Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Blockchain-based Reputation System for Smart Farm Anomaly Detection and Prevention

Ahmed Abubakar Aliyu[1, 2], Shamsuddeen Umaru Adamu[2], Abubakar Muazu Ahmed[2], and Ezekia Gilliard[3]

[1]School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072

[2]Department of Secure Computing, Faculty of Computing, Kaduna State University, Kaduna, Nigeria 800283

[3]Mwalimu Julius K. Nyerere University of Agriculture and Technology Butiama, Tanzania 976

ahmed.aliyu@kasu.edu.ng[1]

Abstract

While smart farming is becoming increasingly popular as a way to improve the efficiency and sustainability of agroecosystems and global food security, its vulnerability to cyber-attacks is rapidly increasing. A distributed reputation system can help detect and prevent malicious activities by tracking the reputation of IP addresses of devices, products, and entities in a smart farming system, thereby enhancing its security and trust. In this paper, we propose a blockchain-based reputation system for IP addresses in smart farms for real-time intrusion detection and prevention. The study uses the Ethereum blockchain smart contracts, Oracles, Intrusion Detection System (IDS), and a Proof-of-Reputation (PoR) consensus mechanism. The system was evaluated on two datasets, the Spamhaus Blocklist, and the Malware Domain List datasets. It achieved high accuracy, recall, and precision rates, F1 score, as well as low false positive and false negative rates. This shows that the proposed system has high potential to be an effective tool for improving malware detection and prevention in real-time, creating a trusted supply chain for a smart farming ecosystem against a wide range of attack types, including denial-of-service attacks, probe attacks, and user-to-root attacks.

Keywords: Blockchain, Reputation System, Intrusion Detection and Prevention, Smart Farm.

1. Introduction

Smart Farming as an integral component of the Internet of Things (IoT), is the application of information and data technologies to optimize complex farming systems, with a focus on data availability and how farmers can use the information intelligently (Alwis et al., 2022). Although smart farms are becoming increasingly popular as a way to improve the efficiency and sustainability of agriculture and general food security, the connected devices make smart farms vulnerable to cyber-attacks. This paper proposes a blockchain-based reputation system that uses blockchain technology to track and manage the reputation of IP addresses of connected devices, and entities in smart farms. Blockchain is a distributed ledger technology that can be used to create secure and tamper-proof records (Aliyu et al., 2024). Blockchain-based reputation system could be used to block IP addresses known to be associated with malware, block devices that have been used to launch attacks on smart farms in the past, isolate devices with low reputation scores from the rest of the smart farm network, and flag smart farm products that have been manufactured or

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

distributed by devices with low reputation scores (Jamal et al., 2023).

The current gap in research on blockchain-based reputation systems and smart farm security is that most existing systems focus on a specific aspect of smart farm security, such as device security or product security (Khezr et al., 2022). Thus, there is a need for more comprehensive systems that can address a wider range of security threats (Z. Wang et al., 2023). For example, some existing systems focus on tracking the reputation of IoT devices (Tu et al., 2022). Although these systems can be used to identify and block devices that have been used to launch an attack in the past, however, they do not address other security concerns, such as malware attacks or attacks on the IoT network. Other existing systems are designed to track the reputation of some IoT products as well as flagging the products that have been produced or distributed by devices with a low reputation score (Liao & Cheng, 2023). These systems do not address other security threats, such as attacks on the smart farm supply chain or attacks on the smart farm data (Rodrigues et al., 2022). As a result, there is a significant need for a blockchain-based reputation system that is able to address a broader scope of security threats. This system is aimed at tracking the reputation of IP addresses of devices, products, and entities on a smart farming system (Dhanaraju et al., 2022), and the information gathered can then be used to detect and prevent a wider range of malicious behaviors. In addition to being more comprehensive, the system will also be more secure, tamper-proof, and transparent than traditional security solutions (T. Wang et al., 2023). Figure 1 illustrates the blockchain-based distributed reputation process.

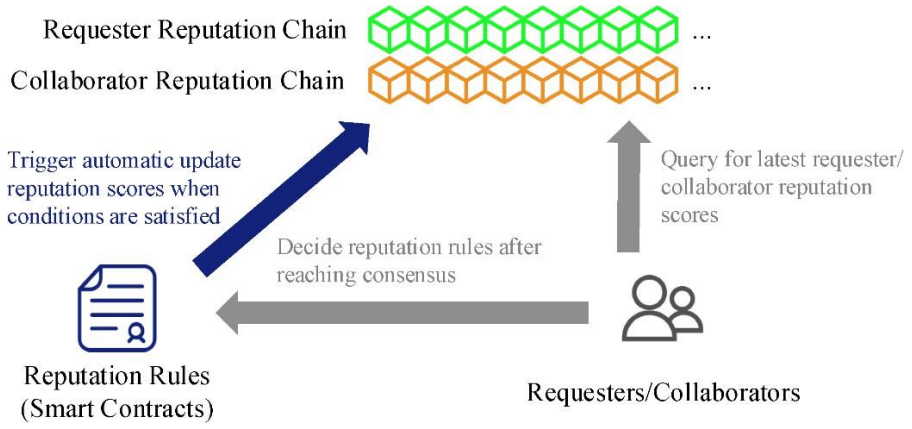

Figure 1. A Reputation System Using Blockchain (T. Wang et al., 2023)

The aim of this study is to design and implement a blockchain-based reputation system for intrusion detection and prevention in smart farms. The study will contribute to the existing body of knowledge on blockchain-based reputation systems for smart farms and the IoT as a whole, and will provide a valuable resource for farmers and other stakeholders interested in using blockchain technology to improve the security of smart farms. Finally, this paper will discuss the design and implementation of the system, as well as the evaluation of its security performance.

