KASU JOURNAL OF MATHEMATICAL SCIENCES (KJMS) VOL. 5, ISSUE 1, JUNE 2024
ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

KASU JOURNAL OF MATHEMATICAL SCIENCES

An Enhanced Intrusion Detection System for IoT DDoS Attack

[1,2]Ahmed Abubakar Aliyu, [1]Jinshuo Liu, [3]Ezekia Gilliard and [4]Wang Meng

[1]School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072
[2]Department of Computer Science, Faculty of Computing, Kaduna State University, Kaduna 800283, Nigeria
[3]Mwalimu Julius K. Nyerere University of Agriculture and Technology, Butiama, 976 Tanzania
Corresponding email: ahmed.aliyu@kasu.edu.ng

Abstract
Smart farming, as an integral part of the Internet of Things (IoT), is gaining popularity as a means of meeting the world's growing demand for food. There are many approaches for smart farms to use technology and connected devices. For example, from receiving real-time information on crop status and soil moisture to operating drones to assist with tasks such as spraying pesticides. However, the use of various internet-connected devices introduces some vulnerabilities in the smart farming ecosystem. Intruders can exploit these vulnerabilities to manipulate and remotely disrupt the flow of data from field sensors. This will have negative consequences, especially in high-risk situations such as harvesting, where real-time monitoring is required. This study uses both qualitative and quantitative approaches to analyse the intended research objectives for Denial of Service (DOS) attack mitigation in smart farms. Furthermore, the study presents an enhanced Intrusion Detection System (IDS) utilising disparate metrics to validate the performance and efficacy of the IDS deployed. Additionally, it asserts that distinct IDS methodologies achieve an accuracy of 0.95, precision of 0.92, recall of 0.90, F1 Score of 0.91, and ROC curve of 96. The study concludes that the application of the IDS measurement method can be effectively employed to resolve instances of Denial of Service (DOS).

Keywords: Smart Farming, Intrusion Detection Systems, DoS Attacks, Internet of Things.

1. Introduction
In recent years, the farming sector has made great strides in developing smart agriculture technologies. Agricultural development is by far one of the most effective tools for eradicating extreme poverty, improving collective well-being, and feeding an estimated 9.7 billion people by 2050 (Istiak & Khaliduzzaman, 2022). Agriculture is also critical to economic development, accounting for nearly 4% and in some developing countries more than 25% of global gross domestic product (GDP) (vanDijk et al., 2021). Although small-scale and artisanal farming has seen a resurgence in the last decade, many traditional farmers want to go further to increase productivity and yields that are comparable to other supply chains, and targeted automation is the way to go (Grogan, 2012). In addition, rapid population growth has significantly increased the demand for agricultural products and food. Therefore, the study of smart agricultural ecosystems and the adoption of new technologies will have a far-reaching impact on the global economy on a

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

large scale (Choi & Shin, 2023). The traditional technologies that have supported the farming sector do not meet this need and are outdated (Abubakar et al., 2023). Today, the agri-food industry is placing more emphasis on automation in almost all facets of farming and agricultural practices, from pre-planting to post-harvest, thereby increasing their efficiency. They use both web data and related materials or "things", i.e. IoT. IoT reduces human interaction with the farm by automating processes through a network of interconnected devices such as sensors and drones, robotic arms, etc. that can exchange messages without human intervention as agricultural production is being enhanced both numerically and qualitatively by IoT technology (Aliyu et al., 2023). However, the use of IoT for agricultural automation. Smart agriculture encompasses a wider range of technologies and practices than just IoT devices. Smart agriculture includes the use of advanced analytics, automation, and robotics to increase productivity and maintain product quality. There are several smart farming use cases around the world that demonstrate the impact of this paradigm shift on farming practices. One example is the smart water metering solution, which controls the water supply and measures varying levels of soil moisture to increase yields (Ahmad et al., 2017). Using coordinated hardware, the data is stored in the cloud. The data provides useful insights into different environmental conditions, enabling a practical way to monitor smart farms. Improving agricultural products is not all that is needed. The role of smart agriculture in achieving zero hunger cannot be achieved without effectively reducing food waste. Precision farming uses modern technologies such as big data, Machine Learning (ML), Deep Learning (DL), swarm intelligence, IoT, blockchain, autonomous systems, cyber-physical systems, cloud fog edge computing, and generative adversarial networks (GANs) to optimize crop yields and reduce waste (AyoubShaikh et al., 2022). However, factors such as connectivity and information flow, which are inherent to IoT systems in the agricultural sector, mean that they are most vulnerable to cyber-attacks, thereby disrupting food production. Attackers can exploit vulnerabilities in the network to remotely control and disrupt communication between connected devices. This makes precision farming systems either those that have been hacked or those that are vulnerable to being hacked (Abdelsalam et al., 2019). The risks associated with cyber-attacks are typically outsourced by domain-specific companies due to limited investment in cybersecurity. Moreover, the problem is exacerbated by the lack of resources and expertise among farmers or the farming community making smart farms fall prey to foreign attackers. Furthermore, Potential attacks can result in a dangerous or unproductive agricultural environment. For example, exploits that cause the device to spray pesticides, destroy an entire field of crops, irrigate farmland, or even flood farmland, etc. can lead to unsafe consumption or, worse, economic deterioration. In addition, potential attacks on agriculture can create a dangerous and inefficient farming environment. For example, the destruction of an entire acre of farmland, flooding, and intelligent drone pesticide spraying can lead to unsafe consumption and economic stagnation (Sharma et al., 2022). Also, a widespread, well-planned attack can cause economic disruption, especially in countries that rely heavily on agriculture.

