ORIGINAL PAPER

Mitigating Data Poisoning Attacks in Smart Farming

Abstract: **Smart farming as an integral part of the Internet of Things (IoT) is growing in popularity as a means of supplying the world's expanding food needs. Many approaches exist for smart farms to leverage technology and connected devices. For instance, from receiving crop status and soil moisture in real-time, to operating drones to assist with tasks like applying pesticide spray. However, the utilization of various Internet-connected gadgets causes some weaknesses in the smart farming ecosystem. Intruders can use these weaknesses to manipulate field sensor data flow and disrupt it remotely. This will have negative consequences, especially in high-risk situations such as harvesting when real-time monitoring is required. The study used both qualitative and quantitative approaches to analyse the intended research objectives to mitigate data poisoning attacks in smart farms. This study also presents different intrusion detection systems (IDS) metrics to validate the performance and effectiveness of IDS deployed and claimed different IDS methods to address smart farming poisoning attacks. The study concludes that the application of IDS measurement method can be actively applied to solve Denial of Service (DOS) incidence.**

Keywords*: Smart Farming, Data Poisoning Attack, Intrusion Detection Systems, Denial of Service Attacks, Internet of Things.*

I. INTRODUCTION

In recent years, the agricultural sector has made great strides in developing smart agriculture and precision farming technology. Agricultural development is by far, one of the most effective instruments to eradicate extreme poverty, increase collective well-being, and provide sustenance for an estimated 9.7 billion individuals by the year 2050. Also, Agronomy is vital to economic development, as it accounts for almost 4% and more than 25% of global gross domestic product (GDP) in some developing countries respectively (WorldBank, 2022). Even though small-scale as well as artisan farming has witnessed a revival for the past decade, however, many traditional farmers want to move further to improve their productivity and yield, comparable to other supply chains, and deliberated automation to be the way to go (Grogan, 2012). Moreover, the rapid population growth has significantly led to the demand for agricultural products and food. Hence, investigations into smart agricultural ecosystems and adopting new technologies will have extensive implications for the global economy at scale (Choi & Shin, 2023; Abubakar, 2023). The traditional technologies that have underpinned the agricultural sector do not meet this need and are outdated.

Today, the agriculture and food industries put more emphasis on automation in almost all facets of agriculture and farming practices, from pre-planting to post-harvesting, thereby Increasing its effectiveness (Abubakar & Shamsuddeen, 2023). They make use of both web data and related materials or “things” i.e. IoT. The IoT lessens human-farm interactions by automating processes, through a network of interconnected devices such as sensors and drones, robotic arms, etc. which can exchange messages without the need for human involvement. The agricultural output is enhanced both numerically and qualitatively by IoT technology. Yet, the use of IoT for agricultural automation. Smart agriculture encompasses a broader range of technologies and practices beyond mere IoT devices. Smart agriculture includes the use of advanced analytics, automation, and robotics to increase productivity and maintain product quality.

Various use cases of smart farming exist around the world which demonstrate the impact of these paradigm shifts on farming methods. Controlling water supply and measuring varying levels of soil

moisture to increase the yield, the smart water metering solution is just one example (Ahmad, et al., 2017). using coordinated hardware, data is stored on the cloud. The data provides useful insight into various environmental conditions and thereby enables a practical way for monitoring smart farms. Improving farm produce is not all you need. The role of smart farming in achieving zero hunger cannot be achieved without effectively mitigating food waste. Precision farming employs modern technologies such as big data, ML, DL, swarm intelligence, IoT, blockchain, autonomous systems, cyber-physical systems, cloud-fog-edge computing, and generative adversarial networks (GAN) to optimize crop yield and reduce waste.

However, factors such as connectivity and information flow which are inherent in the IoT systems in the agricultural sector denote the utmost exposure to cyber-attack, thereby disrupting food production. Attackers may exploit the vulnerabilities in the network to remotely control and disrupt communications between the connected devices. This makes precision agriculture systems to be either those that have been hacked already or those that are susceptible to being hacked (Abdelsalam, Krishnan, & Sandhu, 2019). The risks attached the cyber-attacks are usually outsourced by domain-specific companies due to the limited investments in cybersecurity. The issue is further made worse by the lack of resources and expertise among farmers or the farming community. Intelligent farms could fall prey to foreign attackers (Abubakar, 2022). Possible assaults may result in an agricultural environment that is hazardous or unproductive. For example, exploits that can cause the device to spray pesticides, destroy an entire field of crops, irrigate farmland, or even cause flood the farmlands, etc. can cause unsafe consumption or even worst, economic deterioration. Additionally, potential farming attacks can create a dangerous and inefficient farming environment. For instance, a full acre of agriculture being destroyed, flooding, and the intelligent drone spraying of pesticides can result in dangerous consumption and economic stagnation. An extensive, well-planned attack can cause economic disruption, especially in countries that heavily rely on agriculture (Abubakar, Liu, & Gilliard, 2023)