2. Related Work

IoT devices are vulnerable to a variety of attacks, including malware, phishing, man-in-the-middle (MitM), denial of service (DoS) and physical attacks as categorized in Figure 2. Because IoT devices are often designed to be easy to access and use, they can be more vulnerable to cyber-attacks.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

For instance, the default passwords on many IoT devices are weak or easy to guess. Secondly, IoT devices often lack basic security features such as authentication and encryption, making it easier for attackers to intercept or modify data sent between IoT devices (Rekha et al., 2023). In addition, IoT devices are often deployed in large numbers, making them an attractive target for attackers, and are often connected to the Internet without the necessary security protections, leaving them open to remote attack. Security researchers have analyzed different perspectives to understand the current state of IoT and identify existing challenges. The most common issues found in IoT devices include insecure network interfaces, inadequate authentication, insecure web services, poor privacy controls, inadequate security configurability, insecure software and poor physical security (El-Kady et al., 2023).

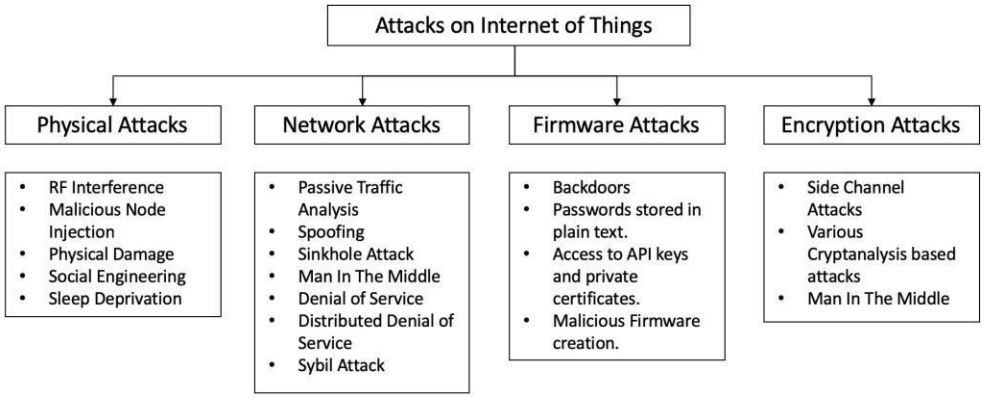

Figure 2. Cyber-attacks that IoT devices are vulnerable to

A recent review of the fundamentals, components, and security challenges of smart farming has been published by Alam (2023), which provides security and reliability through a blockchain-based paradigm for the secure integration of smart farming components. Also, a number of researchers have examined existing IoT technologies used in smart sustainable agriculture to identify architectural components that could support the development of smart agriculture platforms (AlZubi & Galyna, 2023). They assess the state of research and development, look at the current information landscape, and propose an IoT and Artificial Intelligence (AI) framework as a starting point for smart farming in their work. Another recent study by Chatterjee et al. (2023) proposed a structure based on blockchain smart contracts, where all entities involved in the blockchain-based supply chain network manage transactions between participants. In this study, three criteria were used to assess the overall effectiveness of the system: transaction efficiency, system risk reduction, and trust between participants. Furthermore, a study presents a framework that improves the security and privacy of smart farms by using the decentralized properties of the blockchain (Aliyu & Liu, 2023). Using the Ethereum smart contract, which enables the automated execution of pre-defined rules and a proof-of-concept implementation, the system stores and processes data obtained from IoT-connected devices installed in smart farms through a distributed ledger structure, providing secure and tamper-proof data storage while ensuring data validity and integrity. Some other researches such as that of M et al. (2023) have used an IoT method that monitors agricultural fields using PIR and ultrasonic sensors, which have the disadvantage of having a smaller detection range than LiDAR sensors. They used an intrusion detection system based on LiDAR sensors placed outside the fence to detect animal intrusion at the perimeter of the farm. The study also produces a graphical representation of the LiDAR to show the state of

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

field conditions. Many other researches such as that of (Chaganti et al., 2022; Aliyu et al., 2023; & Akella et al., 2023) have integrated blockchain technology to develop cyber secure systems for smart farming and the IoT recently.

