

Accessing the Impact of Smart Farming on Cybersecurity and Food Security Among Rural Farmers in Ekiti State, Southwest Nigeria.

Olatunji Oluwadare, Adeniji Oluwashola David

Department of Agricultural Economics, University of Ibadan
Department of Computer Science, University of Ibadan

Date of Submission: 01-09-2025

Date of Acceptance: 10-09-2025

ABSTRACT

Food insecurity is a major problem in Africa. Due to the increase in Population in Nigeria, there is a significant rise in the poverty index rate due to low agricultural production. Farmers adopt the traditional means of agriculture because it is cheap, affordable and is not technological driven. The output of this traditional means of agriculture as well as high cyber insecurity. The introduction of smart agriculture, farmers are gradually migrating from their primitive way of agriculture to the technology way of advancing agricultural production is a major transformation in smart farming. Farmers are using advanced computing devices to solve basic agricultural problems. However, cyber criminals are exploiting the vulnerabilities of this smart systems via cyber insecurity with the aim of inducing losses to farmers. Cyber security has greatly influenced food insecurity. In this research study, five hundred farmers were selected randomly in various Local Government in Ekiti state – Nigeria. They were segmented into two (2) various groups of those using primitive farming and smart farming. The productivity of both were evaluated to see the impact on smart farming to primitive agriculture. A network intrusion detection system was setup in the Database of those using smart agriculture to record the cyber-attack. The result shows that those that were vulnerable to cyber-attack has less food security compared to those without cyber-attack. This journal evaluates the effect of cyber security on food security and suggests ways of mitigating such cyber attack in order to reduce the influence of cyber security on food security.

Keyword: cyber security, food security, cyber criminals, poverty index, food production

I. INTRODUCTION

• The New Millenium welcomes the arrival of internet technology, Mobile Phones, and lots of Technological innovations in Nigeria. This has brought massive growth and development in various aspect of economic development including Agriculture. Agriculture is the main occupation of Nigerians before the discovery of Crude Oil

In 1956. Despite the economic impact and influence od crude oil, Agriculture still accounts for up to 35% of total employment in 2020.

(...et al, 2021,,...et al, 2022)

The Agricultural sector in Nigeria comprises of basically four sub-sectors which include Crop Production, Livestock, Forestry and Fisheries. The Major Crops Planted in Nigeria include Yam, Maize, Cassava, Guinea corn, Groundnut etc.

Most farmers in the rural areas of Nigeria including Ekiti State complain of inadequate Rainfall, Poor Storage facilities, limited labor force, Rural Urban migration, lack of Electricity, insufficient amenities, the effect of pest and weed on the crops etc. these and other challenges are affecting the cultivation of Crops and Animal in large quantity. Rural Farmers have consistently used the Traditional methods of Agriculture until recent technological developments. These developments include the introduction of Computer Systems, Hardware, Software, Networks sensors and IoT. The adoption of this Technology into Agriculture is the basics for Smart Agriculture. The Agricultural sector generates

\$5,084,800 million, or 6.4% of global economic output in the United State. The U.S. gross domestic product (GDP) in 2017 was \$1.053 trillion, which came from the food, agriculture, and other industries. With a total of \$5,084,800 million, the agriculture sector contributes 6.4% of global economic output. Food, agriculture, and associated sectors added \$1.053 trillion to the GDP of the United States in 2017 (John et al, 2017). The population of Nigeria is estimated to be around 230 million (World meter, 2024) as a result of increase in population, there is more demand for food. (FAO, 2024).

The continual rise in population has led to more demand for food and agricultural resources (Food Security Portal (2014) Food Security Portal-Nigeria. <http://www.foodsecurityportal.org/nigeria> [Citation Time(s):2]

Nigeria is endowed with a wealth of natural and human resources, but the majority of its people live below the poverty line. The primitive and local way of producing crops and livestock production is not enough to meet up with the demand of daily leads-leading to food insecurity.

WDI, (2020), over 75% of Nigerians live on less than US\$1.25 per day. Nigeria is ranked 110th out of 127 nations that were evaluated in 2024 by the Global Hunger Index. This implies that Nigeria has a severe level of hunger, as indicated by its score of 28.8 on the 2024 Global Hunger Index.