A. AIM AND OBJECTIVES

This study aimed at assessing protections against data poisoning attacks for smart farming and the provision of a protective solution. The objectives include:

- Study of various security and privacy challenges faced by smart farming in agricultural settings
- Assessment of various data poisoning attacks faced by smart farming in the agricultural sector
- Enumeration of possible techniques to protect the smart farm from data poisoning attacks.

B. SIGNIFICANCE

Significantly, this research is poised to be of great importance to the farmers, the government, and the data protection experts. The study set out to decipher various data poisoning attacks that have been experienced by smart farming owners in the world. It will reveal various ways that data poisoning attacks can be averted through the application of various designed and implemented frameworks in the security server of the smart farm. It will also bring to the limelight the security and privacy challenges that have hindered the full functioning of smart farming in the agriculture industry.

This study identified the cybersecurity concerns in smart farming and presented scenario-specific cyberattacks categorized into supply chains such as data, networks, and other common attacks.

II. REVIEW OF RELATED LITERATURE

Agribusinesses and farmers are transforming a range of intelligent farming methods that integrate IoT devices to increase productivity (Chae & Cho, 2018). The various sensor connections used on the farm and their communication over the Internet can be hacked. Due to this, there have been more cyberattacks against the agricultural sector, including. According to Window (2019), Data theft, DoS Lately, has brought some concerns about security and privacy in intelligent agroecosystems. In the

study, possible cybersecurity problems in smart agriculture were identified and a layered architecture was provided. service assaults, website modifications, etc. Recently, researchers have shed light on security and privacy issues in intelligent agroecosystems. In the study, possible cybersecurity problems in smart agriculture were identified and a layered architecture was provided. Furthermore, their research provides detailed cyber-attack scenarios divided into data, network, supply chain, and other typical threats (Aung & Chang, 2014). Examples of attacks that enable attackers to steal copious amounts of information from numerous petrochemical businesses include the well-known "The Night Dragon" assault. Another illustration is the destruction of a German steel mill when hackers utilized online phishing to enter the facility's offices, networks, and production equipment.

Farmers are unable to withstand the potential loss and harm to their crops, which has led to major security issues in the agriculture sector as a result of the exponential development in the number of internet-connected gadgets Thus, it is crucial for contemporary agriculture to ensure the diversity of sensors in the smart farm environment. Threats to cyber-security, potential weaknesses, and connected smart farming are covered in (Chetan, et al., 2015). The paper identifies a variety of technologies connected to smart agriculture, such as on-farm equipment, and highlights security, integrity, and availability models for information security in agriculture. location sensing and remote sensing techniques, and machine learning. It also briefly describes relevant groups such as farmers, herders, and industries that support or depend on agriculture. Likewise, security issues in agriculture can arise from the use of IoT sensors as identified in (Choi & Shin, 2023). On numerous IoT sensors installed in smart farms, such as the Mirai botnet, attackers can carry out various attacks, such as DoS or perhaps distributed DoS (DDoS) attacks (Georgios, et al., 2017; Gill, et al., 2020). The botnet exploited a large number of connected smart home devices to launch multiple DoS attacks. Similarly, conditions exist in smart farming ecosystems, such Attacks can be used to obstruct legitimate network services in other domains as well as the proper operation of multiple modules within a single group (Grogan, 2012). A smart farm can turn into an Internet of vulnerabilities for hackers since Georgios

Constantinos and Angelos confirmed that IoT devices can simply be exploited to infect many other networks within an army of compromised farms (Gruschka & Jensen, 2019).

A. SECURITY AND PRIVACY ISSUES IN SMART FARMING DATA:

Smart farms generate large volumes of complex and dynamic spatial data from large numbers of various sensors, devices, and devices. Unauthorized access or disclosure of this information by insiders can lead to potential threats. A leak of information about anti-jamming equipment used in agriculture, for instance, could help an attacker circumvent these security measures, while a leak of information about purchases of land, crops, and agricultural products would be a threat if that information was If acquired from competitors or enemy actors, it can result in severe economic losses for farmers.