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

2. Review of Related Literature

Farmers and agribusinesses are using a variety of smart farming approaches that incorporate IoT devices to increase production (Chae & Cho, 2018). The various sensor connections used on the farm and their communication over the internet can be hacked, as there has been an increase in cyber-attacks against the agricultural sector, including data theft and DoS, which has raised some concerns about security and privacy in smart agro-ecosystems (Vangala et al., 2023). Recently, researchers have been investigating security and privacy issues in smart agriculture systems. The study identifies potential cybersecurity issues in smart agriculture and provides a layered architecture, as well as detailed cyberattack scenarios divided into data, network, supply chain, and other typical threats. Examples of attacks that allow attackers to steal large amounts of information from many petrochemical companies include the well-known "The Night Dragon" attack (Arora et al., 2021). Another example is the razing of a German steel plant after hackers gained access to the plant's offices, networks, and manufacturing equipment through online phishing (Williams et al., 2023). As the exponential growth in the number of internet-connected devices has led to major security issues in the agricultural sector, and it is critical for modern agriculture to ensure the diversity of sensors in the smart farm environment, a study explores cybersecurity threats, potential vulnerabilities, and connected smart farming (Chetan Dwarkani M et al., 2015). The study identifies various technologies related to smart agriculture, such as on-farm equipment, and highlights security, integrity, and availability models for cybersecurity in agriculture using sensing technologies and machine learning. It also briefly describes relevant groups such as farmers, herders, and industries that support or depend on agriculture. Furthermore, attackers, such as the Mirai botnet, can carry out a variety of attacks on the many IoT sensors in smart farms, including DoS and possibly distributed DoS (DDoS) attacks (Gill et al., 2020). The botnet exploits a large number of connected smart home devices to launch multiple DoS attacks. Similarly, in smart farming ecosystems, such attacks can be used to disrupt legitimate network services in other domains, as well as the proper functioning of multiple modules within a single group. A smart farm can turn into an Internet of vulnerabilities for hackers since researchers have confirmed that IoT devices can simply be exploited to infect many other networks within an army of compromised farms (Rosline et al., 2022). Figure 1 displays DDoS detection and prevention architecture.

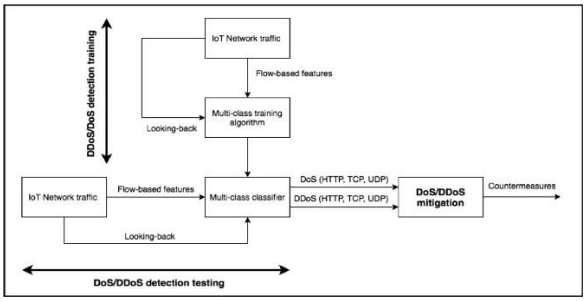


Figure 1. DDoS detection and prevention architecture (Mihoub et al., 2022)

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

A. Security and privacy issues in smart farming data

Smart farms generate large amounts of complex and dynamic spatial data from a wide range of different sensors, devices, and equipment, and unauthorized access or disclosure of this information by insiders can lead to potential threats (Catalano et al., 2022). For example, leakage of information about anti-jamming devices used in agriculture could help an attacker evade these security measures, while leakage of information about purchases of land, crops, and agricultural products would be a threat if this information were acquired by competitors or hostile actors.

Approval and Trust Issue: In smart farming, connected entities such as automated tractors, drones, and field sensors communicate and interact with each other to initiate operations. Such communication can be redirected from one machine to another, or cloud or edge-assisted, possibly supporting Message Queuing Remote Transport (MQTT), Constraint Application Protocol (CoAP22), or other IoT communication protocols It can be redirected through the network (Aliyu & Liu, 2023). Authentication and secure communication Problems: Authentication of connected devices is one of the most important aspects of security and privacy in Smart Farming. In order to connect to the various services of the smart farming system, the device must first be authenticated. These are typically low-power devices with limited processor, memory, and storage capabilities, so traditional PKI (Public Key Infrastructure) authentication mechanisms are not considered a solution. Enforceable rights. In addition, a lightweight and secure multi-factor authentication protocol, delivered as a service, is a more practical solution in a smart agricultural grid environment. Also, an Intermediate Certificate Authority (ICA) can help authenticate connected devices (Kampanakis & Kallitsis, 2022). Although such authentication mechanisms are available, ICAs can help authenticate connected devices without using the device's limited resources to handle authentication and actively prevent unauthorized devices from connecting to and accessing the network. In addition, devices can join and leave different layers of the smart farming ecosystem. It includes a dynamic authentication mechanism that applies authentication as needed, ensuring that only legitimate devices have access to different services at different levels.