Similarly, recent research has conducted a thorough assessment with the aim of exploring and evaluating the application of Blockchain in the context of Distributed Trust and Reputation Management Systems (DTRMS) (Bellini et al., 2020). The research presents taxonomies for blockchain and DTRMS, as well as a formal concept analysis. Moreover, another study has provided some innovative solutions for an IoT-compatible trust and reputation system based on fog computing (Alzoubi et al., 2022). In the study, each IoT device measures trust towards other IoT devices using fog nodes and only interacts with a device if it meets a specified trust threshold. In addition, a number of researchers have developed a blockchain-enabled distributed cloud storage (DCS) architecture that maintains the traceability and tamper-proofness of reputation-related data, as well as a service credibility quantification method based on rating screening to limit the influence of outliers (Dong et al., 2023). A stochastic mechanism was developed to define storage resource changes and quantify the survival probability of Cloud Service Providers (CSPs). Although many other studies have applied reputation systems in various applications such as that of (Debe et al., 2019; Oliveira et al., 2020; Gyawali et al., 2020; Zhang & Huang, 2023a; Yan et al., 2023 & El Mezouari & Omary, 2023), however, there is still a need for more research on blockchain-based reputation systems for the IoT given that existing systems typically focus on a specific aspect of smart farm security, such as device security or product security. There is a need for more comprehensive systems that can address a wider range of security threats.

3. Methodology

The proposed system comprises the following key components designed to enhance network security and manage reputations effectively:

i. **Smart Contracts (SC):** These are self-executing contracts deployed on a blockchain platform. Smart contracts encode the rules and procedures governing the reputation system, including algorithms for reputation calculation and criteria for blocking IP addresses. We can define a smart contract as:

$$SC = \langle Rules, Logic, Conditions \rangle \quad (1)$$

Where, ***Rules*** represent the reputation calculation rules, ***Logic*** encapsulates the decision-making processes, and
Conditions outline triggering events for actions like IP blocking.

ii. **Oracles** (O): These are trusted external entities that provide data to smart contracts. In the context of the reputation system, oracles ***O*** furnish real-time information about the reputations of IP addresses. An oracle ***O*** can be described by:

$$O = \langle Data\ Provider, Data\ Feed, Trust\ Model \rangle \quad (2)$$

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Where, ***Data Provider*** is the entity supplying reputation data, ***Data Feed*** is the mechanism for delivering this data to smart contracts, and ***Trust Model*** outlines the reliability criteria.

iii. ***Reputation Database (RDB):*** This stores the reputation scores of all IP addresses and is integrated either as a smart contract or a separate database linked to the blockchain. Mathematically, the reputation database ***RDB*** can be represented as:

$$RDB = \{(IP_i, \text{Reputation } (Score\ ) / i = 1,2,\ldots,n\} \quad (3)$$

Where IP_i denotes the i-th IP address and ***Reputation*** $Score_i$ denotes its corresponding reputation score.

iv. ***Intrusion Detection System (IDS):*** Deployed within the network, the IDS monitors network traffic and generates alerts in real-time upon detecting suspicious activities. We characterized the IDS by:

$$IDS = \langle Monitoring\ Algorithm, Alert\ Generation\ Logic \rangle \quad (4)$$

Here, ***Monitoring Algorithm*** details the methods for traffic analysis, and ***Generation Logic*** specifies the criteria for generating alerts.

v. ***Firewalls (F):*** These serve as the mechanism to block IP addresses with lower reputation scores from accessing the network. We define the firewall ***F*** as:

$$F = \langle Blocking\ Rules, Access\ Control\ Policies \rangle \quad (5)$$

Where ***Blocking Rules*** outline conditions for denying access based on reputation scores, and ***Access Control Policies*** specify rules governing network access as shown in Figure 3.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

