time adaptation to evolving attack patterns.

As shown in the figure 1, the system architecture consists of three main services, each paired with its respective honeypot. The underlying blockchain technology is used to maintain a distributed ledger that records interactions across all participating hosts. The blockchain operates as a private network, ensuring that the data shared between the hosts remains secure and confidential. Each host in the network forms part of a P2P topology, which is configured with specific parameters, such as packet size, transmission delay, and network topology, to optimize the performance of the distributed system. Every time a block is added to the blockchain, its hash value is computed, and hosts in the private blockchain use this hash to mine new blocks, ensuring that the architecture remains decentralized and distributed. This method of operation eliminates the reliance on a central authority, increasing the security and resilience of the honeypot system.
When a user initiates a transaction within the blockchain, they create a digital signature using their private key. This digital signature serves as proof of ownership and authorization, confirming the legitimacy of the transaction. The signature is paired with the user's public key, allowing other participants in the network to verify the transaction's authenticity without needing access to the private key. The efficiency of ECC not only ensures robust security but also speeds up transaction processing times by reducing the computational load associated with key generation and transaction signing. This makes the system more scalable and responsive, which is crucial for the performance of the blockchain-enabled honeypot network.

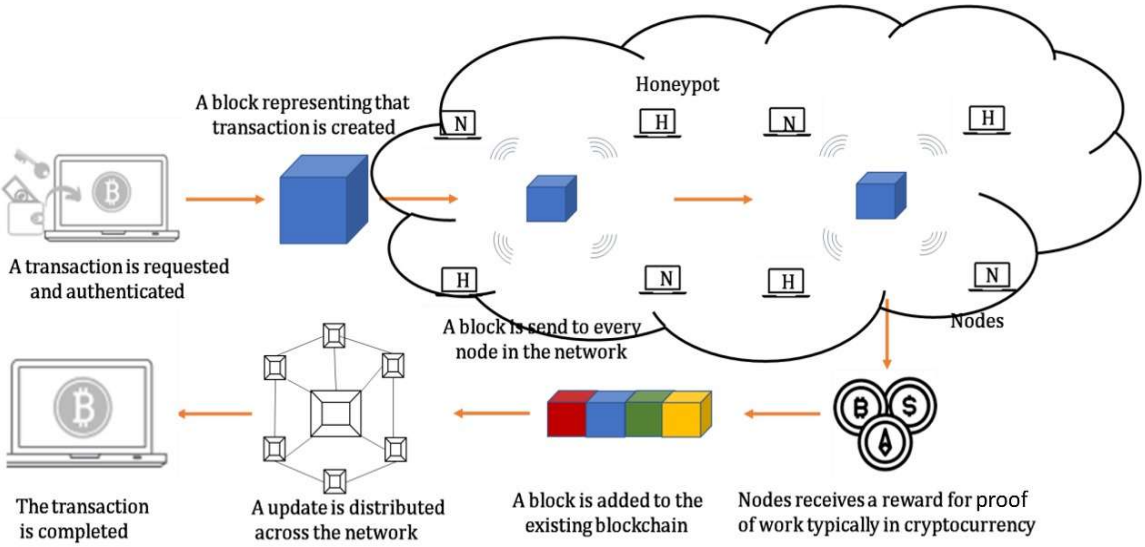

Figure 1: Blockchain enabled dynamic distributed honeypot system [12]

4. Blockchain Attack

Blockchain technology is often considered a secure, decentralized system due to its cryptographic foundations and decentralized nature [11]. However, like any technology, it is not immune to attacks, and adversaries have developed several strategies to compromise blockchain systems [12]. These attacks exploit vulnerabilities in consensus mechanisms, cryptographic protocols, and even the network's distributed nature [13]. To understand how blockchain can be compromised, it is essential to explore some of the key attack vectors, supported by mathematical concepts and cryptographic principles, that can undermine blockchain integrity [5-7].
A 51% attack occurs when an attacker gains control over more than 50% of the computational power (in Proof of Work) or stake (in Proof of Stake) of a blockchain network. This enables the attacker to disrupt the consensus mechanism, prevent the inclusion of legitimate transactions, and potentially reverse previous transactions.
In Proof of Work-based blockchains like Bitcoin, the difficulty of mining a new block is designed to ensure that finding a valid hash requires substantial computational effort. The hash function used in Bitcoin (SHA-256)

takes an input and produces a 256-bit output that appears random. The security of the blockchain relies on the fact that producing a valid hash for a block is computationally difficult and requires a large amount of computational power.