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 (Gruschka & Jensen, 2019).

Authentication and secure communication Problems:

Authentication of connected devices is one of the most important aspects of security and privacy in smart farming. To connect to various services of the smart farming system, the device must first be authenticated. These are typically low-power devices with a limited processor, memory, and storage capabilities, so traditional PKI (Public Key Infrastructure) authentication mechanisms are not considered a solution. Enforceable Rights. Moreover, a lightweight and secure multi-factor authentication protocol delivered as a service is a more practical solution in an intelligent agricultural grid environment (Jahn & Molly, 2019). An intermediate certificate authority (CA) can help authenticate connected devices. While such authentication mechanisms are available, intermediate certificate authorities (CAs) can help authenticate connected devices without using the device's

limited resources to handle authentication. They also effectively 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 only legitimate devices have access to various services at various levels.

Intellectual Property (IP):

An important question from a compliance perspective is who owns the data collected in smart farms. This is especially important because data protection laws cannot solve this problem. While the current legal framework cannot protect data itself, copyright law provides Intellectual Property (IP):

An important question from a compliance perspective is who owns the data collected in smart farms with a high degree of protection. Most farmers include intellectual property protection provisions in their contracts with smart farming technology suppliers.

Agriculture and livestock are highly regulated industries. Different countries around the world have many laws, regulations, and regulatory bodies. These relate to compliance requirements specific to the manufacture 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

Cyber Insurance: Allowing victims to shield themselves from numerous cyber risks is Cyber Insurance. However, cyber insurance policies in farming have lagged in the coverage of cyber incidents and events. Most of the current available agriculture-based cyber insurances are very ambiguous and with limited coverage (Kim & Laskowski, 2018).

Internal data breach: Among other threats, farmers fear the exposure of sensitive data the most. Insiders (such as disgruntled employees) may disclose this data to intentionally cause harm or sell the data for profit.

B. SMART FARMING ECOSYSTEM CYBER DATA ATTACKS

Cloud Data Leakage: Smart farming data is sensitive and can reveal 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 may make your data less secure (Kolias, et al., 2017).

Attacks by injecting bogus data: In this attack, the attacker assumes to know about the system and its configuration and tries to modify/change data that contribute to important decisions in real-time. For example, entering incorrect soil moisture information can lead to waterlogging and crop damage as a result.

Misinformation attack: The purpose 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

High-frequency jamming (Fr) attack: Smart farming devices often rely on radio frequency communications such as cellular and satellite networks. Smart agricultural equipment often uses the global positioning satellite system (GNSS) to improve the efficiency of products and technologies such as route planning, autopilot, seeding rates, and spreading. GNSS is achieved by combining GPS and real-time kinematics (RTK) technology to improve the accuracy of real-time location data (Kushwah & Ranga, 2020; Maanak & Ravi, 2018).

Malware injection attack: Here, 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. Precision agriculture is booming and more and more farms are connected to the internet. Most of these farm implementations typically use similar software components (e.g. LoRa and ZigBee) (Madushanki, et al., 2019).

Botnets: With IoT, everything can be connected to the Internet. In the smart farming 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 the "object botnet network" (Manos, et al., 2017).

Side-channel attack: Attacks that originate from gathering information about how the system is deployed, rather than weaknesses that exist in the system's implementation, are known as side-channel attacks. Since smart farming is one of the use cases of IoT, it inherits some common IoT vulnerabilities, including side-channel attacks.

D. SUPPLY CHAIN ATTACKS

The entire agroecosystem and the concept of "farm to fork" involve multiple entities working in tandem to deliver quality food to the end consumer in a just-in-time environment. This supply chain system starts at the farm, where raw materials are produced, then stored and processed in the food industry (Maria, et al., 2014). Processed foods are packaged and sent to retailers. distribution where the final customer buys the processed product. With IoT technology at every stage of the supply chain, it creates potential cybersecurity threats, as a security breach in an instant delivery system can also have a major impact on customers, with the entire supply chain.

