Internet of Things-Based Agriculture: A Review of Security Threats and Countermeasures.

Onoja Emmanuel Oche[*], Suleiman Muhammad Nasir[**], Alhassan Hauwa Muhammed [**]

[*] Department of Cyber Security Federal University of Technology Minna, Nigeria
[**] Computer Science Department, Federal polytechnic Nasarawa Nigeria

DOI: 10.29322/IJSRP.10.08.2020.p10494
http://dx.doi.org/10.29322/IJSRP.10.08.2020.p10494

Abstract- The agriculture sector is gradually becoming more digitalize with large integration of Internet of Things into various farming processes such as land cultivation, farm monitoring, product processing, food marketing and consumers-farmers interaction. This paradigm shift from mechanical (or wired) agriculture technology to a wireless (or sensor based) agriculture system comes along with its own security challenges as viewed from cyber security perspective. This paper therefore provides an overview of IoT-based agriculture from cybersecurity perspective by (i) analyzing possible application of IoT devices in agriculture (ii) classifying IoT-based agriculture into four architectural layers (iii) analyzing security threats to IoT based agriculture and suggesting possible countermeasures based on IoT architectural layers for secure deployment of IoT devices in agriculture. With good consideration of threat and security requirements of IoT-based agriculture drawn from literature reviews, this paper presents possible countermeasures against attacks on IoT devices in agriculture. The proposed countermeasures prove to be highly secure against attacks on privacy, authentication, integrity, confidentiality and availability, with low power and time consumption. This research will assist researchers and agriculturists to choose the most suitable and flexible security mechanisms for IoT deployment in agriculture.

Index Terms- IoT, IoT-Based Agriculture, Smart Farming, Sensing Devices, IoT Threat Model, IoT Attack,

I. Introduction

In an attempt to address the problem of global food requirement, agricultural products exportation standard, economy diversification and digital economy, most developing countries (especially Nigeria) agricultural sector have started receiving more attention with gradual integration of modern digital technology and Internet of Things into various farming processes such as land cultivation, farm monitoring, irrigation, soil pH setting, product processing, food marketing and consumers-farmers interaction [1]. As developing countries' farming systems move towards embracing more advanced IoT deployment in water and soil quality monitoring, Intelligent greenhouses, milk and egg production, scientific disease and pest monitoring, the need to emphasize on IoT security become of great important [2].

Obviously, the primary purpose of IoT is the creation of interconnection between devices (such as computing devices), machines (both digital and mechanical machines), objects and people through applications using the web interface and mobile applications. In IoT network, sensor and actuator with unique attribute and identity usually communicate with each other to achieve certain functions such as perception, intelligent positioning, monitoring and tracking. This dynamic remote control in IoT network converts traditional control to an intelligent control thereby increasing efficiency and productivity [3]. Since all devices in IoT network need to interact with each other, security threats and attacks on devices, network and data become the greatest challenge [4, 5].

The concept of IoT-based agriculture involves the integration of IoT sensor, wireless communication, cloud computing, machine learning, big data technologies, and IoT technologies into agricultural (farming) processes in order to increase yield and quality of food products [6]. Advanced IoT technologies and solutions are incorporated into agricultural processes to minimize waste, maximize yield, and improve operational efficiency as in the case of underground remote sensors used for measuring blueberry irrigation in Chile which has reduced water wastage by 70%, and use of data analysis to predict and prevent crop diseases in India and Slovenia [7].

Although IoT based farming is highly beneficial and may help in solving the problem of food scarcity with the alarming population growth, but the deployment of heterogeneous interconnected devices comes along with its own potential cyber security challenges [8].

This research therefore presents an overview of IoT-based agriculture from cybersecurity perspective by (i) analyzing possible application of IoT devices in agriculture (ii) classifying IoT-based agriculture into four architectural layers (iii) analyzing security threats to IoT-based agriculture and suggesting possible countermeasures based on architectural layers for secure deployment of IoT devices in agriculture.

II. An Overview of IoT Ecosystem for Agriculture

Internet of Things interconnectivity involves the use of different technologies such as (computers, smart phones, smart watches, sensors, actuators and Radio-Frequency Identification (RFID) tags) for the purpose of information sharing and processing [9]. IoT is a global network of infrastructures based on standard and interoperable communication protocols where unique and identifiable devices interconnect using intelligent interfaces [10].