<https://www.globalhungerindex.org/nigeria.html>

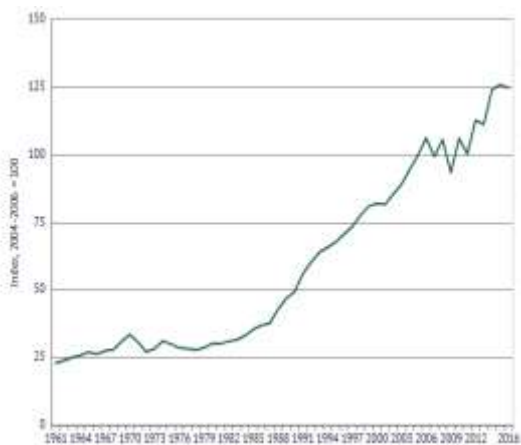


Fig 1.0: Nigeria food production index from 1961-2016. Source: world development indicator

As a result of these challenges, most economy are implementing Smart Agriculture as a means of optimizing agricultural production for efficient food security.(....et al, 2023)

II. TRADITIONAL MEANS OF AGRICULTURE

The Traditional means of A agriculture is the Primitive and local way of practicing agricultural processes. This includes:

- Land preparation- Bush Burning, Crop rotation, application of Manure etc.
- Use of farm Tools for cultivation such as the use of cutlass, Hoes, Rakes, Shovel, Fork, Knives, Wheel barrow etc.
- Weeding the Manual removal of Weeds from plant
- Irrigation: the use of buckets, containers to take water from streams, rivers to the farmland. At times, animals are used as a means of moving water from rivers to farmlands
- Storage: this includes the use of Silos, Bags, Nylon, as a means of storing agricultural produce. etc



Fig 2.0: The use of Bag to store and Beans



Fig 3.0: The use of Animals for irrigation system in a farmland.

The Increase in Population and more demand for human consumption, adoption of the Smart farming system is an integral part of any economy (...et al, 2023) the traditional means of farming has lots of demerits which are listed below

- Low productivity
- Low income
- Precious time is wasted
- More manual labor is used
- Flooding and erosion

- Destruction of precious produce
- No proper record
- Delayed processes
- Production is extremely low compared to demand
- As a result, Farmers are adopting the smart farming as a better means of agriculture compared to the traditional method of Agriculture.

III. SMART FARMING

Smart farming is usually the application of IoT devices, Sensors, Network, Computers, Hardware, Software Artificial intelligent systems to drive Agricultural operations in farms. This is faster, better, with high level of accuracy and precision compared to the traditional way of cultivation. These have helped to brought massive increase to the per capita income of farmers, increase agricultural produce exponentially, and also made farming operations easy and more efficient and with more accurate precision. (Ju et al, 2024)

It involves the adoption of advanced technologies and data-driven farm operations to optimize and improve sustainability in agricultural production.

It enhances operational efficiency by providing real-time data on crop conditions, weather & soil health, allowing farmers to make data-driven decisions, optimize resource allocation, and reduce waste.

Smart system of Agriculture is currently the method used in Europe and Asia. This is one of the keys to their massive produce and economic development. (Tue et al, 2022)

Various Technologies are been introduced into Farming processes in order to increase the rate of production at a geometric and exponential rate. This is because Food is a necessity for every human being. Such Technologies include

1. Hardware
2. Software
3. Artificial intelligence
4. IoT
5. Internet
6. Sensors
7. Machine Learning and Deep Learning
8. Data Analytics

a. Hardware

One of such is the development of Computer Drone and the Unmanned Aerial Vehicle (UAV). A Drone is a flying robot or aircraft that is designed to fly through a region without a pilot. In the Military it can be used to spy the enemy or to give information or data about others. Agricultural drones are designed using computer Hardware and software with a camera

and some other component. They can be used for the monitoring of livestock, soil surveillance, irrigation, planting of seed, harvesting of crops, spraying of insecticides, protection of crops, planting of seed etc Drones can also be used to monitor the health of animals in a farm.

b. Software -

Farm software is designed to take farm data, farm inventory, farm stock and financial transactions in the farm are recorded in a farm management software.