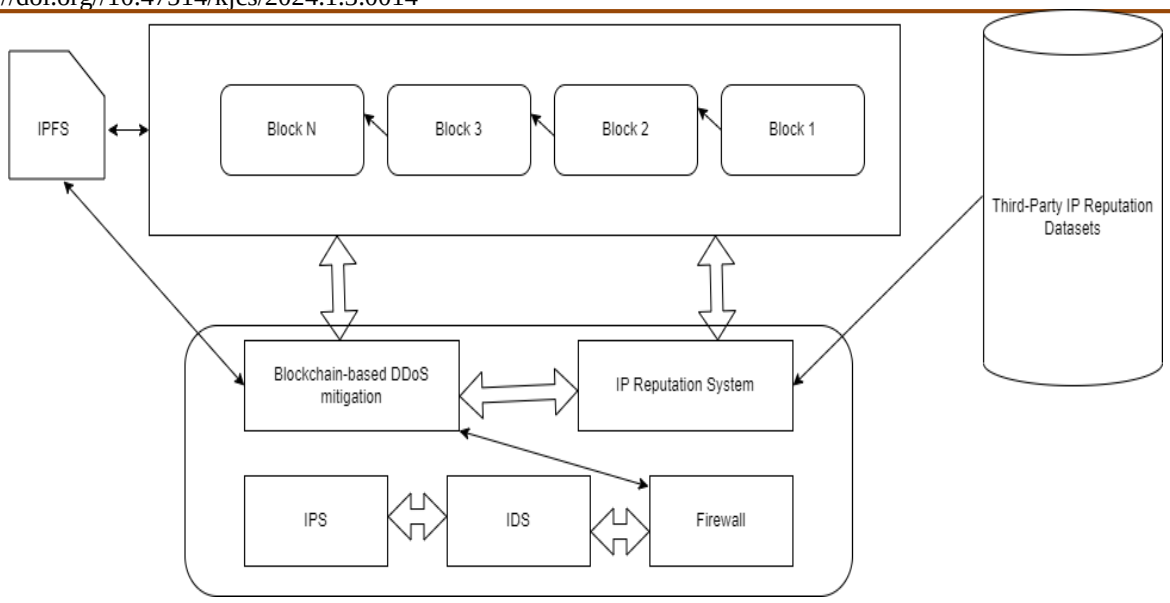

Figure 3. The Proposed Reputation System

The proposed system can be used to detect and prevent malware attacks on smart farms. The IDS is deployed on the network and configured to generate alerts in real-time. The alerts are sent to a smart contract that calculates the reputation score of an IP address based on the alerts received. If the reputation score falls below a certain threshold, the smart contract triggers the blocking mechanism (Firewall) that prevents the IP address from accessing the network as shown in Figure 3. The system uses weighted reputation scoring, which is the algorithm that assigns a weight to each piece of evidence about a reputation entity, such as the type of evidence, the source of the evidence, and the timeliness of the evidence (Zaccagni et al., 2022). The weights are used to calculate a weighted average reputation score for the entity. The reputation scores are then stored in the reputation database to ensure that all nodes in the system agree on the reputation of IP addresses, we employed a consensus mechanism. Proof-of-Work (PoW) and Proof-of-stake (PoS) are the two consensus mechanisms which reputation systems often use (Ipchi Sheshgelani et al., 2022). PoW is the consensus mechanism used by Bitcoin and other early blockchains (Sapra et al., 2023). It works by requiring nodes to solve complex mathematical problems in order to add new blocks to the blockchain. Although this process could be computationally expensive and requires a lot of energy, it is very secure and resistant to attack. PoS on the other hand, is a more energy-efficient consensus mechanism that does not require nodes to solve complex mathematical problems (Abbasi et al., 2023). Instead, nodes are rewarded for staking their tokens on the network. The more tokens a node stakes, the more likely it is to be selected to add the next block to the blockchain. This makes PoS less secure than PoW, but it is also more energy-efficient and scalable. The preferred consensus method is usually determined by a number of variables, including the required level of security, scalability, and efficiency (Gilliard et al., 2023). For blockchain-based reputation systems for IP addresses on smart farms, it is critical to select a consensus method that is both secure and scalable (Zubaydi et al., 2023). Moreover, Proof-of-Reputation (PoR) is a new reputation-based consensus algorithm that addresses the security, performance, and centralization concerns of existing permissionless blockchain consensus algorithms. PoR achieves a balance between scalability, security, and decentralization by combining BFT, reputation, reward, and

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

punishment mechanism (Zhang & Huang, 2023b). Experimental results show that PoR is highly performant and scalable for both permissionless and permissioned blockchains, making this proposed approach to choose the PoR consensus mechanism. Our proposed system makes a number of contributions to the field of distributed reputation systems. For example, the proposed system presents a new way to use oracles to collect data about the reputation of IP addresses. It also proposes a new way to use smart contracts to calculate the reputation score of IP addresses and to block IP addresses with low reputation scores. These contributions have the potential to improve the security and efficiency of smart farms and distributed IoT networks. In furtherance, the proposed system is integrated with an IDS for a stronger malware detection in real-time (Abubakar et al., 2023). The system also uses a new PoW consensus mechanism that is designed to be more efficient and secure than existing the consensus mechanisms. This is important for a system designed to protect smart farms, which are often large and complex operations, in addition to the new reputation scoring algorithm, which can also effectively identify and block malicious IP addresses.Datasets are needed to train machine learning algorithms to detect malicious domains and IP addresses, hence this study uses machine learning training due to the time factor, as larger datasets with deep learning approach can take a long time to train the system, while simpler algorithms can provide equivalent results. Similarly, a binary classification approach was used to label all entries as either benign or malicious based on the nature of the data, with benign meaning no malicious activity is present (Gilliard, Liu, & Aliyu, 2024). The study uses two synthetic datasets; the Spamhaus Blocklist and Malware Domain List (MDL) datasets (Rao et al., 2021). The first system's evaluation was carried out using the metrics; Accuracy, Recall, Precision, F1 Scores, AUC, False Positive, and False Negative Rates. However, it is important to note that evaluation of this system is a challenging task, as it is difficult to obtain a complete and accurate set of malicious IP addresses. In addition, the system may need to be evaluated over a long period of time to ensure that it is effective in detecting new and emerging malware threats. Also, determining the level of maliciousness of websites may require retraining, thus, the study employed the Spamhaus Blocklist and MDL IP address datasets to test the effectiveness of the system. The Spamhaus Blocklist is a larger dataset containing over 2 million IP addresses while MDL is a smaller dataset, containing around 100,000 IP addresses that is more focused on detecting malware domains

The Ethereum blockchain is selected given that when certain conditions are met, its smart contract deterministically executes unambiguous code without the need to wait for a human to interpret or negotiate the outcome, eliminating the need for trusted intermediaries. The smart contracts implement the logic of the reputation system, such as how reputation is calculated and how IP addresses are blocked as shown in Figure 3. The confusion matrix formulas for the five metrics are:

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP+TN}}{\boldsymbol{TP+TN+FP+FN}} \quad (7)$$

Where TP = True Positive

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

TN = True Negative
FP = False Positive
FN = False Negative

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

$$F1\ Score = \frac{2 \times Precision \times Recall}{Precision+Recall} \quad (9)$$

For the true positive value and calculating the AUC,
we say Given:

$$TP = 1 - FN = 1 - 0.015 = 0.985$$

Now, we can compute the AUC using the ROC curve formula:

$$AUC = \frac{1}{2} X\ TPR_1 \times FPR_2 + FPR_3 + \ldots (10)$$

Assuming the False Positive Rate (FPR) varies from 0 to 1:

$$FPR_1 = 0, \quad FPR_2 = 0.009, \quad FPR_3 = 1$$

And the True Positive Rate (TPR) varies from 0 to 1:

$$TPR_1 = 0, \quad TPR_2 = 0.985, \quad TPR_3 = 1$$

$$AUC = \frac{1}{2} \times (0 \times 0.009 + 0.985 \times 0.009 + 1 \times 1)$$

$$AUC = \frac{1}{2} \times (0 + 0.008865 + 1) = \frac{1}{2} \times 1.008865 = 0.5044325$$

$$Weighted\ average\ reputation\ score = \frac{(w1 * r1 + w2 * r2 + \ldots + wn * rn)}{(w1 + w2 + \ldots + wn)}$$

where:

- ***wi*** is the weight assigned to the ***i-th*** piece of evidence
- ***ri*** is the reputation score of the entity based on the ***i-th*** piece of evidence

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

4. Results and Discussion

The system stores data about IP addresses, including the number and types of malicious activity associated with each address, the dates and times of the malicious activity, and the sources of information about the malicious activity. Based on this information, the system calculates a reputation score for each IP address and tracks the history of malicious activity associated with each address to identify trends and patterns. Specifically, the system calculates a reputation score for each IP address based on the number of times it has been associated with malicious activity. For example, an IP address that has been associated with a large number of malware attacks would have a lower reputation score than an IP address that has only been associated with a few phishing attacks. This information is used to identify IP addresses associated with new and emerging malware threats.

In summary, the proposed system tracks the sources of information about malicious activity associated with an IP address, which it uses to assess the credibility of the information and identify IP addresses that are associated with a high level of confidence. This information is used by the system to block malicious IP addresses and protect smart farms from attack. The system was evaluated against the five-performance metrics and achieved the results shown in Table 1, and Figures 4 and 5.

Table 1. Tests results

Metric	Spamhaus Blocklist	Malware Domain List
Accuracy	99.5%	99.7%
Precision	99.2%	99.4%
Recall	98.9%	99.1%
F1 score	99.1%	99.3%
AUC	0.998	0.999
False positive rate (FPR)	0.5%	0.3%
False negative rate (FNR)	1.1%	0.9%

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 593-606
https://doi.org//10.47514/kjcs/2024.1.3.0014