Intellectual Property (IP): An important question from a compliance perspective is who owns the data collected in smart farms. This is particularly important because data protection laws cannot solve this problem. Whereas the current legal framework cannot protect the data itself, copyright law provides IP. Another important issue from a compliance perspective is who owns the data collected in highly protected smart farms. Most farmers include IP protection provisions in their contracts with suppliers of smart farming technology. In addition, agriculture and livestock are highly regulated industries as there are many laws, regulations, and regulatory bodies in different countries around the world. These relate to compliance requirements specific to the production and marketing of products. Such compliance is easier to achieve through the use of smart farming technologies that help farmers and regulators track, test, and inspect every step of the production process (Zanella et al., 2022).

Cyber Insurance: Cyber insurance allows victims to protect themselves against numerous cyber risks. However, agricultural cyber insurance policies have been slow to cover cyber incidents and

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

events. Most of the cyber insurance policies currently available for agriculture are very vague, with limited coverage (Kim & Laskowski, 2017).

Internal data breach: Among other threats, farmers are most concerned about the exposure of sensitive data. Insiders (such as disgruntled employees) may disclose this data to deliberately cause damage or sell the data for profit.

B. Attacks on smart farming systems

Cloud data leakage: Smart farming data is sensitive and can expose a lot of sensitive agricultural and economic information across the country. Cloud data centres span the globe and, in some cases, virtual machines may be located in data centres in different countries. Hosting in data centres in other countries can make your data less secure.

False data injection attacks: In this attack, the attacker assumes knowledge of the system and its configuration and attempts to modify/change data that contributes to important real-time decisions. For example, entering incorrect soil moisture information can lead to waterlogging and crop damage. Misinformation attack: The aim of this attack is to compromise the integrity of the data. Attackers can publish smart farm data that fake disease claims on crops and livestock.

C. Networking and Equipment Attacks

Radiofrequency (RF) jamming attack: Smart farming equipment often relies on radio frequency communications such as cellular and satellite networks. Smart farming equipment often uses the Global Navigation Satellite System (GNSS) to improve the efficiency of products and technologies such as routing, autopilot, seeding rates, and application. GNSS is achieved by combining GPS and real-time kinematics (RTK) technology to improve the accuracy of real-time location data (Kushwah & Ranga, 2020).

Malware injection attack: This is where attackers inject malware into connected smart devices. Malware is a very common threat in large systems because it is largely automated and spreads throughout the system, making it a very attractive target for attackers. As smart arming is booming and more farms are connected to the internet, most of these farm implementations typically use similar software components such as LoRa and ZigBee. (Madushanki et al., 2019).

Botnets: With IoT, anything can be connected to the Internet. In the smart agriculture ecosystem, there are many IoT-related devices at every architectural level. These devices are vulnerable and can be controlled by a malicious central system. This is known as an "object botnet network" (Gharehchopogh et al., 2023).

Side-channel attacks: Attacks that come from gathering information about how the system is being used, rather than weaknesses in the implementation of the system, are known as side-channel attacks (Devi & Majumder, 2021). As smart farming is one of the use cases of the IoT, it inherits some common IoT vulnerabilities, including side-channel attacks.

D. Supply Chain Attacks

The whole agroecosystem and the concept of 'farm to fork' involves a number of entities working together to deliver quality food to the end consumer on a just-in-time basis. This supply chain system starts at the farm where raw materials are produced, stored, and processed in the food

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

industry. The processed food is then packaged and shipped to retailers, and finally to distribution, where the final consumer buys the processed product. The use of IoT technology at each stage of the supply chain creates a potential cybersecurity threat, as a security breach in the immediate delivery system could have a significant impact on the customer, along with the entire supply chain (Andreoli et al., 2023).

E. **Cloud computing attacks**

The cloud is a very diverse, decentralized, heterogeneous, and powerful ecosystem and a large amount of distributed resources makes the cloud a difficult target (Aliyu, 2020). Cloud computing systems, in which computing resources are rented on an on-demand, pay-as-you-go basis, and multiple users share the same physical infrastructure, have recently gained traction. (Rabbani et al., 2020). However, with the advent of new cloud concepts (on-demand services, auto-scaling, self-provisioning, etc.), attackers have taken advantage of these resources and the cloud has become one of the most desirable targets for attackers. For example, with the advent of cloud auto-scaling, the majority of virtual machines hosted in the cloud are similarly configured. If one virtual machine is vulnerable, all auto-scaled virtual machines may be vulnerable. Therefore, malware that infects one virtual machine can quickly spread to other virtual machines.