Farm Management Software (FMS) is an integral aspect of smart farming. They have a user-friendly interface for ease of administration. Some are designed as a mobile application for easy access remotely. Farm Managers do not need to physically at the farm to identify the quantity of food consumed by day by the livestock, the remaining food, the number of weakling animal, the gestation period and other information that is relevant to the farm. Data gathered from the farm can also be used for data analytics and business intelligence evaluation.

c. Artificial Intelligence

The introduction of A.I. into Agriculture has helped to revolutionize the Agricultural sector. It combines the Deep learning and Machine learning, with robot to solve agricultural activities within the shortest time. The Covid -19 was pandemic was a global disaster that had a major effect on every facet of human activities including the agricultural sector. Businesses were shut down; farmers were incarcerated and the adoption of digital technology was evidently seen. Artificial intelligent Systems and Machines created in forms of robots to solve agricultural problems. These complex machines incorporate various sensors and integrated chips for automation in agriculture. Farmers are utilizing A.I for efficient & remote management solutions in precision agriculture.



Fig 4.0: The use of Mobile Phone and Application for Smart Framing



Fig 5.0: The use of Drone for smart Agriculture

d. Machine Learning and Deep Learning

Machine Learning and Deep Learning are two (2) aspects of the Artificial Intelligence field that has helped to solve agricultural problems either independently or collectively. Machine Learning involves the use of data to make predictions without been explicitly programmed to do so. Farm data are used to make predictions on weather, rainfall, Plant performance, Animal and Livestock Production etc.

Deep learning is an index of Machine Learning that uses Neural Networks, to simulate the complex decision-making power of the human Brain. Neural Networks are created to work in farms, to increase agricultural produce. Machine learning and deep learning are integrated to solve problems.

e. Sensors

Sensors is device that detects and responds to some type of input from the physical environment. Sensors are used to design Temperature Sensors, Humidity sensors, Pressure sensors, underground wireless Sensory Network, Mobile wireless sensory network, underwater wireless sensory network. These are used to check the health of animals, Plant, Livestock and the atmosphere. They are also used to build smart machines agricultural systems. (et al, 2022)

IV. FOOD SECURITY

The term “food security” emerged at the World Food Conference in the middle of the 1970s. it was defined as "ensuring the availability and price stability of basic foodstuffs at the international and

national level" According to (FAO, 2024) Food security is when People have physical and financial access to enough food to meet their nutritional needs for a productive, healthy existence both now and in the future. This definition lists a number of indicators that can be used to gauge how much food security a nation has attained. These indicators include availability, accessibility, affordability, utilization, stability, nutritious content, and an adequate national food supply. absence of food can be referred to as food insecurity. food insecurity is the absence of adequate access to food. When an individual, state or Nation cannot provide adequate food for its people or citizen and make such food available and accessible to its people, such individual, state or Nation is said to experience food insecurity. The food produced must be adequately available, accessible, affordable, fully utilized and stable frequently before food security is said to occur. Hence, if a nation produces adequate food but its not accessible and available to its citizen – it is food insecurity. All the components of food security must be achieved before food security can be said to occur. According to FAO, et al. (2024), the core determinants of food security are availability, accessibility, utilization and stability.

Food Availability: - is a cardinal point in food security. The physical presence and accessibility of wholesome, safe food at a given place and time is referred to as food availability. It is affected by things like the production, exchange, and distribution of food.

Food accessibility is another component of food security. This refers to having access to the food commodity. Some factors could limit food accessibility which include but not limited to poor transportation, weather condition, cyber insecurity, kidnapping, inadequate preservation etc. Example-food may be available in a store house but not accessible because the online platform has been compromised by cyber hackers- though the food is available but not accessible. In such situation, food insecurity is said to occur because one of the components of food security is unsettled.

Food utilization is another aspect of food security. In order to achieve a state of nutritional well-being when all physiological needs are satisfied, the human body must be able to absorb and metabolize food through a sufficient diet, clean water, proper sanitation, and medical attention. It is measured by two indicators. The first result is determined by the nutritional status of children under five, while the second is determined by food quality, health, and hygiene. (Matemiola and Elegebde 2017)

Food stability is the fourth component of food security. This involves exposure to short-term

hazards might jeopardize long-term progress, which is related to stability. The Key indicators for exposure to risk include climate shocks such as droughts, erosion and volatility in the prices of inputs for food production. Nigeria's food production index dropped from 125.8 in 2015 to 124.6 in 2016, a 0.97% decrease. In 2016, the food production index increased by 0.51% since the 11.54% increase in 2014.