Mathematically, the probability of an attacker successfully mining a block is proportional to their computational power relative to the total network power. If an attacker controls more than 50% of the network's hash rate, they can consistently generate a longer valid chain (also known as a fork) faster than the rest of the network. Since blocks are added to the longest valid chain, the attacker can potentially cause a reorganization of the blockchain, invalidating legitimate transactions.

The probability P that an attacker with 51% control will win the race to mine a block in a network of total hash rate can be approximated as:

$$P_{attacker} = \frac{\text{Attack Hash Rate}}{\text{Total Hash Rate}} > 0.5$$

4. Results and Discussion

The simulation was configured with a total of twenty nodes, two of which were designated as honeypots. These honeypots have a 50% chance of detecting malicious activity in each round, mimicking probabilistic attack behaviour in real-world networks. The simulation runs for hundred rounds, during which nodes record events, mine blocks, and propagate them across the network. A simplified hash function based on ASCII summation is used due to compatibility with MATLAB 2015a, and a basic consensus mechanism ensures that each node adopts the longest valid blockchain it sees from its peers. The full broadcasting approach ensures rapid dissemination of new blocks across the network. The list of parameters are detailed in Table 1.

Table 1: List of simulation parameters

Parameter	Value	Description
Number of Nodes	5	Total number of nodes in the network (including honeypot and normal nodes).
Honeypot Nodes	2	Number of nodes configured to act as honeypots (first two nodes).
Simulation Rounds	10	Number of simulation cycles to run.
Event Detection Rate	0.5	Probability that a honeypot detects a suspicious event in a round.
Genesis Block Index	1	Starting index of the blockchain; each chain begins with a single genesis block.
Broadcasting Type	Full	Each node sends mined blocks to all peers directly (full peer-to-peer network).
Consensus Rule	Longest Chain	Nodes adopt the longest valid blockchain among their peers.
Attack rate		0.1 and 0.3

Figure 2 illustrates the variation in the number of suspicious or malicious events detected by honeypot nodes over multiple simulation rounds. Each bar on the graph corresponds to a specific simulation round, while the height of the bar represents the total number of honeypot events detected during that round. The purpose of this plot is to provide insights into the frequency and distribution of simulated attack activities targeting honeypot systems across time.