3. Materials and Methods

To assess the impact of Wi-Fi de-authentication attacks on smart farms and evaluate the effectiveness of an IDS, a comprehensive experimental setup was devised. The experimental environment included a Raspberry Pi 3 Model B and a Raspberry Pi 3 Model B+ to simulate connected devices, representative of smart sensors or drones in a smart farming system. These devices were subjected to Wi-Fi de-authentication attacks to observe the effects on network connectivity and data-driven decision-making processes. The attacks targeted the devices' ability to transmit real-time data, crucial for operations like automated irrigation based on soil moisture levels. Data collection was integral to this process, involving the monitoring of connectivity status, sensor data transmission, and response times. The IDS was configured to detect such attacks by analysing network traffic for anomalies and leveraging advanced computational techniques. Accuracy, precision, recall, and F1 Score were used as primary metrics to evaluate IDS performance, while the Area Under the Curve (AUC) from the Receiver Operating Characteristic (ROC) curve provided a comprehensive measure of the system's diagnostic ability. The IDS implementation included enabling IEEE 802.11w-2009 to encrypt and protect management frames, thus preventing de-authentication attacks. This standard was particularly noted for its applicability in large-scale enterprise environments, though its support was hardware-dependent. The Raspberry Pi 3 Model B+ was identified as capable of supporting these enhanced security features, unlike its predecessor. Data from multiple experimental thresholds were collected to plot the ROC curve, showcasing the true positive rate (recall) against the false positive rate at various levels of sensitivity. The defence against attack in smart farming using IDS evaluation metrics includes:

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

A. **Security metrics**

The metrics in this category represent the effectiveness of the IDS in distinguishing between intrusive and non-intrusive activity. As a binary classifier, the IDS can have one of the following outputs

True Positive (TP): When an intrusion is correctly classified as an intrusion.

True Negative (TN): When a legitimate action is justified.

False Positive (FP): When a legitimate action is considered an intrusion.

False negative (FN): When the intervention is considered a lawful act, it is wrong.

Confusion Matrix: This metric reflects the results of the classification. For example, it represents the true and false results of the classifier. The confusion matrix itself is not a metric, but a basic metric from which other performance measures can be quantified.

Accuracy: This metric is essentially the correct classification rate of the IDS, whether on a validator or a test set. Accuracy is achieved with:

$$(TP + TN)/(TP+TN+FP+FN) \quad (1)$$

Precision: This metric represents the ratio of the classified actions by the IDS that are intrusive. Precision is obtained with:

$$TP/(TP+FP) \quad (2)$$

Recall: This metric is the ratio of intrusive actions classified by the IDS as intrusive. The recall is obtained with:

$$TP/(TP+FN) \quad (3)$$

ROC curve: The receiver operator characteristic (ROC) curve is a powerful metric that shows the sensitivity and specificity associated with a continuous variable. It is a coordinate plot consisting of a true positive ratio (TPR), vertical axis, and a false positive ratio (FPR), horizontal axis. The area under the ROC curve, known as the AUC, is considered the primary assessment measure.

$$FP/(FP+TN) \quad (4)$$

B. **Performance-Based Metrics**

Computational cost: Computational cost is the time required to perform a task necessary to classify an action as intrusive or legitimate. Communication cost is the amount of data that can be processed by an IDS per second. This is the speed expressed in gigabits per second to confirm the performance displayed by the IDS.

CPU usage: This metric represents the percentage of CPU overhead when adding an IDS to the infrastructure.

Memory Usage: This metric represents the amount of memory required by the IDS.

Power Consumption: This metric represents the additional power consumed by the device when the IDS is deployed. This measurement is critical for hardware-constrained devices such as mobile devices and IoT devices.

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

Figure 2: Attacks on Extreme Learning Machines and Voting IDSs

The procedure involves a successful denial of service attack using a Wi-Fi deauthorisation attack. The Wi-Fi deauthorisation tool was used to disrupt the communication between the Raspberry Pi and the Wi-Fi access point. For this study, we used the Maker-Focus ESP8266 Deauther Monster WiFi Development Board. This disconnected the Raspberry Pi from the network and stopped it from sending data to the Azure cloud. It also disabled all devices connected to the network as the attack spread across the network. Deauther sends packets that isolate the device, but do not interfere with the frequency.