(<https://opendataforafrica.org/atlas/Nigeria/Food-production-index>)

Effect of smart farming food security

Since the adoption of Smart Farming, the farm production has increased tremendously in production. Farmers can rely on Smart Farming as a means of meeting up with consumers demand to attain food security. In Europe and continent, where this method is primarily adopted and implemented, it has positively affected various aspect of life. It has helped to achieve the following-

- Abundance of food production
- Prediction of weather forecast and Organized irrigation system
- Online Technology
- Application of insecticides and fertilizer
- Erosion control and Pest Control
- Increased income and resources to farmers and countries
- Advanced storage devices and Online Technology
- Artificial Intelligent system

CYBER SECURITY AND FOOD SECURITY.

The practice of defending programs, networks, and systems from unwanted threats is known as cybersecurity. This entails guarding against unwanted access to Data, Software, Hardware, etc. Cyberattacks typically try to disrupt farming operations, extort money from users using ransomware, or access, alter, or delete important information. A ransomware assault in January 2021 cost a U.S. farm \$9 million, forcing it to temporarily halt operations.

The Federal Government of Nigeria received reports of 12.99 million cyberattacks during the 2023 National Assembly and Presidential elections. The assaults occurred between February 24 and February 28, 2023.

According to the NCC, Nigeria loses about \$500 million annually as a result of cybercrime. Patricia, a cryptocurrency platform based in Nigeria, reportedly lost about \$2 million to hackers in 2022. The Federal Bureau of Investigation (FBI) ranked

Nigeria as the 16th most cybercrime-affected country in 2020.

(<https://punchng.com/almost-13-million-cyber-attacks-recorded-during-polls-fg/>)

Every computer driven machine (Hardware or software) is prone to cyber-attack. Cyber criminals and hackers are constantly exploiting the vulnerabilities of this IoT machines in order to induce losses on its victim, data destruction, financial and personal data theft, intellectual property theft, lost productivity, embezzlement, fraud and service disruption and make financial gain. Such cyber-attack has caused high level of food insecurity in the agricultural sector. Such attacks include DOS, Man in the middle attack, zero-day attack, password guessing and ransomware etc. cyber security is a concept that is used for securing and protecting computers driven devices against unwanted intruders and cyber hijackers. Most farmers are not exposed to cyber security and its principles, most of them who are victim of food insecurity via cyber criminals' activities are forced to either pay a ransomware or be grounded in their daily activities. Cyber criminals have caused high level of food insecurity, and caused lots of financial losses to farmers, reduced farming activities and also frustrate lots of farming operations. Cyber criminals have the ability to underfeed your livestock, overspray or under spray insecticide, reduce quantity of fertilizer on a farm, destroy farmland, make agricultural product inaccessible by either compromising the domain or making it inaccessible. They can also hack into the systems and disabling the control, and Networks of the devices. They could compromise the WIFI, reduce the internet activities by loading unnecessary application to frustrate the system. Introduction of virus, worms, trojans, malwares etc. could be another medium just to ensure smart farming is rendered incarcerated. This kind of attack is referred to as Cyber Agroterrorism (Luis et al, 2018).

- Various aspect of the agricultural farming are victims of cyber-attack which include but not limited to, Crop production
- Livestock farming
- Dairy production
- Poultry farming
- Aquaculture
- Meat processing
- Grain milling
- Food packaging

- Beverage production
- Food retailing
- Distribution and logistics

the effects of this cyber-attack often leads to,
Operational downtime,
Damage of the farmland

The crop or food produced that is available for
consumption standard is reduced

The welfare of the animal is also compromised

There is a disruption in the supply chain

There is a heavy financial loss.