According to [11] IoT ecosystem for agriculture consist of four (4) components namely; IoT devices, communication technology, internet, data storage and processing (as represented in figure 1.0 below).

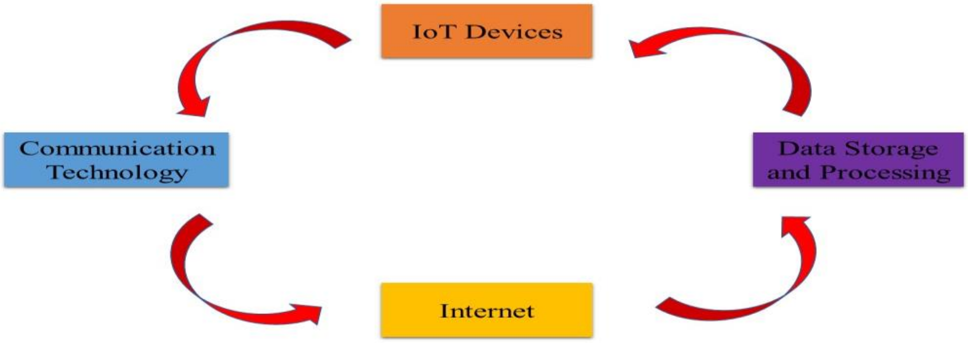

Figure 1.0 IoT Ecosystem

IoT sensors which may be mechanical, optical, electrochemical and airflow sensors are also known as IoT devices. They are made up of embedded systems with wireless connectivity to interacts with sensors and actuators. They are used to gather and monitor data on environmental variables (such as soil nutrients, rainfall, leaf wetness, wind speed, humidity, solar radiation and air temperature) responsible for plant growth and animal production [12].

The communication spectrum is a mean of cellular network data transmission mechanism which may be licensed (with high cost of subscription and power consumption during transmission as drawback) or unlicensed (with high interference rate and security flaws as drawback) [13].

According to [14], there are many standards for wireless communications. These may be grouped into short-range standard such as ZigBee, Bluetooth, Z-Wave, passive and active radio and long-range standard such as Sigfox Lora, and NB-IoT

In [15], it was observed that availability of IoT data across the globe is made possible through a core network layer component known as the internet. It provides connectivity of heterogeneous devices through the middleware and connectivity protocols such as the service-oriented architecture (SOA), cloud-based IoT middleware and actor-based IoT middleware.

Some agricultural information system developed to manage and store agricultural data are; the silent herdsman platform, Onfarm system, Farmlogs, Cropx, Easyfarm and KAA [16].

III. Application of IoT in Agriculture

Although there are numerous applications of IoT in agriculture, this research focuses on most recent applications of IoT in agriculture as represented in figure 3.0 below.