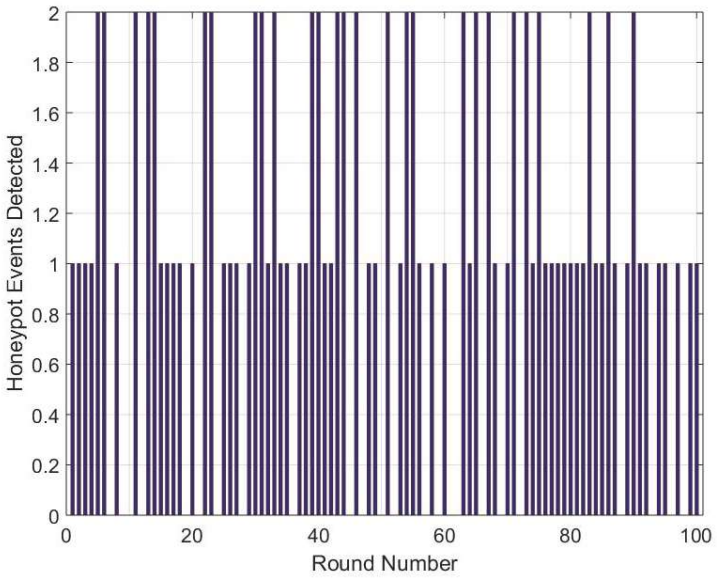

Figure 2: Number of Honeypot event detected vs. round number

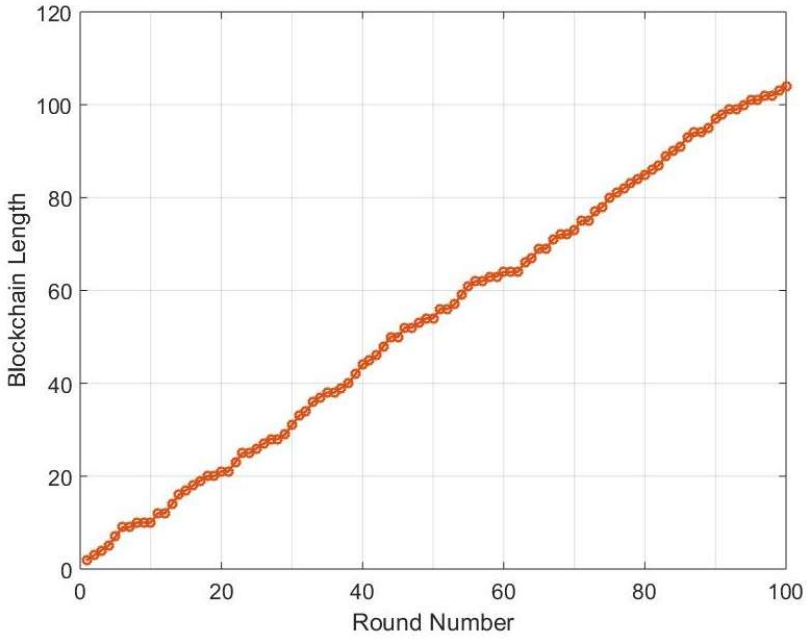

Figure 3: Blockchain Length vs. round number

As shown in the figure, the number of detected events fluctuates from one round to another, reflecting the probabilistic nature of attack simulation in the model. Since honeypot nodes are configured to randomly detect events with a certain probability (e.g., 50% per round), some rounds result in multiple detections, while others may have fewer or none. This randomness simulates real-world network conditions, where attack patterns are often irregular and unpredictable. Overall, this plot helps evaluate the responsiveness of the honeypot-based detection system by showing how effectively honeypots can identify potential threats during continuous operation. It also allows for the analysis of trends, such as whether certain rounds experienced more attacks and whether the honeypot configuration is sufficient to capture malicious activity over time.

Figure 3 presents the growth of the blockchain across different nodes as the simulation progresses over multiple rounds. The x-axis represents the round number, corresponding to each simulation cycle, while the y-

axis shows the length of the blockchain, i.e., the number of blocks each node holds at the end of each round. Each line on the plot represents a specific node, allowing for a comparative view of how individual blockchains evolve over time within the distributed network. The blockchain length increases whenever a node successfully mines a block or receives a valid block from its peers. In this simulation, honeypot nodes are more likely to generate new blocks, as they actively detect suspicious events and package them into blocks for broadcasting. Normal nodes, while not generating events themselves, still receive and validate blocks, contributing to the overall growth of their chains. The figure highlights how blockchain propagation and consensus work in a peer-to-peer honeypot network. Although block generation is event-driven and occurs primarily at honeypot nodes, the full broadcasting mechanism ensures that other nodes remain synchronized by adopting newly mined blocks. Additionally, the implementation of a simple consensus rule—where nodes adopt the longest valid chain from their peers—helps maintain consistency and resilience across the network.