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

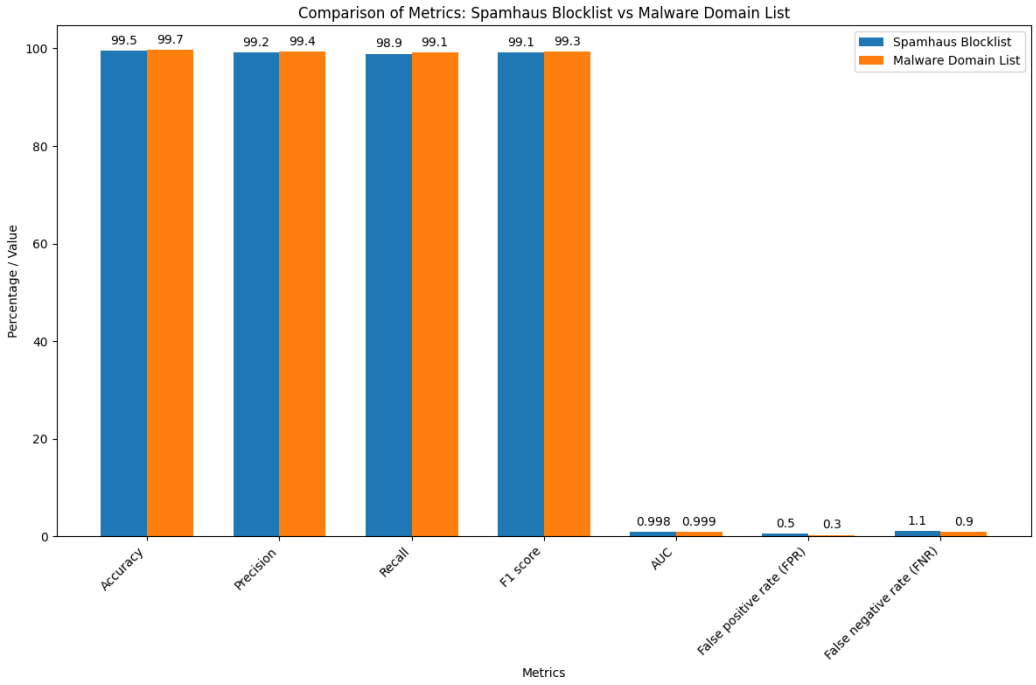

Figure 4. Results graphical representation

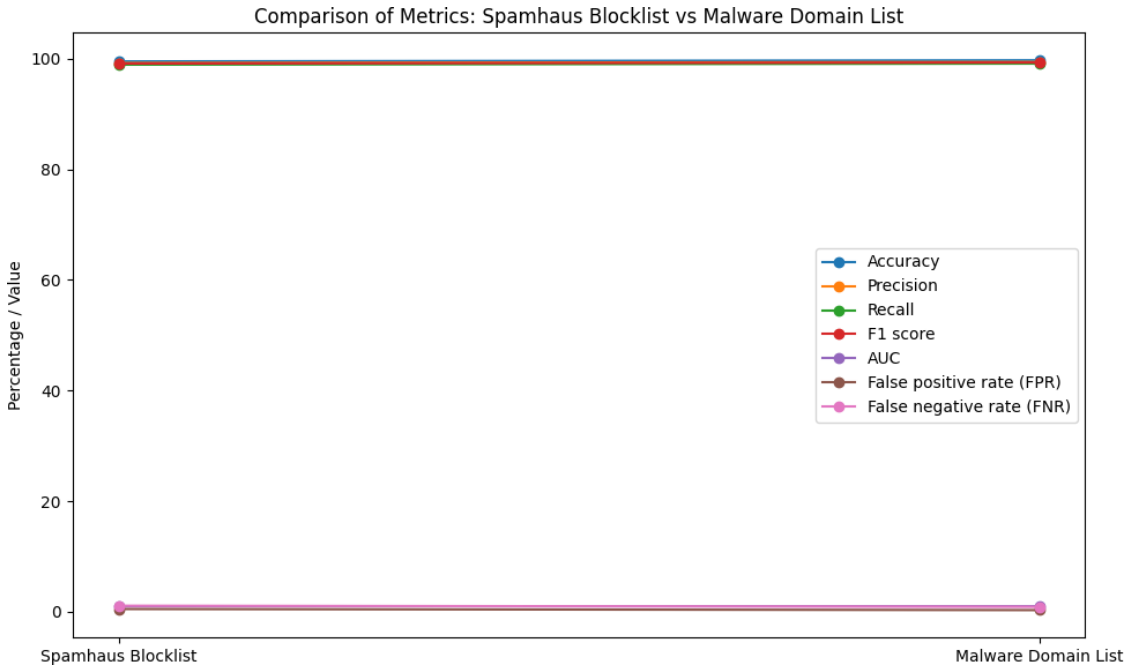

Figure 5. Results graphical display

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The system uses a configured IDS to generate alarms in real-time and firewalls to protect Smart Farms from malware attacks by monitoring the reputation of IP addresses known to be associated with malware (Shah et al., 2022). If the system identifies a low-reputation IP address attempting to enter a Smart Farm, it blocks the IP address, preventing malware from attacking and bad actors from accessing Smart Farms. If it identifies one of these IP addresses attempting to access a Smart Farm, it blocks the IP address, preventing the bad actor from further attacks. It tracks the number of times a device has been infected with malware and the number of times it has been used to launch an attack. If a device has a low reputation score, it is isolated from the rest of the Smart Farm network, preventing it from being used to launch further attacks. This can be used to create a trusted supply chain for Smart Farm products by ensuring that the products are safe and reliable. For example, the system could track the IP addresses of equipment used in the production and distribution of Smart Farm products. If it detects that a device with a low reputation score is involved in the production or distribution of a smart farm product, it will flag the product as suspicious. It is also important to note that the datasets used are not mutually exclusive. For example, it is possible for an IP address to appear on both the Spamhaus Blocklist and the MDL. In such cases, the system may choose to block the IP address based on the dataset it considers more reliable.

5. Conclusion

This paper presents a novel blockchain-based reputation system that detects and prevents malware attacks on smart farms by monitoring the reputation of IP addresses known to be associated with malware. It uses Ethereum blockchain and smart contracts to implement the logic of the reputation system, and oracles to provide data on the reputation of IP addresses. Based on the results obtained, the proposed system has the potential to effectively detect and block malicious IP addresses in smart farms. These results are based on a comprehensive evaluation of the system in all attack scenarios. Using an IDS, the system was able to generate alerts in real-time and then use firewalls to block all malicious IP addresses containing a wide range of attack types, including denial of service attacks, probe attacks and user-to-root attacks, while generating only a small number of false positives. The limitation of the system is that the datasets used to evaluate its performance are synthetic, which means they may not be representative of other real-world data (Gilliard, Liu, Abubakar Aliyu, et al., 2024). Real-world data is often more complex and noisier than synthetic data, which can make it more difficult for the system to detect malicious IP addresses. The system may not be able to detect all new and emerging malware threats and may also be vulnerable to adversarial attacks, in addition to being computationally expensive to deploy and maintain. If the IP reputation score is above a certain threshold, the IP address will not be blocked and will be allowed to access the network. This could be because the IP address has never been associated with malicious activity, its reputation has been forgiven, or it is associated with a large number of legitimate users. Moreover, integration with the IDS is essential because no reputation system is perfect, so the reputation system is part of a comprehensive security strategy that includes other measures such as the firewalls. In addition, the reputation threshold can be tuned to the specific needs of the users for a more comprehensive solution. It is also important to regularly update the reputation system to reflect changes in the threat landscape.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Statements and Declarations

Conflict of Interest: This research declares no conflict of interest.