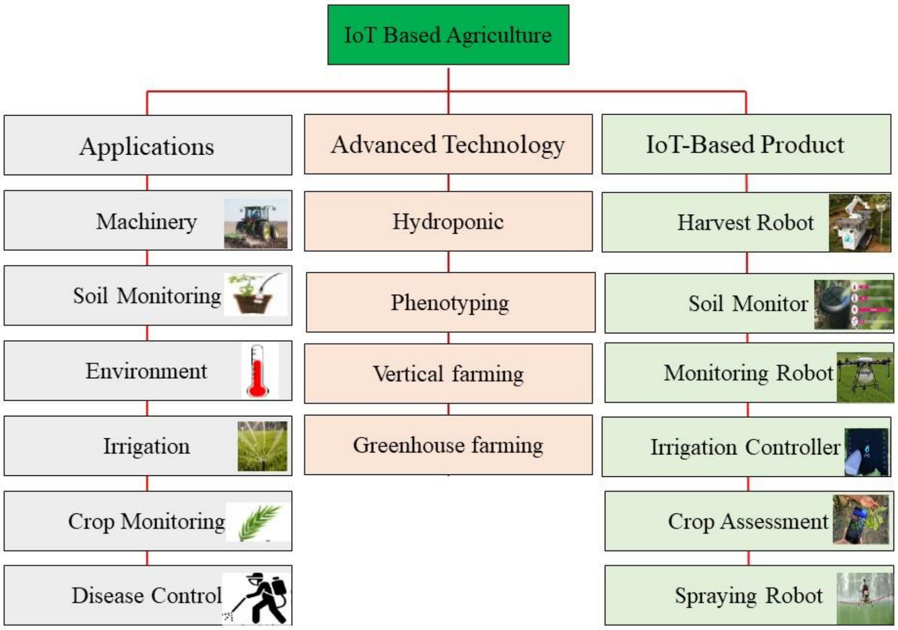

Figure 2.0 Application of IoT in Agriculture

The ability of IoT sensors to perform functions such as monitoring, tracking, tracing, precision and production have increased their applications in various fields of agriculture such as automation and precision farming, soil monitoring, irrigation monitoring, weather monitoring, greenhouse production, pest and disease control. The application of IoT in different field of agriculture shows the acquisition of agricultural data through different IoT sensors such as Wi-Fi, Zigbee, Bluetooth Sigfox, LTE-M1, LoRa and LTE-NB1. Such data are transmitted to the IoT cloud server through gateway which also receives commands (from the sever) that are sent for automation purposes. The cloud server supports services such as data storage, data analysis for decision making and visualization. This allows agriculturist to remotely manage farming processes via IoT devices [17, 18, 19].

According to [11], different factors in various agricultural areas can be monitored. IoT devices are applied based on their monitoring capability. The pattern and process of crop farming are affected by several environmental factors such as temperature, amount of rainfall, humidity, soil moisture, salinity, climate, solar radiation and pest movement. Collecting data on such factors enables proper planning and decision making in farm profit, risk and yield management. Libelium a company in Columbia, has installed several IoT kits to control such environmental conditions of the soil. This enables the farmer to get information about the humidity, temperatures, soil moisture, radiation and leaf wetness. Elaborating on other application areas of IoT based on its monitoring function, [20] mentioned that, IoT devices collate environmental factors data that can be used for automation purposes in other agricultural areas such as Aquaponics (a combination of aquaculture and hydroponics), forestry and livestock farming.

According to [21], using RFID and cloud base global positioning system, IoT devices are applied in tracking and tracing agricultural assets and products which allows data on the origin, location, life history, cropping environment, farming conditions, pest effect, storage conditions and supply time of products to be accessed along the supply chain.

According to [22], IoT applications have improved autopiloting in agricultural machineries such as vehicles, unmanned aerial vehicles (UAVs) and robots through GPS, proper mapping system and global navigation satellite systems (GNSSs). Such machines are controlled remotely based on available data collected through IoT system. Manufactural of agricultural machines such as CLAAS, implement IoT on their equipment, for purpose of auto pilot mode.

According to [24], IoT is applied in precision agriculture whereby advanced technologies such as Remote Sensing (RS), Geographic Information System (GIS) and Global Positioning System (GPS) that utilize wireless Sensor Network (WSN) are used to effectively reduce the potential risks in agricultural production processes which help farmers in making accurate and controlled farming processes and thereafter gathering important data (such as animal health, crop growth, environmental factors) required for agricultural production. The use of agricultural drones and other low-power, multi-function and wireless communication devices are remarkable application of IoT in precision farming.

According to [25] in precision agriculture, greenhouse where plants are grown in a controlled glasshouse, parameters are monitored and controlled through wireless sensor network technology. Mostly in field bus concept, hybrid systems wireless protocols such as ZigBee protocols based on IEEE 802.15.4 are used to control data transfer. IoT can be applied in greenhouse technology in order to achieve high efficiency, reduced human resource and low energy consumption [26].

IV. Application of IoT in Agriculture

Although there are different architectural layers of IoT-Based farming, this research grouped IoT-based agriculture into four different layers as represented in figure 3.0 below.