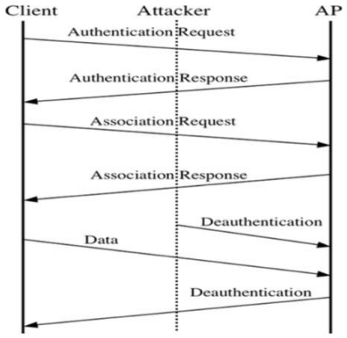


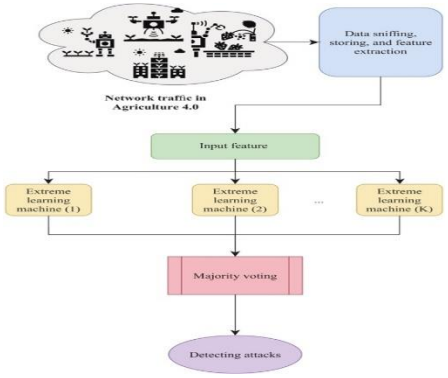
Figure 3: De-authentication attack graphical representation

C. Wi-Fi De-Authentication Attack

Stage One: Authentication Required

A Wi-Fi DE authentication attack is actually performed on a smart farm architecture connected to a 2.4 GHz network. This attack can be classified as a DoS attack and exploits a vulnerability in 802.11. The attacker first discovers the target of the attack by observing the raw frames combined with information such as the source and destination MAC (Media Access Control) addresses. For example, Wireshark packet capture can be used to detect traffic patterns and identify victims.

Stage two



Here, the victim must send sensor updates to the cloud every few seconds to minutes, so observing packet activity can help detect the victim. After finding a data or link response frame, an attacker

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

will typically send a spoofed unauthentication frame with the spoofed source MAC address of the victim's access point or station.

Stage three: Challenge

Unauthenticated frames are typically sent when all communication from a station or access point is complete. Deauthorisation is a notification, not a request. This means that when a station tries to disconnect from an access point, or an access point tries to disconnect from a station, any device can send unauthenticated and unauthenticated frames. One can reject them unless protected by management. means compatible framework.

Stage Four: Feedback from associations

Automatic unauthentication requires unlinking because authentication is a prerequisite for binding. Sending unauthenticated spoofed frames causes the destination station to be unauthenticated and disconnected from the network. The attacked station then attempts to reconnect and to block this reconnection, the attacker continues to send unauthenticated frames. To reconnect, the attacked client must repeat its IEEE 802.11 binding and authentication process.

Stage Five: De-authentication

At this point, the station cannot connect to the network by retaining the spoofed frames for a long time. Repeated transmission of these frames is considered a DoS attack against the target MAC address, which is then denied access to the network.

Stage Six: Data

Data from this type of attack is difficult to detect because the frames are sent directly to the client without being detected or logged by the access point or IDS. Also, MAC filtering will not prevent this attack. Such attacks are often used to prevent unauthorized stations from connecting to a wireless IDS provider's access point.

Stage Seven: Deauthorisation

At this stage, the main reason this attack is possible is that management frames are not encrypted using the IEEE 802.11 protocol. However, the 802.11w protocol prevents Wi-Fi de-authentication attacks by incorporating cryptographic protection into the de-authentication and split frames. This makes it very difficult to spoof these frames in a DoS attack. The main reason for the success of this attack is that many vendors have not upgraded their hardware and software to 802.11w.

Steps in a DoS attack

For a successful Wi-Fi source attack, the Wi-Fi signalling tool must be within range of your network. The Deauther Monster MakerFocus ESP8266 WiFi development board comes with an antenna for better signal reception. This allows opponents of WiFi-enabled smart farms to carry out such attacks. Note that this attack only works on their 2.4GHz network. Below are the steps to complete the attack (see Figure 3). These steps may change if a different deauthorisation tool is used. The first step is to scan for access points and stations. This is the most important step as the attack cannot be carried out if the desired station or access point is not found. Depending on the signal strength, antennas can be attached to the Deauther tool. This procedure requires stations and access points, if you try to deauthorize your Raspberry Pi you will need to go back to the main menu and select your Raspberry Pi in the Station. As you search for Stations and Access Points in

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

Step 1, your Raspberry Pi should be found and listed under Stations. In this step, we have selected the Raspberry Pi as the station we want to attack. The final step is to organize the attack. This means going back to the main menu and selecting Deauthorise attack under Attack. The deauthorisation frame is sent to the Raspberry Pi to disconnect it from the network. The hacked Raspberry Pi is not connected to the network and the cloud cannot receive sensor updates.