References:

Abbasi, M., Prieto, J., Plaza-Hernández, M., & Corchado, J. M. (2023). A Novel Aging-Based Proof of Stake Consensus Mechanism. In L. F. Castillo Ossa, G. Isaza, Ó. Cardona, O. D. Castrillón, J. M. Corchado Rodriguez, & F. De la Prieta Pintado (Eds.), *Trends in Sustainable Smart Cities and Territories* (pp. 49–61). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-36957-5_5

Abubakar, A. A., Liu, J., & Gilliard, E. (2023). An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. *Electronics Letters*, *59*(18), e12888. https://doi.org/10.1049/ell2.12888

Akella, G. K., Wibowo, S., Grandhi, S., & Mubarak, S. (2023). A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture. *Big Data and Cognitive Computing*, *7*(2), Article 2. https://doi.org/10.3390/bdcc7020086

Alam, S. (2023). Security Concerns in Smart Agriculture and Blockchain-based Solution. *2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)*, 1–6. https://doi.org/10.1109/OTCON56053.2023.10113953

Aliyu, A. A., & Liu, J. (2023). Blockchain-Based Smart Farm Security Framework for the Internet of Things. *Sensors*, *23*(18), Article 18. https://doi.org/10.3390/s23187992

Aliyu, A. A., Liu, J., & Gilliard, E. (2023). Blockchain-Based Poisoning Attack Prevention In Smart Farming. *Scientific and Practical Cyber Security Journal*, *7*(2), 38–53.

Aliyu, A. A., Liu, J., & Gilliard, E. (2024). DETERMINANTS OF INTENTION TO ADOPT BLOCKCHAIN TECHNOLOGY IN NIGERIA. *Science World Journal*, *19*(2), Article 2. http://dx.doi.org/10.4314/swj.v19i2.25

Alwis, S. D., Hou, Z., Zhang, Y., Na, M. H., Ofoghi, B., & Sajjanhar, A. (2022). A survey on smart farming data, applications and techniques. *Computers in Industry*, *138*, 103624. https://doi.org/10.1016/j.compind.2022.103624

Alzoubi, Y. I., Al-Ahmad, A., & Kahtan, H. (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. *Computer Communications*, *182*, 129–152. https://doi.org/10.1016/j.comcom.2021.11.005

AlZubi, A. A., & Galyna, K. (2023). Artificial Intelligence and Internet of Things for Sustainable Farming and Smart Agriculture. *IEEE Access*, *11*, 78686–78692. https://doi.org/10.1109/ACCESS.2023.3298215

Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey. *IEEE Access*, *8*, 21127–21151. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2969820

Chaganti, R., Varadarajan, V., Gorantla, V. S., Gadekallu, T. R., & Ravi, V. (2022). Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet*, *14*(9), Article 9. https://doi.org/10.3390/fi14090250

Chatterjee, K., Singh, A., & Neha. (2023). A blockchain-enabled security framework for smart agriculture. *Computers and Electrical Engineering*, *106*, 108594. https://doi.org/10.1016/j.compeleceng.2023.108594

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Debe, M., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2019). IoT Public Fog Nodes Reputation System: A Decentralized Solution Using Ethereum Blockchain. *IEEE Access*, *7*, 178082–178093. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2958355

Dhanaraju, M., Chenniappan, P., Ramalingam, K., Pazhanivelan, S., & Kaliaperumal, R. (2022). Smart Farming: Internet of Things (IoT)-Based Sustainable Agriculture. *Agriculture*, *12*(10), Article 10. https://doi.org/10.3390/agriculture12101745

Dong, Q., Tang, J., Dang, S., Chen, G., & Chambers, J. A. (2023). Blockchain-Assisted Reputation Mechanism for Distributed Cloud Storage. *IEEE Systems Journal*, 1–12. https://doi.org/10.1109/JSYST.2023.3277194

El Mezouari, H., & Omary, F. (2023). Studying Consensus Mechanisms for Blockchain. In A. Idrissi (Ed.), *Modern Artificial Intelligence and Data Science: Tools, Techniques and Systems* (pp. 213–223). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33309-5_17

El-Kady, A. H., Halim, S., El-Halwagi, M. M., & Khan, F. (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. *Process Safety and Environmental Protection*, *173*, 384–413. https://doi.org/10.1016/j.psep.2023.03.012

Gilliard, E., Liu, J., Abubakar Aliyu, A., Juan, D., Jing, H., & Wang, M. (2024). Intelligent load balancing in data center software-defined networks. *Transactions on Emerging Telecommunications Technologies*, *35*. https://doi.org/10.1002/ett.4967