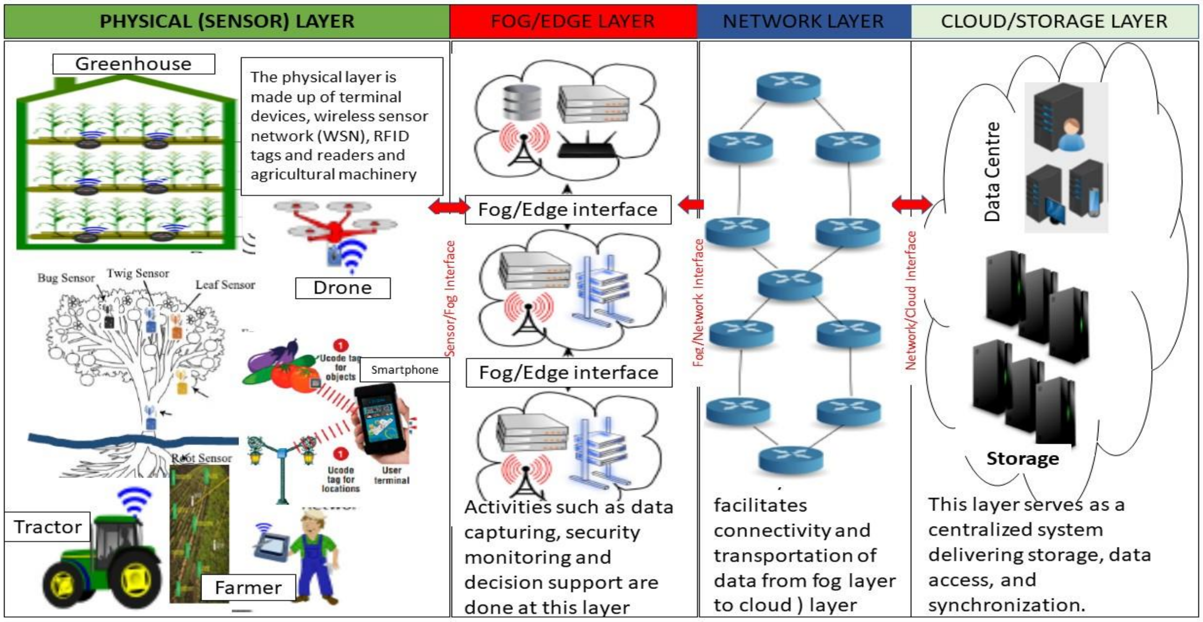
PHYSICAL (SENSOR) LAYER
FOG/EDGE LAYER
NETWORK LAYER
CLOUD/STORAGE LAYER
Greenhouse
The physical layer is made up of terminal devices, wireless sensor network (WSN), RFID tags and readers and agricultural machinery
Drone
Bug Sensor
Twig Sensor
Leaf Sensor
Root Sensor
Ucode tag for objects
Smartphone
Ucode tag for locations
User terminal
Tractor
Farmer
Sensor/Fog Interface
Fog/Edge interface
Fog/Edge interface
Activities such as data capturing, security monitoring and decision support are done at this layer
Fog/Network Interface
facilitates connectivity and transportation of data from fog layer to cloud) layer
Network/Cloud Interface
Data Centre
Storage
This layer serves as a centralized system delivering storage, data access, and synchronization.

Figure 3.0 IoT-Based Agriculture Architectural Layers

A. Physical (Sensor) Layer

The physical layer consists of sensors (such as optical sensors, electrochemical sensors, acoustic sensors, airflow sensors, field-programmable gate array (fpga)-based sensors, ultrasonic ranging sensors, optoelectronic sensors, mechanical sensors, electromagnetic sensors, eddy covariance-based sensors, soft water level-based (swlb) sensors, light detection and ranging (lidar), remote sensing) smartphones and other IoT-enabled devices equipped with Global Positioning System for developing different IoT technologies in IoT agriculture for hydroponic, phenotyping, vertical farming photovoltaic farm, solar insecticidal lamp, greenhouse and irrigation farming. Processes in IoT-based agriculture are controlled by digital control system (e.g. Supervisory Control and Data Acquisition (SCADA)). In this layer of the IoT based Agriculture, data such as wind speed, temperature, humidity, pest and diseases are collected by the sensing devices using protocol such as Zigbee and processed by embedded devices which are transmitted through the network for processing and analysis. Most times, installation of agriculture sensor is done in areas where they can be easily accessed and monitored. This may easily give attackers unauthorized access to sensing devices which may give room for physical attacks. Other security challenges of this layer are unauthorized capturing of sensing devices like drones, Denial of Service (DoS) attacks, timing and replay attack, routing threat and other attacks [12].