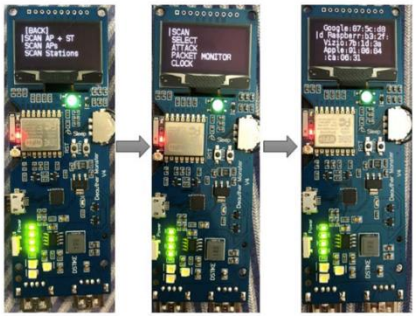


Figure 4: DoS Attack Implementation Stages

Figure 5: The Complete Network Attack

4. Results and Discussion

Wi-Fi authentication attacks are among the leading availability attacks that disrupt the accessibility of networks and communication devices and negatively impact the productivity of smart farms. For the purposes of these tests, the Raspberry Pi can be considered a 'connected device' (similar to a smart sensor or drone). A Wi-Fi de-authentication attack targets the Raspberry Pi and disconnects it from the network. This attack affects smart farms in a variety of situations. Data collected from various sensors forms the basis of smart farms, where most data-driven decisions are automated. For example, the farm's smart farming system turns on and off based on soil moisture, as measured by the moisture sensor. Typically, this is based on a single specific threshold. However, modern systems take into account more dynamic factors, requiring AI technology and real-time data analysis (Keleko et al., 2022). Real-time AI services are used to understand how environmental factors affect the crops we irrigate and how soil moisture responds to farming, soil, and other conditions. Therefore, a DoS attack that prevents moisture sensors from connecting to the network would disrupt real-time communication and interfere with farming system decisions. This could lead to over or under-watering of the crop, ultimately damaging the crop and affecting the success of the harvest. The potential damage in this particular case also applies to pets, which lack sensors to monitor their food, water, and health. As discussed in this article, deauthorisation attacks can be the basis for malicious duplicate access point attacks and subsequent password cracking attacks. The attackers obtained the farmer's credentials by redirecting him to a similarly spoofed network. The attackers then had access to the entire Smart Farm and could target and damage various devices. For example, attackers can sabotage crops by flying agricultural drones or spraying excess

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

fertilizer on crops. This can cause premature crop failure and serious damage. It is also important to recover quickly from a DoS attack or communication failure before serious damage occurs. Detection and recovery techniques must therefore be carefully considered. Such an attack, if carried out on a large scale, could result in severe economic losses for the entire country. By enabling IEEE 802.11w-2009, management frames are encrypted and protected to prevent and detect de-authentication attacks. WPA3 requires IEEE 802.11w. The paired unique key is used for unauthentication and splits the frame sent after the key is generated. One for the access point and one for the client. The client determines if the unauthentication is valid. Inexpensive 2009 802.11w routers are popular with large enterprises such as Cisco and Aruba. One possible reason for this is manufacturing costs. Password issues related to missing passwords can make 802.11w routers non-compliant and cause problems in the production cycle. For example, 802.11w requires a strong secure network (RSN) with AES/CCMP encryption. 802.11w requires the vendor to update their code/firmware on both the access point and client side. In addition, some routers require IEEE 802.11w to be enabled and should not be enabled automatically. The Raspberry Pi 3 Model B in this architecture does not support 802.11w because the NIC 134 does not support the encryption protocol required for protected management frames. However, the Raspberry Pi 3 Model B+ is capable of handling protected frames. Therefore, upgraded hardware with built-in cryptographic management framework capabilities can protect against such attacks. Furthermore, Table 1 shows the security metrics evaluation results.

Table 1: The IDS security performance metrics

Metric	Value
Accuracy	0.95
Precision	0.92
Recall	0.90
F1 Score	0.91
AUC (ROC Curve)	0.96

Table 2 and Figure 6 represent the ROC curve data points values for our different experimental thresholds.

Threshold	True Positive Rate (Recall)	False Positive Rate
0.1	0.98	0.20
0.2	0.95	0.15
0.3	0.92	0.10
0.4	0.90	0.07
0.5	0.85	0.05
0.6	0.80	0.03
0.7	0.75	0.02
0.8	0.70	0.01
0.9	0.65	0.005

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

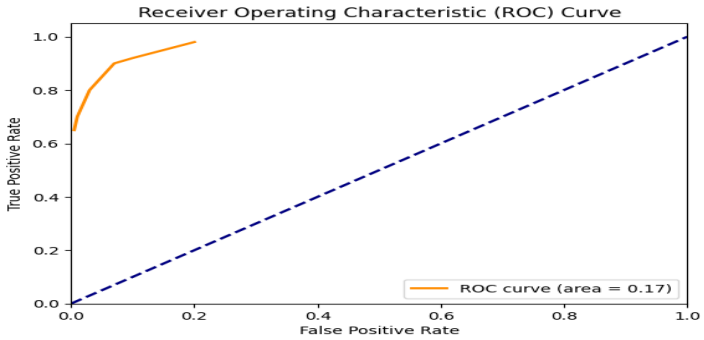


Figure 6. the ROC Curve

The results, as detailed in Table 1 and Table 2, demonstrated high accuracy (0.95), precision (0.92), recall (0.90), and an AUC of 0.96, indicating robust performance in detecting and mitigating the impact of Wi-Fi de-authentication attacks on smart farms outperforming some recent work such as that of (Rababah & Srivastava, 2023). This methodology underscores the necessity of robust detection and quick recovery mechanisms to minimize economic losses and operational disruptions in smart farming environments.