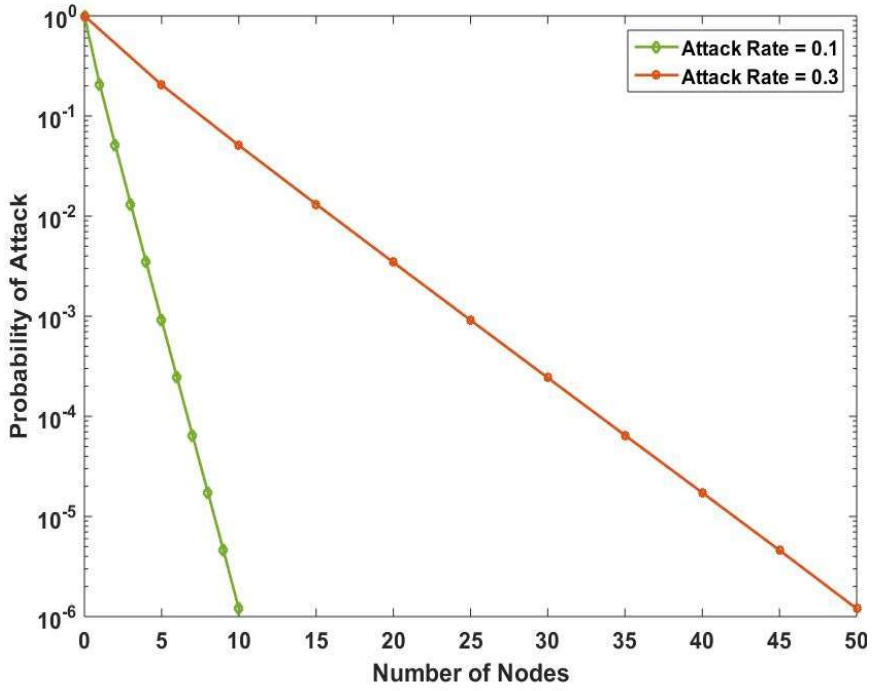

Figure 4: Probability of attack vs. Number of nodes

A 51% attack on a blockchain refers to a scenario in which a single individual or a group of colluding entities gains control over more than 50% of the network's computational power, also known as the mining power or hash rate in Proof of Work (PoW) systems, or the majority of the voting power in Proof of Stake (PoS) systems [14]. The control gained through this majority stake can enable the attacker to perform several malicious activities that would undermine the integrity and security of the blockchain. These activities include the ability to double-spend tokens, reverse transactions, and halt the confirmation of new transactions, disrupting the normal functioning of the network and eroding the trust placed in it by users. Essentially, a 51% attack allows the malicious actors to manipulate the blockchain's consensus mechanism, making it difficult for other participants to trust the validity of transactions and blocks being added to the chain.

Figure 4 explores the relationship between network size and the security of blockchain systems by analyzing how the number of nodes in the network influences the probability of a 51% attack. This analysis provides valuable insights into the importance of decentralization as a defense against malicious attacks. At the outset, when the network consists of only a small number of nodes, the attack probability is 1, which indicates that the system is completely vulnerable to a 51% attack. This high probability reflects the ease with which an attacker can take control of the majority of the network's power, as the concentration of computational resources or voting power is minimal and easily exploitable.

However, as the network grows in size and the number of nodes increases, the probability of a successful attack decreases sharply. By the time the network expands to 50 nodes, the probability of an attack falls dramatically to as low as 0.0000012. This significant drop in the attack probability illustrates the core principle that larger blockchain networks, which have a more distributed and decentralized distribution of computational resources or voting rights, become increasingly resistant to attacks. The increased number of participants, each contributing to the network's consensus process, makes it exponentially more difficult for any single entity or group to dominate the network and manipulate its operations.

Moreover, the data from the figure also highlights that while the attack rate remains at 0.3 in some instances, providing a baseline or context for the overall frequency of attacks, the most critical factor in enhancing blockchain security is the level of decentralization. The findings emphasize that the more distributed the network's resources and control, the less feasible it becomes for attackers to carry out a 51% attack or other types of manipulation. This aligns with existing literature on blockchain security, which consistently emphasizes that decentralization is one of the most effective defense mechanisms against attacks. A larger, more decentralized blockchain network is inherently more secure, as it becomes exponentially harder for malicious actors to coordinate and execute an attack that would have significant consequences. In conclusion, the analysis reinforces the idea that decentralization serves as the cornerstone of blockchain security. By increasing the number of nodes and ensuring that power and control over the network are distributed across a broader group of participants, the likelihood of a successful 51% attack or similar attacks diminishes drastically. This highlights the importance of scaling blockchain networks to enhance their security and resilience against potential threats, making the blockchain a more trustworthy and reliable system for its users.