The physical layer of IoT is made up of terminal devices, wireless sensor network (WSN), RFID tags and readers and agricultural machinery. Most of the agriculture related sensors are soil sensors, water sensors, plant and animal data sensors. Agricultural data such as wind speed, temperature, humidity pest and diseases are collected by the sensing devices using protocol such as Zigbee and processed by embedded devices which are transmitted through the network layer to other higher layers for processing and analysis. Most at times, installation of sensing (perception layer) devices are done in area where they can be easily accessed and monitored. This may easily give attackers unauthorized access to sensing devices which may give room to physical attacks. Other security challenges of this layer are unauthorized capturing of sensing devices like drones, Denial of Service (DoS) attacks, timing and replay attack, routing threat and other attacks [21].

B. Fog Computing Layer

In order to save processing time of data generated by sensing devices in the physical layer and timely decision, data need to be processed closer to the IoT devices. This bring in the concept of Fog/Edge Computing in the architecture of IoT based agriculture. This layer is made up of multiple edge nodes, closer to the farmer and end-devices and reduces the workload on the network and centralized cloud layer. Activities such as data capturing (and data aggregation, filtering, encrypting and encoding of data), detection (anomaly detection and device failures prediction.), prediction (which mostly rely on machine learning models), security monitoring and decision support are done at this layer [27, 28].

C. Network (Connectivity) Layer

This layer facilitates connectivity and transportation of data through high speed networks such as 5G from fog computing layer to cloud (storage) layer [29]. It also provides interaction interface between the storage (cloud) layer. It binds all layers through means of communication [30, 31]. This layer controls routing by delivering interconnectivity of strategies-based network and transmit various agriculture data through a wired transmission channels such as CAN bus and RS485 bus or wireless transmission channel such as Zigbee, Bluetooth, LoRa and NB-IoT. It also sends controls command to the sensor or physical layer so that IoT devices can take necessary action.

C. Cloud Computing (Storage) Layer

This layer serves as a centralized system delivering storage, data access, and synchronization. It follows the platform as a service architecture, running applications and importing their data. Data pushed in from the edge layer are saved in distributed file system (DFS) which are mined using analytical software. Some examples of cloud computing platforms are Amazon Web Services, Google Cloud, John Deere Farmers Business Network. Some examples of IoT based agriculture data storage platforms are Easyfarm, Farmobile, the silent herdsman, Farmlogs, Onfarm and system [16, 32, 33].

IV. THREAT MODEL OF IOT-BASED AGRICULTURE AND COUNTERMEASURES

Attackers can orchestrate diverse attacks on IoT devices and data in smart farming. These devices are Heterogeneously interconnected and generate enormous amount of dynamic and spatial data. This data is used for day to day monitoring and control of the farm. Unauthorized access to such information may cause potential threat to agricultural processes. An attacker may use information leakage to bypass security measures, gain competitive advantages cause economic losses, Some IoT-based farms analyze collected data using third party agronomy analytics. Such parties may compromise IoT system, inject malicious code to redirect data transmission when given legitimate credentials to farm data on the edge for real time analytics [34, 35].

Discussing IoT device vulnerabilities [16] and [35], stated that, IoT devices are highly vulnerable to physical attack, tampering, theft, predators and animals. Some IoT devices use weak security algorithms with limited memory, high power energy consumption with gateway highly prone to attacks such as forwarding, congestion attack and denial of service (DoS). Sometimes, the IoT devices applied in precision agriculture are vulnerable to attacks such as device capture attack [35] whereby an attacker captures IoT device such as drones and extracts cryptographic implementations and gains unrestricted access to the information stored in the device's storage. The agriculture network layers can be vulnerable to DoS attacks, wireless signal jamming, and man in the middle attack [16]. The cloud layer is also very prone to data tampering, session hijacking, logon abuse, DoS, unauthorized services attack which can affect automated processes in the farms.