Gilliard, E., Liu, J., & Aliyu, A. A. (2023). Knowledge graph-guided object detection with semantic distance network. *Electronics Letters*, *59*(24), e13051. https://doi.org/10.1049/ell2.13051

Gilliard, E., Liu, J., & Aliyu, A. A. (2024). Knowledge graph reasoning for cyber attack detection. *IET Communications*, cmu2.12736. https://doi.org/10.1049/cmu2.12736

Gyawali, S., Qian, Y., & Hu, R. Q. (2020). Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology*, *69*(8), 8871–8885. IEEE Transactions on Vehicular Technology. https://doi.org/10.1109/TVT.2020.2996620

Ipchi Sheshgelani, M., Pashazadeh, S., & Salehpoor, P. (2022). Cooperative hybrid consensus with function optimization for blockchain. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03746-5

Jamal, A., Javed, M. U., Alrajeh, N., Bouk, S. H., & Javaid, N. (2023). Blockchain based reputation management, data storage and distributed revocation in vehicular energy networks in smart health care systems. *Cluster Computing*. https://doi.org/10.1007/s10586-023-04085-9

Khezr, S., Yassine, A., Benlamri, R., & Hossain, M. S. (2022). An Edge Intelligent Blockchain-Based Reputation System for IIoT Data Ecosystem. *IEEE Transactions on Industrial Informatics*, *18*(11), 8346–8355. IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2022.3174065

Liao, Z., & Cheng, S. (2023). RVC: A reputation and voting based blockchain consensus mechanism for edge computing-enabled IoT systems. *Journal of Network and Computer Applications*, *209*, 103510. https://doi.org/10.1016/j.jnca.2022.103510

M, K., S, U., C, M., Ravi, S., S, S., & R, T. K. (2023). An Integrated Security for Smart Farming and Monitoring System based on LiDAR Technology. *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, 761–767.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

https://doi.org/10.1109/ICEARS56392.2023.10085666

Oliveira, M. T. de, Reis, L. H. A., Medeiros, D. S. V., Carrano, R. C., Olabarriaga, S. D., & Mattos, D. M. F. (2020). Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications. *Computer Networks*, *179*, 107367. https://doi.org/10.1016/j.comnet.2020.107367

Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications*, *186*, 115742. https://doi.org/10.1016/j.eswa.2021.115742

Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, *80*, 3554–3559. https://doi.org/10.1016/j.matpr.2021.07.295

Rodrigues, B., Franco, M., Killer, C., Scheid, E. J., & Stiller, B. (2022). On Trust, Blockchain, and Reputation Systems. In D. A. Tran, M. T. Thai, & B. Krishnamachari (Eds.), *Handbook on Blockchain* (pp. 299–337). Springer International Publishing. https://doi.org/10.1007/978-3-031-07535-3_9

Sapra, N., Shaikh, I., & Dash, A. (2023). Impact of Proof of Work (PoW)-Based Blockchain Applications on the Environment: A Systematic Review and Research Agenda. *Journal of Risk and Financial Management*, *16*(4), Article 4. https://doi.org/10.3390/jrfm16040218

Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, *22*(3), 1094. https://doi.org/10.3390/s22031094

Tu, Z., Zhou, H., Li, K., Song, H., & Yang, Y. (2022). A Blockchain-based Trust and Reputation Model with Dynamic Evaluation Mechanism for IoT. *Computer Networks*, *218*, 109404. https://doi.org/10.1016/j.comnet.2022.109404

Wang, T., Ai, S., Cao, J., & Zhao, Y. (2023). A Blockchain-Based Distributed Computational Resource Trading Strategy for Internet of Things Considering Multiple Preferences. *Symmetry*, *15*(4), Article 4. https://doi.org/10.3390/sym15040808

Wang, Z., Zhang, S., Zhao, Y., Chen, C., & Dong, X. (2023). Risk prediction and credibility detection of network public opinion using blockchain technology. *Technological Forecasting and Social Change*, *187*, 122177. https://doi.org/10.1016/j.techfore.2022.122177

Yan, K., Ma, W., Yang, Q., Sun, S., & Wang, W. (2023). Info-Chain: Reputation-Based Blockchain for Secure Information Sharing in 6G Intelligent Transportation Systems. *IEEE Internet of Things Journal*, 1–1. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.3323011

Zaccagni, Z., Dantu, R., & Morozov, K. (2022). Maintaining Review Credibility Using NLP, Reputation, and Blockchain. *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 58–66. https://doi.org/10.1109/TPS-ISA56441.2022.00018

Zhang, T., & Huang, Z. (2023a). FPoR: Fair proof-of-reputation consensus for blockchain. *ICT Express*, *9*(1), 45–50. https://doi.org/10.1016/j.icte.2022.11.007

Zhang, T., & Huang, Z. (2023b). FPoR: Fair proof-of-reputation consensus for blockchain. *ICT Express*, *9*(1), 45–50. https://doi.org/10.1016/j.icte.2022.11.007

Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors*, *23*(2), Article 2. https://doi.org/10.3390/s23020788