According world health organization, Food security is the state in which everyone, everywhere, has physical and financial access to enough wholesome food that satisfies their dietary requirements and tastes for an active and healthy living. (FAO 2024). Food security will ensure that every one have the right quantity of nutritional diet daily for a healthy living. However, study has shown that cyber security has greatly affected food security in Nigeria . Cyber security is a concept that helps to secure computers, software, systems, database, website, Network and computer infrastructures against zero-day attack, cyber-attack, hackers and cyber criminals from exploiting the vulnerabilities of such. Such vulnerabilities include, insecure database, weak password, inadequate security, weak algorithm for encryption, predicted interface, deciphered code, expired antivirus, worms, trojans, malwares, spywares, and non- updated application that has caused severe losses to farmers who use E- computing for the management of their farm produce. The population of Nigeria is estimated to be over 230 124 315, million as at October, 2024 (world meter, 2024), while Nigeria is regarded as the most populous black nation earth. Approximately 690 million people worldwide experienced hunger in 2019, and 135 million people in 55 countries and territories experienced severe food insecurity, with 73 million of those people living in Africa. Nigeria is one of the worst of the 113 countries chosen, according to its Global Food Security Index (GFSI) ranking for 2022. If this reduction in food security is not completely eradicated, the nation may deteriorate, slow down, and descend into abject poverty.

REASONS FOR FOOD INSECURITY IN NIGERIA.

Several factors were responsible for Food insecurity which include:

- I. Traditional Means of Agriculture
- II. Gender inequality
- III. Inefficient Policies and Corruption
- IV. Conflicts and Civil Insecurity

V. Climate Change and Natural Disasters

VI. Low Processing and Storage facilities

VII. Nigerian Food Security Policy Review
Cyber insecurity

V. RELATED WORKS

Intelligence report by the US food and agriculture shows that over 167 ransomware attacks was experienced in the year 2023 (...ty et al, 2021)

Data received from FBI in 2023 shows that 2,825 ransomware complaint was experienced in various sectors in the United States of America. This led to \$59.6 billion, and 1,193 of such ransomwares were involves major sectors including the food industry. (<https://extension.sdstate.edu/growing-threat-cyber-attacks-agriculture>)

In January 2021, a U.S. farm lost \$9 million in a ransomware attack, which resulted in a temporary shutdown of its operations. (<https://extension.sdstate.edu/growing-threat-cyber-attacks-agriculture>)

According to studies, hackers launch an assault every 39 seconds. Nigeria is not immune to cyberattacks on its citizens, companies, and vital infrastructure; the COVID-19 epidemic and other unjustified factors are contributing to an increase in cyberattacks in our nation.

(<https://www.presencesecure.com/cybersecurity-food-security-nigeria/#:~:text=Attack%20on%20industrial%20control%20systems,point%20A%20to%20point%20B>)

The data consumed by internet subscribers has increased exponentially, as at July 2024, Nigeria's monthly internet consumption increased from 125,149.86 terabytes (TB) in December 2019 to 753,388.77 TB in March 2024, according to the Nigerian Communications Commission (NCC).

(<https://businessday.ng/technology/article/nigerias-digital-boom-threatened-as-fg-issues-33-alerts/>)

According to a recent Threat Intelligence Report by Check Point Research, Nigerian companies see over 2,308 attacks per week in all industries. Nigeria experienced the second-highest number of cyberattacks in Africa and the 50th most worldwide, citing a June 2023 Kaspersky report. (<https://businessday.ng/technology/article/nigerias-digital-boom-threatened-as-fg-issues-33-alerts/>)

12.99 million cyberattacks were reported to the Federal Government during the 2023 presidential and National Assembly elections. The attacks took place from February 24 to February 28.

The NCC estimates that cybercrime costs Nigeria roughly \$500 million a year. According to reports, Patricia, a Nigerian cryptocurrency platform, lost almost \$2 million to hackers in 2022. Nigeria was listed by the Federal Bureau of Investigation (FBI) as the 16th most cybercrime-affected nation in 2020.