E. CLOUD COMPUTING ATTACKS:

Shabadi and Biradar confirmed that the cloud is a very diverse, decentralized, heterogeneous, and powerful ecosystem (Masoumeh & Nasour, 2017). A large amount of distributed resources makes the cloud a difficult target. Cloud computing systems that rent computing resources on-demand, pay-as-you-go, and share multiple users on the same physical infrastructure are gaining traction (Rabbani, et al., 2020; Roshanianfard, et al., 2019). However, with the advent of new cloud concepts (on-demand services, auto-scaling, self-provisioning, etc.), attackers have taken advantage of such resources and the cloud has become one of the most desirable. rice field. attacker`s target. For example, with the advent of cloud auto-scaling, the majority of cloud-hosted virtual machines are similarly configured. If one virtual machine is vulnerable, all auto-scaled virtual machines can be vulnerable as well. Therefore, malware that infects one virtual machine can quickly spread to other virtual machines (Santhana & Biswas, 2023; Shabadi & Biradar, 2018; Sontowski, et al., 2020).

III. MATERIALS AND METHODS

The Defence Against Attack in Smart Farming Using IDS Evaluation Metrics include:

A. **SECURITY METRICS:**

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

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

True negative (TN): When a lawful action is justified.

False positive (FP): When a legitimate act is considered trespassing.

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

Chaos Matrix: This metric reflects the results of the classification. For example, it represents the true and false results of the classifier (Sucuri, 2017; Ukil, et al., 2011). 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 obtained 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 curve (ROC) is a powerful metric showing 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 evaluation measure.

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

Performance-Based Metrics:

Cost calculation: computational cost represents the amount of time it takes to complete a task required to classify an action as intrusive or legitimate.

Communication cost is the volume of data that can be processed by one IDS per second. This is the speed expressed in Giga Bits per second to confirm the performance shown by the IDS (West, 2018).

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

Memory usage: This metric represents the memory consumption required for the IDS to

Energy consumption: this metric represents the additional power consumed by the device when introducing the IDS. This measurement is essential for hardware-limited devices such as mobile devices and IoT devices.

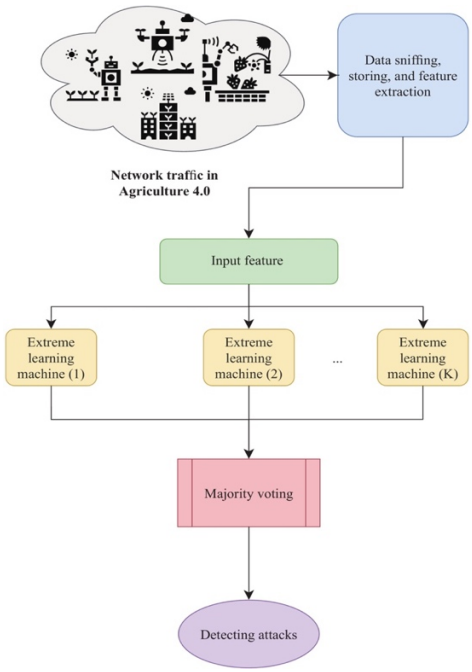

***Figure** 1:Extreme learning machine-based and Voting IDS for Smart Agric Attacks Materials and Method*

The procedure involves a successful denial of service attack using a Wi-Fi deauthorization attack. Using the Wi-Fi deauthorization tool interrupted 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 sending data to the Azure cloud. In addition, all devices connected to the network were disabled as the attack

spread through the network. Deauther sends packets that isolate the device but do not interfere with the frequency.

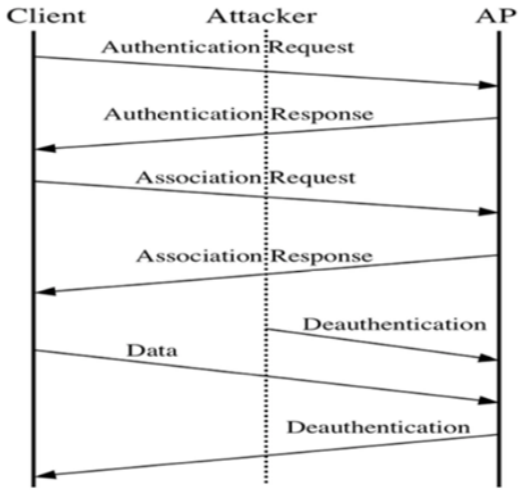

***Figure 2**: De-authentication Attack Graphical Representation*

B. 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 applied to detect traffic patterns and identify victims.

Stage two: Here, the victim has to push sensor updates to the cloud every few seconds to minutes, so observing packet activity can help detect the victim. After a data or link response frame is found, an attacker usually sends a forged unauthentication frame with the spoofed source MAC address of the victim's access point or station.