In IoT-based agriculture, interconnected objects such as flying drones, on field sensors and autonomous tractors communicate with each other either directly in the form of machine to machine (M2M) or through cloud based assisted network of which can support Message Queue Telemetry Transport (MQTT21), Constrained Application Protocol (CoAP22) or other IoT communication protocols. The major security issue here is authorization and trust issues. It is important that messages and commands are sent from trusted and secure entity rather than vulnerable and malicious entity This implies that only authorized entity and farm owner can send farm data on crop yield, livestock health, breeding and other important information [36].

IoT-based farms consist of interconnected entities which allows high rate propagation of malware through the network. Arriving at malware detection mechanism that perfectly fits into IoT based farming still remains a great security challenge as malware detection mechanism that works against malware in physical layer may not work in edge or cloud layer of IoT agriculture architectural layer. Although AI assisted malware detection techniques have been proposed but no IoT based farming malware detection system in specific [37].

In a situation where all devices are connected together in smart farming, IoT devices at each architectural layer can be prone to a remote-control attack such as botnet where zombies of infected systems are used to infect and attack other farm devices and network.

The Physical/Sensor layer which consist of physical IoT entities such as sensors, RFID tags, zigbee and bluetooth devices mostly developed in open fields are basically prone to physical attacks such as physical damage, malicious code injection, node tampering, mass node authentication, fake node and side channel attack. In some case of physical/sensor layer attack, an attacker may physically destroy sensor devices installed in open and closed area to cause physical denial of services. Sometimes the adversary may choose to add fake nodes to sensory systems and inject malicious code into the IoT network through the network. At times the adversary may attack the encryption mechanism of the farm devices by capitalizing on factors such as electromagnetic radiation, power and time consumption [12].

In the work of [38], researchers considered the network layer of IoT based farming to be vulnerable to attacks such as man in the middle attack, wireless signal jamming, DoS and DDoS. The cloud/edge layer is vulnerable to attacks such as unauthorized services, data tampering, logon abuse, session hijacking, SQL injection and DoS, which have adverse effects on automated processes.

Attacks on IoT devices in IoT-based farming was classified into different categories according to [23] which include attacks against confidentiality, integrity, availability, privacy and authentication. Explaining attacks against privacy, [23] pointed out that this type of attack is based on knowing and identifying the location and identity of IoT devices at the physical or sensor layer to gather privacy data and compromise the privacy of the IoT devices. Attacks against authentication impersonate authorized nodes by forging identities of IoT devices or fog, edge or cloud nodes. This attack may take the form of replay attack or masquerade attack. Attack against confidentiality eavesdrop IoT network traffic between IoT devices and access point at the physical or sensor layer so as to misuse the IoT devices to fulfil the adversary intention. Such attack may be in the form of known key and password attack, brute force attack and tracing attack. Attack against availability tends to create Denial of Service (DoS) or Distributed Danial of Service (DDoS) in order to make services unavailable for IoT based farming. This may happen when an attacker floods the servers with huge amount of unwanted data and false data injection. Attack against integrity tends to modify private agriculture data such as pH settings through unauthorized access. Attacker can do this through biometric template attack, man-in-the-middle (MITM), forgery attack and trojan horse attack.