[\(https://businessday.ng/technology/article/nigerias-digital-boom-threatened-as-fg-issues-33-alerts/\)](https://businessday.ng/technology/article/nigerias-digital-boom-threatened-as-fg-issues-33-alerts/)

The Introduction of information technology, computers, systems and internet of things (IoT) to agricultural practices is often referred to as smart farming or smart agriculture. Smart farming makes use of smart networking, mobility, interoperability and flexibility in agricultural operations, business model innovation, and interaction with suppliers and customers. (Kamilaris et al. 2017). It involves intelligent systems that can take a proactive decision in real time to optimize agricultural practices. (Barreto et al. 2017). This intelligent device includes but not limited to sensors, communication devices, integrated circuits, Routers, switches etc. the future of agriculture is evidently seen in smart agriculture where Artificial intelligent machines will be involved in basically all farming operations, from cultivation of soil, to spraying of insecticides, application of fertilizers, weeding, harvesting, storage etc.

The potential for cybercrime is growing daily these days. The usage of ICT and IoT in agriculture is raising the level of exposure of this industry, and new types of cyberterrorism attacks are being reported. As a result, the agriculture industry is increasingly susceptible to cyberattacks on its production facilities and infrastructure.

The World Health Organization (WHO) reports that 600 million people become ill each year as a result of food contamination by bacteria, viruses, and chemicals, 10 million people pass away from food-related illnesses.

According to the World Health Organization (WHO), more than 10 million people die each year from food-related illnesses, and 600 million people get sick because food is contaminated with bacteria, viruses, chemicals. In order to mitigate and reduce this risk, economy that introduces IoT tends to reduce the number of lives lost to those hazard-

Hasan et al. in his journal titled 'Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems' proposed the use of Industrial control systems (ICSs) as a security measure to identifying food security. He proposed an anomaly detection using an artificial intelligence algorithm. This was focused primarily to detect: man-in-the-

middle (mitm) attack, web-server access attack, and telnet attack. This was implemented to enhance food security van der et al conducted research that was published in December 2020 titled 'Cybersecurity for Smart Farming'. In his research, he explained how agri business has suffered losses due to cyber incident. He explained how food availability, production and distribution can be delayed by cyber-attacks. He concluded that there is an urgent need to protect systems for malicious attacks that could lower or reduce agricultural production.

Lu's Barreto and Antonio Amaral collectively did comprehensive research on the challenges of cybersecurity on smart farming in 2018. The combination of information technology, computer innovations and Internet of Things (IoT) has greatly impacted smart agriculture. Despite the positive impact of smart farming in boosting and optimizing agricultural production, lots of vulnerabilities are been experienced which tends to reduce the performance of such devices. Some of the problems faced by smart farming leading to food insecurity were highlighted in his paper.

Zsanett et al. embarked on tripartite research and published his journal in 2021 in his paper titled "the importance of cyber security in, modern agriculture" in his research work, he estimated the population of the world to be approximately 11 billion by 2100 and there is a need to increase the quantity of food produced to be able to meet the daily need of everyone. For this to be achieved there must be maximum cyber security measures installed to reduce cyber warfare that may lead to reduction in agricultural food production. He explained that agricultural systems connected to the internet via website could be easily compromised by cyber criminals if there are not enough security techniques to protect them. Data acquired by cyber criminals could be used to exploits agriculturist and farmers to cause lots of harm and losses which include financial, mental, material, data loss on its victim.

Andrew Geil et al conducted research in a 2017 titled, "Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry" he used health believe farmer work as a model to evaluating the effect of cyber security on farmers and Agric business. In his survey those that are prone to cyber-attack were those who did not implement cyber security into their systems. Those who neglected the principles of cyber security were more vulnerable to cyber-attack unlike those who took security measures in place.

Researchers from Scuri, a security company, found that a DoS botnet could send out 50,000 HTTP requests every second [scurry, 2020].

Here, DDoS attack was used against a number of websites.

Similar circumstances are present in the ecosystem of smart farming. As a result, comparable attacks could occur in the context of smart farming.

In addition to interfering with the regular operations of various modules inside a single farm, these assaults can be used to impair trustworthy cyber services in other domains.

The Importance of Cybersecurity in Protecting Smart Farming.