5. Conclusion

In this paper, we explored the growing importance of blockchain technology in securing decentralized systems and examined its vulnerabilities, particularly the threat of 51% attacks and other malicious manipulations. We demonstrated that while blockchain's decentralized nature offers inherent security benefits, it remains susceptible to attacks when the network's computational power or voting control is concentrated in the hands of a few entities. The analysis highlighted the significant role of network size and decentralization in mitigating the risk of such attacks, with larger, more distributed networks being much more resilient to security breaches. Furthermore, we proposed the integration of blockchain technology with dynamic honeypots to enhance cybersecurity by proactively detecting and responding to threats. By utilizing a decentralized, immutable ledger system, blockchain can help maintain the integrity of honeypot systems, ensuring that data collected from attacks remains secure and tamper-proof. The combination of blockchain's cryptographic properties and honeypot mechanisms creates a robust framework for detecting, analyzing, and mitigating cyber threats, addressing many of the limitations faced by traditional security systems.

Ultimately, this research underscores the importance of scalability and decentralization in blockchain systems as essential components of security. As blockchain technology continues to evolve, understanding its potential vulnerabilities and implementing effective countermeasures will be crucial to ensuring its integrity in diverse applications, from cryptocurrencies to secure data sharing and beyond. By focusing on enhancing decentralization and integrating advanced security techniques like dynamic honeypots, we can build stronger, more resilient blockchain systems capable of withstanding the increasingly sophisticated cyber threats of the future.

References

1. George, A. Shaji, T. Baskar, and P. Balaji Srikaanth. "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors." *Partners Universal International Innovation Journal* 2, no. 1 (2024): 51-75.
2. Javadpour, Amir, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaïd. "A comprehensive survey on cyber deception techniques to improve honeypot performance." *Computers & Security* 140 (2024): 103792.
3. Touch, Sereysethy, and Jean-Noël Colin. "A comparison of an adaptive self-guarded honeypot with conventional honeypots." *Applied Sciences* 12, no. 10 (2022): 5224.

4. Vinod, S., C. Pandi, S. Sheik Dhanveer Hussain, C. Pavithran, M. Arjun Sathish, and R. S. Tejas. "Distributed Honey pot Based on Block chain." In *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, pp. 205-207. IEEE, 2024..
5. Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-peer Networking and Applications* 14, no. 5 (2021): 2901-2925.
6. Liu, Songsong, Pengbin Feng, Jiahao Cao, Xu He, Tommy Chin, Kun Sun, and Qi Li. "Consistency is All I Ask: Attacks and Countermeasures on the Network Context of Distributed Honeypots." In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 197-217. Cham: Springer International Publishing, 2022..
7. Wang, Xiran, Leyi Shi, Chi Cao, Weixin Wu, Zhihao Zhao, Ye Wang, and Kai Wang. "Game analysis and decision making optimization of evolutionary dynamic honeypot." *Computers and Electrical Engineering* 119 (2024): 109534..
8. Limouchi, Elnaz, and Imad Mahgoub. "Reinforcement learning-assisted threshold optimization for dynamic honeypot adaptation to enhance iobt networks security." In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1-7. IEEE, 2021..
9. Pittman, Jason M., Kyle Hoffpauir, Nathan Markle, and Cameron Meadows. "A taxonomy for dynamic honeypot measures of effectiveness." *arXiv preprint arXiv:2005.12969* (2020).
10. Shrimali, Bela, and Hiren B. Patel. "Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities." *Journal of King Saud University-Computer and Information Sciences* 34, no. 9 (2022): 6793-6807.
11. Vaigandla, Karthik Kumar, RadhaKrishna Karne, Mounika Siluveru, and Madhavi Kesoju. "Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications." *Mesopotamian journal of Cybersecurity* 2023 (2023): 73-84.
12. Nishad, Neharika, and Rahul Singh. "Honeypot deployment: A blockchain-based distributed approach." *International Journal of Intelligent Communication and Computer Science* 2, no. 1 (2024): 72-81.
13. Tiwari, Aparna, and Dinesh Kumar. "Securing Networks with ConvLSTM-Based Traffic Prediction and Attention Mechanism for Intrusion Detection." *International Journal of Engineering* (2024).
14. Nishad, Neharika, and Rahul Singh. "Enhancing security with a distributed honeypot system based on blockchain: A mathematical attack analysis." *International Journal of Intelligent Communication and Computer Science* 2, no. 2 (2024): 17-26.