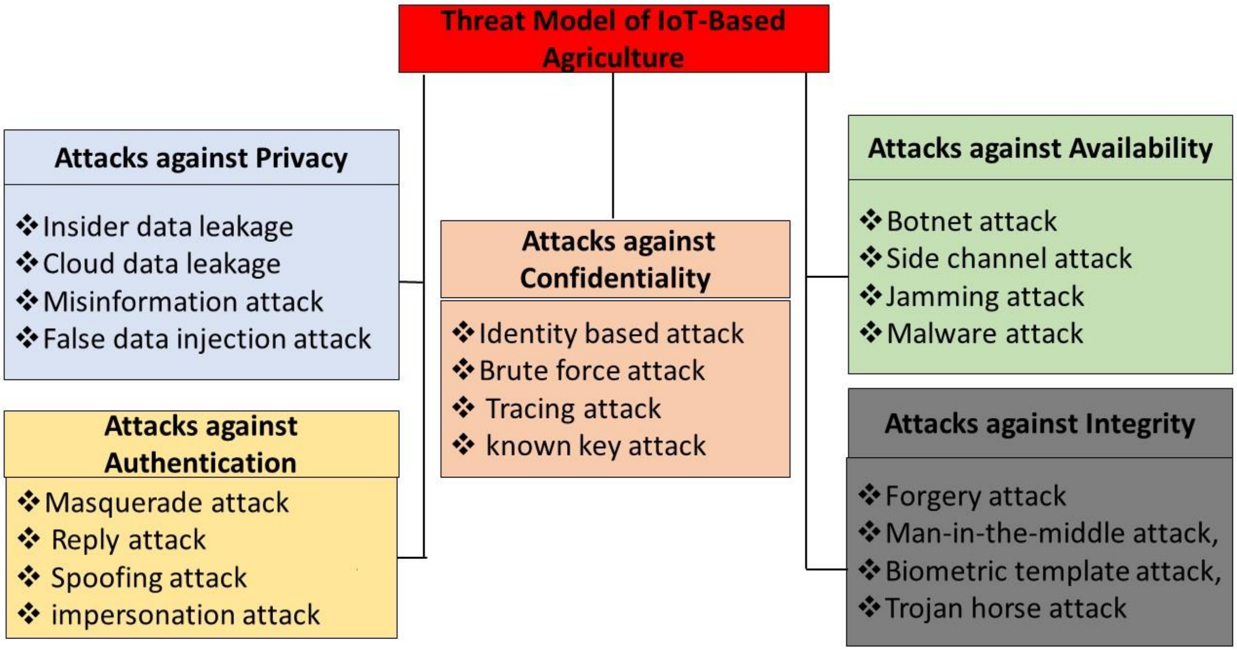

Figure 4.0 IoT-Based Agriculture Architectural Layers

A. Classes of Attacks on IoT-Based Agriculture

Considering different literatures, this research classifies attacks on IoT-based agriculture into five (5) different classes namely privacy, authentication, confidentiality, availability and integrity attack.

1). Attacks Against Privacy

These attacks occurred when an attacker capitalized on the location and identity of smart devices at the agriculture sensor layer to gain an unauthorized access to data and compromise device privacy. Accessing farm data such as crop growth, soil nutrients, humidity, rainfall, soil type and pH settings that are collected at the IoT sensory layer may expose farmer's daily activities and give a competitor undue advantage. Farm data need to be preserved from any form of unauthorized access as it may lead to different form of attack like agricultural espionage. Farm privacy is based on the principle of secrecy, anonymity and autonomy [39, 40].

2). Attacks Against Authentication

This attack attempt to gain authorized access to devices and nodes through identity forgery. The attacker impersonates a legitimate device user and gain access to agriculture devices either at the sensor, network, fog or cloud layer. This identity-based attack may come in the form of masquerade, reply, Spoofing, and impersonation attack [42].

In masquerade attack, fake nodes are presented as legitimate nodes in order to log into server at agriculture sensor or edge layer.

In replay attack, the privacy of agriculture devices and data are exploited by an attacker through interception of agriculture data packets between IoT devices with an access point at the sensor layer and relaying them without modification to their destinations.

The major target in spoofing are agriculture sensory and other farm RFID system. The attacker gains unauthorized access to farm IoT devices and network by capturing information from farm network after injecting fake information on nodes and RFID system.

3). Attacks Against Confidentiality

In attack against confidentiality, the attacker eavesdrop IoT based agriculture device and network with access point at the sensor layer in order to misdirect and compromise smart agriculture devices into making wrong discussions and performing wrong activities category of attacks attempts to adversarial eavesdrop. This attack may take the form of identity based, brute force, tracing and known key attack.

In Identity-based attack, an adversary steal device identity by applying three attack techniques. First, the attacker collects farm device data using eavesdropping Secondly, the attacker tracks and trace farm device to using identification information gathered through eavesdropping. Thirdly, he duplicates password to gain to compromise farm device and data confidentiality [43].

In brute force attack, the attacker systematically tries all possible passwords of agriculture device and node, passphrases them until an accurate password is gotten. This attack is used to obtain private IoT and user data such as username, password and personal identification number. The targeted devices are mostly those at the sensor layer [44].