Stage Three: club request

Unauthentication frames are typically sent when all communication from a station or access point is complete. Deauthorization is a notice, not a request. This means that when a station tries to unsubscribe from an access point or an access point tries to unsubscribe from a station, any device

can send unauthenticated and unauthenticated frames. No one can refuse them unless protected by management. means compatible framework.

Stage Four: Feedback from associations

Auto-unauthentication requires unlinking because authentication is a prerequisite for binding. Sending unauthenticated spoofed frames will cause the destination station to be unauthenticated and disconnected from the network. The attacked station then tries to reconnect and to block this reconnection, the attacker keeps sending unauthenticated frames. To reconnect, the attacked client must repeat its IEEE 802.11 binding and authentication process.

Stage Five: De-authentication

At this time, the station cannot connect to the network by keeping the spoofed frames for a long time. The repeated transmission of these frames is considered a DoS attack against the target MAC address, which is then prevented from accessing 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 does 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: Deauthorization

At this point, the main reason this attack is possible is that the management frames are not encrypted using the IEEE 802.11 protocol. However, the 802.11w protocol prevents Wi-Fi deauthentication attacks by incorporating cryptographic protection into de-authentication and split frames. Therefore, it is 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 DoS Attack

For a successful Wi-Fi source attack, the Wi-Fi signal tool must be within range of your network. 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 its 2.4 GHz network. Below are the steps to complete the attack (see Figure 3). These steps may change if a different deauthorization tool is used. The first step is to search 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. Antennas can be attached to the Deauther tool depending on the signal strength. This procedure requires stations and access points to be found in this procedure.

- . 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. Since you searched for Stations and Access Points in Step 1, your Raspberry Pi should be found and listed under Stations. In this step, we have chosen the Raspberry Pi as the station we want to attack.
- 2. The final step is to organize the attack. That is, go back to the main menu and select Deauthorize attack under Attack. The de-authentication 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.

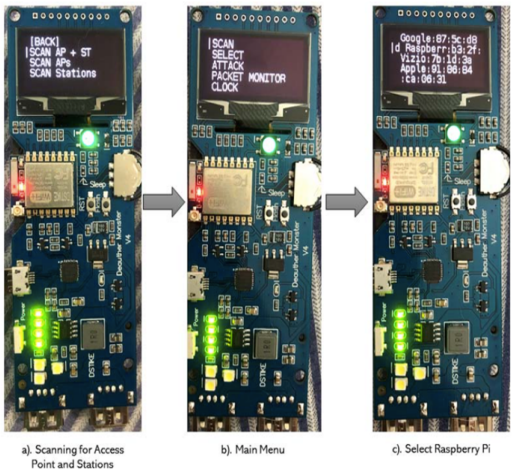

***Figure 3**: DoS Attack Implementation Stages*

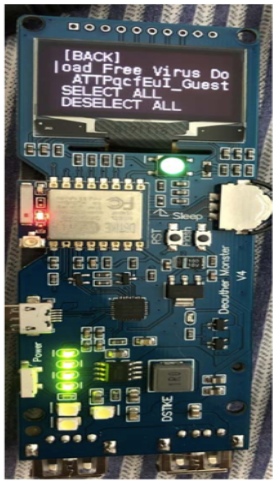

***Figure 4**: The Complete Network Attack*

V. RESULTS AND DISCUSSION

Wi-Fi authentication attacks are among the leading availability attacks, disrupting the accessibility of networks and communications equipment, and negatively impacting smart farm productivity. For these tests, the Raspberry Pi can be viewed as a "connected device" (similar to a smart sensor or a 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 form the basis of smart farms where most data-driven decisions are automated. For example, the farm's smart irrigation system turns on and off based on soil moisture as measured by the humidity sensor. Usually, it is based on a single specific threshold. However, modern smart irrigation systems think of more dynamic factors, requiring AI technology and real-time data analysis. Use real-time AI services to understand how environmental factors affect the crops we water and how soil moisture reacts to crop watering, soil, and other conditions. different environmental conditions. Therefore, a deauthorization attack that prevents moisture sensors from connecting to the network would interfere with real-time communication and impede irrigation system decisions. This results in too much or too little watering of the crop, which ultimately harms the crop and affects the success of the harvest. The potential harm in this particular case also applies to pets that lack sensors to monitor their food, water, and health. Control connected devices:

As discussed in this article, deauthorization attacks can be the basis for malicious duplicate access point attacks and subsequent password cracking attacks. The attackers obtained Farmer's credentials by redirecting him to a similar fake network. The attackers could afterward have access to the entire Smart Farm, targeting and damaging various devices. For example, attackers can sabotage crops by flying agricultural drones or spraying excess fertilizers on crops. This leads to premature crop damage and heavy damage. It is also important to recover quickly from a DoS attack or communication failure before serious damage occurs. Therefore, detection and recovery techniques need to be carefully considered. Such an attack, if launched on a large scale, could lead to severe economic losses for the whole country. Enabling IEEE 802.11w-2009 will encrypt and protect management frames to prevent and detect de-authentication attacks. WPA3 requires IEEE 802.11w. The pairwise unique key is used to unauthenticate and split the frame sent after key generation. One for the access

point and one for the client. The client determines whether the de-authentication is valid. Inexpensive 2009 802.11w routers are popular with large enterprises like Cisco and Aruba. One possible reason for this is the cost of production. Password problems related to missing passwords can make routers 802.11w 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 provider to update their code/firmware on both the access point and the 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 network interface card 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.

VI. CONCLUSION

This article discusses the problem of DoS attacks against the intelligent farm ecosystem. Using the MakerFocus ESP8266 WiFi Deauther Monster development board, we implemented a Wi-Fi re-authentication attack on a Wi-Fi network within a smart farm, preventing deployed sensors from connecting to the network. Additionally, the study discusses the cybersecurity threats with various metrics used to evaluate the performance of IDS and presented various solutions to prevent data poisoning in intelligent farming. This attack is limited to 2.4GHz networks because it has a wider range compared to 5GHz networks, using 5GHz could give a different result. The steps to perform the attack are also discussed but may differ if you are using another deauthentication tool. In summary, this study shows that applying IDS metrics techniques can solve DOS attacks in intelligent farming.

CONFLICT-OF-INTEREST DISCLOSURE

This research declares no conflict of interest.

FUNDING

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

REFERENCES

Abdelsalam, M., Krishnan, R. & Sandhu, R., 2019. *Online malware detection in cloud auto-scaling systems using shallow convolutional neural networks.* Switzerland, Springer, pp. 381-397.

Abubakar, A. A., 2020. Improving Cloud Data Security by hybridization of Zero- Knowledge Proof and Time-Based One-Time Password. *KASU Journal of Mathematical Sciences,* December, 1(2), pp. 116-126.

Abubakar, A. A., 2022. A SURVEY ON KNOWLEDGE AND COMMONSENSE REASONING FOR NATURAL LANGUAGE PROCESSING. *Scientific and Practical Cyber Security Journal,* 6(2), pp. 23-29.

Abubakar, A. A., Liu, J. & Gilliard, E., 2023. BLOCKCHAIN-BASED POISONING ATTACK PREVENTION IN SMART FARMING. *Scientific and Practical Cyber Security Journal,* 7(1), pp. 38-53.

Abubakar, A. A. & Shamsuddeen, A. U., 2023. Information Security: An Effective Tool for Sustainable Nigerian National Security and Development. *Scientific and Practical Cyber Security Journal,* March, 7(1), pp. 11-15.

Ahmad, Z. et al., 2017. *Performance evaluation of IEEE 802.15.4-compliant smart water meters for automating large-scale waterways.* Bucharest, Romania, IEEE, pp. 746-751.

Aung, M. M. & Chang, S. Y., 2014. Traceability in a food supply chain: Safety and quality perspectives. *Food Control,* 39(2), pp. 172-184.

Barreto, L. & Amaral, A., 2018. *Smart farming: Cyber security challenges.* s.l., ISI, pp. 870-876.

Chae, C. & Cho, J. H., 2018. Enhanced secure device authentication algorithm in P2P-based smart farm system. *Peer-to-Peer Network Application,* 11(6), pp. 1230-1239.

Chetan, D. M., Ganesh, R. R., Jagannathan, S. & Priyatharshini, R., 2015. *Smart farming system using sensors for agricultural task automation.* Chennai, India, IEEE, pp. 49-53.