The Protection of smart farming is very important for the continuity and availability of food production. It helps in the following areas:

- Protects personal data.
- Protects business reputation.
- Enhances productivity.
- Assists remote working.
- Ensures regulation compliance.
- Enhances cyber posture.
- Improves data management.
- Helps educate the workforce.
- Helps in protecting farm software

TYPE OF CYBER-ATTACKS ON SMART FARMS

Most farms are not aware that their data has been compromised nor attacked until they get a ransomware message. This is because they have little knowledge on cyber security while some do not have the technical know how to prevent, or mitigate such incoming attacks. Most of these attacks are rarely predicted, hence most farmers operate at the mercy of the cyber criminals. Some of the cyber-attack experienced are discussed below:

a. Denial of service attack (DOS)

This is a type of attack is mainly experienced by farmers, who use online platform and website for the sales and marketing of their agricultural produce.

A denial of service (DoS) attack is an attempt to overload a website or network, with unnecessary traffic with the aim of making either the website inaccessible or to reduce its performance. In DOS attack, the cyber attacker uses various method to deny the service or make the service of the smart machines and farms unavailable. This may result in slow computer processes, system hanging, malfunctioning, operating at variance to the instruction of the user and making works frustrating. It can even lead to system shutting down consistently and making web payment platform inaccessible, not responsive and service denied. Example – is trying to affect a payment for

various food items and the system is not inputting the actual digit- this can make work frustrating and make food unavailable to end user – causing food insecurity. This is one of the most common forms of cyber-attack experienced by farmers in Ekiti state- Nigeria

b. Zero-day Attack

There are some forms of cyber attacks that are rarely predicted because of its cryptic nature. When vulnerabilities are seen or detected in a software, systems or networks – the same day it is detected, cyber attackers exploit such vulnerabilities on its victim to induce massive losses and request for a ransomware. Zero-day attack are been experienced in Mobile application, banking software, website and in Networks. Hackers are consistently seen making research on developed software in order to launch an attack. This has rendered farming operations and smart farming redundant and stagnant for a particular period until its vendor gets a solution to this kind of attack.

c. Password Guessing attack

This is a type of attack that the attacker either guess or use some Artificial intelligent tool to guess the password of the WIFI, system, Network or website. Most farmers in the rural areas use their names, date of birth, name of the parents and environment as the password of their WIFI, Internet or systems. Hackers usually guess this and exploits the vulnerabilities to induce loss to its victim and also steal their tool. Some pretend to make purchases and request for their WIFI password to login to internet banking and scan on other devices to keep on using. Some artificial intelligent tool are also used for guessing and for hacking into unsecure database and wifi used by smart farms for their respective operations.

How to Protect Farm Data from Cyber Hackers.

Any organization or nation that wants to imbibe smart technology needs adequate cyber security to protect its database, system, Network, website from unnecessary Intruder. The following steps has been outlined as some of the possible ways of mitigating cyber-crime on smart devices. In Nigeria, Pirated Software is been used by over 95% of most users (Mik et al 2023). This counterfeiting software are installed as Operating systems, Users software on Desktops, Laptops etc. if installed on Farm- Data can be compromised. The following tips has been outlined as part of the ways of protecting Smart Farming Devices from been compromised

1. Original Operating system with license key

2. Original Antivirus
3. Original Antimalware, Antispyware, Anti -worms and Anti trojans
4. Updated application regular
5. Using alphanumeric password
6. Frequent change of password
7. Secured wifi-key

VI. LIMITATION

One of the major challenges with this research work is the non-availability of funds. Limited funds limited the scope and dimension of this research work.

VII. CONCLUSION

Nigeria is the target of cyber attackers because of its adoption of Smart Agriculture, and Technology. Many Businesses and farming operations has been reduced because of the cyber hacking causing high level of food security.

Inadequate cyber security measures can leads to high level of food insecurity Cyber security has a direct Impact on food insecurity. There is an urgent need for Researchers, scientist, scholars to engage in more research in the areas of cyber security in smart farming as Nigeria is progressing in the areas of smart farming