5. Conclusion

This article addresses the critical issue of DoS attacks against the smart farm ecosystem, focusing on the impact of Wi-Fi de-authentication attacks. Using the MakerFocus ESP8266 WiFi Deauther Monster development board, we successfully implemented a Wi-Fi re-authentication attack on a smart farm's Wi-Fi network, effectively preventing deployed sensors from maintaining network connectivity. Additionally, we evaluated the cybersecurity threats using various metrics to assess the performance of the IDS and proposed multiple solutions to mitigate DDoS attacks in smart farming. The study revealed that the attack was limited to 2.4GHz networks, highlighting the broader range of this frequency compared to 5GHz networks, which could yield different results. The methodology for performing the attack was discussed, noting that variations could occur with different de-authentication tools. Overall, our findings demonstrate that employing IDS metrics techniques is an effective strategy for addressing DoS attacks in smart farming.

Future research should focus on expanding the scope of this study to include 5GHz networks to compare the effectiveness and range of attacks across different frequencies. Additionally, exploring the integration of more advanced IDS techniques, such as machine learning algorithms and AI-driven anomaly detection, could enhance the system's ability to identify and respond to a wider range of cybersecurity threats. Investigating the development and deployment of resilient network protocols and hardware that are inherently resistant to de-authentication attacks will also be crucial. Furthermore, a comprehensive analysis of the economic impact of DoS attacks on smart farms, coupled with cost-benefit analyses of implementing various IDS solutions, would provide valuable insights for stakeholders. Finally, conducting large-scale field tests in diverse agricultural settings would validate the effectiveness and practicality of the proposed solutions in real-world scenario.

ISSN 2734-3839 (Print), ISSN 2735-962X (E-Copy)
http://www.journal.kasu.edu.ng/index.php/kjms DOI/10.5281/zenodo.12647546.svg

Statements and Declarations

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

Acknowledgment: Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University.

Funding: China National Key R & D Plan 2020YFA0607902

Author contribution: Ahmed Abubakar Aliyu: Conceptualization, Methodology, Data curation, Writing-Original draft. Jinshuo Liu: Supervision, Visualization, Investigation, Funding Acquisition. Ezekia Gilliard: Software, Validation, Meng Wang: Writing- Review and Editing.

References:

Abdelsalam, M., Krishnan, R., & Sandhu, R. (2019). Online Malware Detection in Cloud Auto-scaling Systems Using Shallow Convolutional Neural Networks. In S. N. Foley (Ed.), *Data and Applications Security and Privacy XXXIII* (Vol. 11559, pp. 381–397). Springer International Publishing. https://doi.org/10.1007/978-3-030-22479-0_20

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

Ahmad, Z., Pasha, M. A., Ahmad, A., Muhammad, A., Masud, S., Schappacher, M., & Sikora, A. (2017). Performance evaluation of IEEE 802.15.4-compliant smart water meters for automating large-scale waterways. *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 746–751. https://doi.org/10.1109/IDAACS.2017.8095189

Aliyu, A. A. (2020). Improving Cloud Data Security by hybridization of Zero-Knowledge Proof and Time-Based One-Time Password. *KASU JOURNAL OF MATHEMATICAL SCIENCES (KJMS)*, *1*(2), 116–126.

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.

Andreoli, A., Lounis, A., Debbabi, M., & Hanna, A. (2023). On the prevalence of software supply chain attacks: Empirical study and investigative framework. *Forensic Science International: Digital Investigation*, *44*, 301508. https://doi.org/10.1016/j.fsidi.2023.301508

Arora, P., Kaur, B., & Teixeira, M. A. (2021). Evaluation of Machine Learning Algorithms Used on Attacks Detection in Industrial Control Systems. *Journal of The Institution of Engineers (India): Series B*, *102*(3), 605–616. https://doi.org/10.1007/s40031-021-00563-z

Ayoub Shaikh, T., Rasool, T., & Rasheed Lone, F. (2022). Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming. *Computers and Electronics in Agriculture*, *198*, 107119. https://doi.org/10.1016/j.compag.2022.107119

Catalano, C., Paiano, L., Calabrese, F., Cataldo, M., Mancarella, L., & Tommasi, F. (2022). Anomaly detection in smart agriculture systems. *Computers in Industry*, *143*, 103750. https://doi.org/10.1016/j.compind.2022.103750

Chae, C.-J., & Cho, H.-J. (2018). Enhanced secure device authentication algorithm in P2P-based smart farm system. *Peer-to-Peer Networking and Applications*, *11*(6), 1230–1239. https://doi.org/10.1007/s12083-018-0635-3

Chetan Dwarkani M, Ganesh Ram R, Jagannathan S, & Priyatharshini, R. (2015). Smart farming system using sensors for agricultural task automation. *2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR)*, 49–53. https://doi.org/10.1109/TIAR.2015.7358530

Choi, S.-W., & Shin, Y. J. (2023). Role of Smart Farm as a Tool for Sustainable Economic Growth of Korean Agriculture: Using Input–Output Analysis. *Sustainability*, *15*(4), 3450. https://doi.org/10.3390/su15043450