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,* February, 15(4), p. 13.

Georgios, K., Constantinos, K. & Angelos, S., 2017. *The mirai botnet and the iot zombie armies.* s.l., IEEE, pp. 267-272.

Gill, S. K., Saxena, S. & Sharma, A., 2020. GTM-CSec: A game theoretic model for cloud security based on ids and honeypot. *Comput Secure,* pp. 10-21.

Grogan, A., 2012. Smart farming. *Engineering & Technology,* July , VII(6), pp. 38-40.

Gruschka, N. & Jensen, M., 2019. *Attack surfaces A taxonomy for attacks on cloud services.* s.l., IEEE, pp. 276-279.

Gupta, M., Mahmoud, A., Sajad, K. & Sudip, M., 2020. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access,* pp. 34564-34584.

Jahn, T. & Molly, M., 2019. *Cyber Risk and Security Implications in Smart Agriculture and Food Systems.* [Online]
Available at:
https://jahnresearchgroup.webhosting.cals.wisc.edu/wpcontent/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-andSecurity.pdf
[Accessed 11 2019].

Kim, H. & Laskowski, M., 2018. *Agriculture on the blockchain: Sustainable solutions for food, farmers, and financing, in Supply Chain Revolution..* Chile: Barrow Books.

Kolias, C., Kambourakis, G., Stavrou, A. & Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. *Computer,* 50(7), pp. 80-84.

Kushwah, G. S. & Ranga, V., 2020. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *J. Inf. Secure. Appl.,* 53(4), p. 102532.

Maanak, G. & Ravi, S., 2018. Authorization framework for secure cloud-assisted connected cars and vehicular internet of things. *23rd ACM on Symposium on Access Control Models and Technologies,* 5(4), pp. 193-204.

Madushanki, A. R. et al., 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,* 4 April, X(4), pp. 11-28.

Manos, A. et al., 2017. *Understanding the mirai botnet.* s.l., Unisex Security , p. 1093–1110.

Maria, B., Ali, Z., Gianluca, S. & Richard, K., 2014. Targeted attacks against industrial control systems: Is the power industry prepared?. *ACM Conference on Computer and Communications Security,* pp. 13-22.

Masoumeh, S. & Nasour, B., 2017. Passive secret disclosure attack on an ultralightweight authentication protocol for the internet of things. *The Journal of Supercomputing,* 73(8), p. 3579–3585.

Rabbani, M. L. et al., 2020. A hybrid machine learning approach for malicious behavior detection and recognition in cloud computing. *J. Netw. Comput. Appl.,* 151(4), p. 202507.

Roshanianfard, A., Noguchi, N. & Kamata, T., 2019. Design and performance of a robotic arm for farm use. *International Journal of Agricultural and Biological Engineering,* January, XI(1), pp. 146-158.

Santhana, P. & Biswas, A., 2023. *Blockchain Risk Management– Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy.* [Online]
Available at: https://www2. deloitte.com/content/dam/Deloitte/us/Documents/financial-services/usfsi-blockchain-risk-management.pdf, 2017, pp. 45-50.
[Accessed February 2023].

Shabadi, L. S. & Biradar, B. H., 2018. Design and implementation of IoT based smart security and monitoring for connected smart farming. *Int. J. Comput. Appl,* 179(11), pp. 1-4.

Sontowski, S. et al., 2020. *Cyber Attacks on Smart Farming Infrastructure.* Atlanta, GA, USA, s.n., pp. 135-143.

Sucuri, 2017. *IoT botnet: 25,513 CCTV cameras used in crushing DDoS attacks.* [Online]
Available at: https://www.csoonline.com/article/3089298/iot-botnet-25-513- cctv-cameras-used-in-crushing-ddos-attacks.html
[Accessed 02 2023].

Ukil, A., Sen, J. & Koilakonda, S., 2011. *Embedded security for Internet of Things.* s.l., s.n., pp. 1-6.

West, J., 2018. A prediction model framework for cyber-attacks to precision agriculture technologies. *Journal of Agricultural Food Information,* 19(4), pp. 307-330.

Window, M., 2019. *Security in precision agriculture: Vulnerabilities and risks of agricultural systems,* Luleå, Sweden: s.n.

WorldBank, 2022. *Agriculture.* [Online]
Available at: https://www.worldbank.org/en/topic/agriculture/overview
[Accessed 23 Sep 2023].