REFERENCES

- [1]. <https://therecord.media/food-and-agriculture-hit-with-ransomware-attacks>
- [2]. John V Stafford. Precision agriculture'19. Wageningen Academic Publishers, 2019
- [3]. Muhammad Shoaib Farooq, Shamyala Riaz, Adnan Abid, Kamran Abid, and Muhammad Azhar Naeem. A survey on the role of iot in agriculture for the implementation of smart farming. IEEE Access, 7:156237 156271, 2019.
- [4]. Lu'is Barreto and Antonio Amaral. Smart farming: Cyber security challenges. In 2018 International Conference on Intelligent Systems (IS), pages 870–876. IEEE, 2018.
- [5]. Shawn Cupp, David E Walker, and John Hillison. Agroterrorism in the us: key security challenge for the 21st century. Biosecurity and bioterrorism: biodefense strategy, practice, and science, 2(2):97–105, 2004.
- [6]. Sucuri. IoT botnet: 25,513 CCTV cameras used in crushing DDoS attacks. <https://www.csoonline.com/article/3089298/iot-botnet-25-513-cctv-cameras-used-in-crushing-ddos-attacks.html>. [Online]. David, A. O., & Oluwasola, O. O. (2020).
- [7]. Zero-day attack prediction with parameter setting using bi direction recurrent neural network in cyber security. International Journal of Computer Science and Information Security (IJCSIS), 18(3), 111-118.
- [8]. John V Stafford. Precision agriculture'19. Wageningen Academic Publishers, 2019. [2] Muhammad Shoaib Farooq, Shamyala Riaz, Adnan Abid, Kamran Abid, and Muhammad Azhar Naeem. A survey on the role of iot in agriculture for the implementation of smart farming. IEEE Access, 7:156237 156271, 2019.
- [9]. Deepak Vasisht, Zerina Kapetanovic, Jongho Won, Xinxin Jin, Ranveer Chandra, Sudipta Sinha, Ashish Kapoor, Madhusudhan Sudarshan, and Sean Stratman. Farmbeats: An iot platform for data-driven agriculture. In 14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17), pages 515–529, 2017.
- [10]. Andreas Kamilaris, Feng Gao, Francesc X Prenafeta-Boldú, and Muhammad Intizar Ali. Agri-iot: A semantic framework for internet of things-enabled smart farming applications. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pages 442–447. IEEE, 2016.
- [11]. Sjaak Wolfert, Lan Ge, Cor Verdouw, and Marc-Jeroen Bogaardt. Big data in smart farming—a review
- [12]. Sontowski, S., Gupta, M., Chukkapalli, S. S. L., Abdelsalam, M., Mittal, S., Joshi, A., & Sandhu, R. (2020, December). Cyber attacks on smart farming infrastructure. In 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC) (pp. 135-143). IEEE.
- [13]. Hemavathi B Biradar and Laxmi Shabadi. Review on iot based multidisciplinary models for smart farming. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pages 1923–1926. IEEE, 2017.
- [14]. Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. Security and privacy in smart farming: Challenges and opportunities. IEEE Access, 8:34564–34584, 2020.
- [15]. BBC. Hack attack causes 'massive damage' at steel works. <https://www.bbc.com/news/technology-30575104>. [Online]. [13] Aida Boghossian et al. Threats to Precision Agriculture. Technical report, U.S. Department of Homeland Security, 2018.

- [16]. Molly M. Jahn et al. Cyber Risk and Security Implications in Smart Agriculture and Food Systems. at : Available <https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf> (Accessed on: 2019/11/14), 2019.
- [17]. Daniel Lopez, Maria Uribe, Claudia Santiago, Andr es Torres, Nicolas Guataquira, Stefany Castro, Pantaleone Nespoli, and Felix Gomez Mar mol. Shielding iot against cyber-attacks: An event-based approach using siem. *Wireless Communications and Mobile Computing*, 2018, 10 2018.
- [18]. Constantinos Koliass, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.
- [19]. Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In 26th {USENIX} Security Symposium ({USENIX} Security 17), pages 1093–1110, 2017.
- [20]. Sucuri. IoT botnet: 25,513 CCTV cameras used in crushing DDoS attacks. <https://www.csoonline.com/article/3089298/iot-botnet-25-513-cctv-cameras-used-in-crushing-ddos-attacks.html>. [Online].
- [21]. Tarini Tyagi. Botnet of things: Menace to internet of things.
- [22]. Georgios Kambourakis, Constantinos Koliass, and Angelos Stavrou. The mirai botnet and the iot zombie armies. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pages 267–272. IEEE, 2017.
- [23]. Matemilola, S. and Elegbede, I. (2017) The Challenges of Food Security in Nigeria. *Open Access Library Journal*, 4: e4185. <https://doi.org/10.4236/oalib.1104185>