Devi, M., & Majumder, A. (2021). Side-Channel Attack in Internet of Things: A Survey. In J. K. Mandal, S. Mukhopadhyay, & A. Roy (Eds.), *Applications of Internet of Things* (pp. 213–222). Springer. https://doi.org/10.1007/978-981-15-6198-6_20

Gharehchopogh, F. S., Abdollahzadeh, B., Barshandeh, S., & Arasteh, B. (2023). A Multi-Objective Mutation-based Dynamic Harris Hawks Optimization for Botnet Detection in IoT. *Internet of Things*, 100952. https://doi.org/10.1016/j.iot.2023.100952

Gill, K. S., Saxena, S., & Sharma, A. (2020). GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot. *Computers & Security*, *92*, 101732. https://doi.org/10.1016/j.cose.2020.101732

Grogan, A. (2012). Smart farming. *Engineering & Technology*, *7*(6), 38. https://doi.org/10.1049/et.2012.0601

Istiak, M. S., & Khaliduzzaman, A. (2022). Poultry and Egg Production: An Overview. In A. Khaliduzzaman (Ed.), *Informatics in Poultry Production: A Technical Guidebook for Egg and Poultry Education, Research and Industry* (pp. 3–12). Springer Nature. https://doi.org/10.1007/978-981-19-2556-6_1

Kampanakis, P., & Kallitsis, M. (2022). Faster Post-Quantum TLS Handshakes Without Intermediate CA Certificates. In S. Dolev, J. Katz, & A. Meisels (Eds.), *Cyber Security, Cryptology, and Machine Learning* (pp. 337–355). Springer International Publishing. https://doi.org/10.1007/978-3-031-07689-3_25

Keleko, A. T., Kamsu-Foguem, B., Ngouna, R. H., & Tongne, A. (2022). Artificial intelligence and real-time predictive maintenance in industry 4.0: A bibliometric analysis. *AI and Ethics*, *2*(4), 553–577. https://doi.org/10.1007/s43681-021-00132-6

Kim, H., & Laskowski, M. (2017). Agriculture on the Blockchain: Sustainable Solutions for Food, Farmers, and Financing. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3028164

Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications*, *53*, 102532. https://doi.org/10.1016/j.jisa.2020.102532

Madushanki, A. A. R., N, M., A., W., & Syed, A. (2019). Adoption of the Internet of Things (IoT) in Agriculture and Smart Farming towards Urban Greening: A Review. *International Journal of Advanced Computer Science and Applications*, *10*(4). https://doi.org/10.14569/IJACSA.2019.0100402

Mihoub, A., Fredj, O. B., Cheikhrouhou, O., Derhab, A., & Krichen, M. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. *Computers & Electrical Engineering*, *98*, 107716. https://doi.org/10.1016/j.compeleceng.2022.107716

Rababah, B., & Srivastava, S. (n.d.). *Hybrid Model For Intrusion Detection Systems*. Retrieved July 9, 2023, from https://arxiv.org/ftp/arxiv/papers/2003/2003.08585.pdf

Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. *Journal of Network and Computer Applications*, *151*, 102507. https://doi.org/10.1016/j.jnca.2019.102507

Rosline, G. J., Rani, P., & Gnana Rajesh, D. (2022). Comprehensive Analysis on Security Threats Prevalent in IoT-Based Smart Farming Systems. In P. Karuppusamy, I. Perikos, & F. P. García Márquez (Eds.), *Ubiquitous Intelligent Systems* (pp. 185–194). Springer. https://doi.org/10.1007/978-981-16-3675-2_13

Sharma, V., Tripathi, A. K., & Mittal, H. (2022). Technological revolutions in smart farming: Current trends, challenges & future directions. *Computers and Electronics in Agriculture*, *201*, 107217. https://doi.org/10.1016/j.compag.2022.107217

van Dijk, M., Morley, T., Rau, M. L., & Saghai, Y. (2021). A meta-analysis of projected global food demand and population at risk of hunger for the period 2010–2050. *Nature Food*, *2*(7), Article 7. https://doi.org/10.1038/s43016-021-00322-9

Vangala, A., Das, A. K., Chamola, V., Korotaev, V., & Rodrigues, J. J. P. C. (2023). Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. *Cluster Computing*, *26*(2), 879–902. https://doi.org/10.1007/s10586-022-03566-7

Williams, B., Soulet, M., & Siraj, A. (2023). A Taxonomy of Cyber Attacks in Smart Manufacturing Systems. In L. Knapčíková & D. Peraković (Eds.), *6th EAI International Conference on Management of Manufacturing Systems* (pp. 77–97). Springer International Publishing. https://doi.org/10.1007/978-3-030-96314-9_6

Zanella, A. R. de A., da Silva, E., & Albini, L. C. P. (2022). CEIFA: A multi-level anomaly detector for smart farming. *Computers and Electronics in Agriculture*, *202*, 107279. https://doi.org/10.1016/j.compag.2022.107279