In tracing attack, the attacker finds the real identity of IoT devices at the agriculture sensor layer after gathering privacy information on devices [44].
In known-key attack, the attacker uses the knowledge of previously compromised session key to generate new session keys. This attack may also get access to encrypted keys after series of monitoring and evaluation of encryption time or leaked information on devices processing duration. Device confidentiality is mostly compromised [44].

4). Attacks Against Availability

The goal of this attack is to make the service of agriculture IoT devices unavailable. This form of Denial of Service may occur when the attacker flood server with large amount of unwanted data, update IoT software remotely with false data injection or lunch attack on the accurate localization for UAV with a malicious 5G station. Another example of availability attack is Botnet attack [46].
In botnet attack, attackers may capitalize on the interconnection of devices in IoT agriculture, to control them by a central malicious system. An army of infested farm IoT devices called zombies are used to infect other farm network through different means [47].

5). Attacks Against Integrity

This attack may take the form of misinformation attack, trojan horse attack and biometric attack. The goal of the attacker is to gain unauthorized access to IoT devices and modify device settings and data. This may lead to malfunctioning and inaccurate data generation. Misinformation attack endanger farm data integrity through the release of false information about crops and IoT devices. The attacker present fake data report that mimic the form of original farm data report claiming the outbreak of crop diseases or device malfunctioning. At the end, it will consume time and farm resources to analyze data and prove initial result wrong. Other forms of attacks against integrity are forgery attack, trojan horse attack, man-in-the-middle attack, biometric template attack [49].

B. Countermeasures to Attack on IoT-Based Agriculture

In order to secure IoT device in agriculture environment, they need to a proper implantation of some security measures during IoT device development, deployment and usage. Some of these measures are proposed in different literatures.

1). Solutions to Privacy Attacks

In protecting the privacy of IoT based farming data, [50] proposed an APPA protocol that uses cryptographic based techniques such as signature of knowledge and paillier cryptosystem to achieve anonymity and unforgeability with the aim of protecting IoT devices against false data injection attack and eavesdropping attack.
Considering the security of location privacy of IoT-based agriculture [51], proposed the implementation of location privacy algorithm which can resist attacks such as inference and colluding attack.
In order to protect farmer's privacy when data are collected and combined from sensor layer, [52] suggested that the dynamic privacy protection model should be implemented. The model which is also referred to as DPP model, uses three basic security phase which include; security classification in terms of privacy weight definition, data pair identification (content-oriented) and input data table (for evaluation performance).
To ensure trust relationship between IoT devices in an agriculture environment [53] proposed the adoption of homomorphic encryption which consist of two schemes trust evaluation techniques for agriculture IoT devices. The first scheme suggests that authorized proxy is fully trusted and collusion is completely eliminated between evaluation party and authorized proxy. The second scheme suggests that no collusion between evaluation party and authorized proxy and authorized proxy may not be fully trusted. These schemes are implemented whenever a node decrypts data, with trust evaluation done using the trust evaluation algorithm.

2). Solutions to Authentication Attacks

Information in electronic tags are automatically identified and captured by Radio Frequency Identification (RFID) technology. This technology allows easy control and monitoring of farm crops and animals. An attack on the RFID tags will compromise automated processes in farm. To secure this technology, a lightweight authentication solution for IoT application was proposed by [54] This mechanism is based on entities such as an authenticated cloud and backend database servers, reader and RFID-tag based on some cryptographic principles such as unconnected pseudo-identity, hash function and emergency key. This security techniques proves to secure IoT application against attacks such as location tracking, forgery, cloning and DoS [55].
A delegated authentication mechanism for securing IoT data collection as it is being transported over insecure channels was suggested by [56]. This mechanism is called SOPP (Semi-Outsourcing Privacy Preserving Scheme), it applied cryptographic algorithm (called elliptic curve) as a non-interactive (one way) authentication between the cloud layer and physical device layer. Delegating authentication process to the cloud layer, blocks unnecessary access. Data integrity is achieved through data decryption at the data centre.
One of the existing security flaws in present RFID technology is that Authentication process in existing RFID protocol is done without encryption. In order to overcome this flaw, [57] proposed a light weight cryptographic technique by which authentication is done based on encrypted password.
A code structure authentication technique for IoT devices that overcome the resource constrained in existing certificate-based signatures authentication in IoT environment was created by [58]. The technique seems efficient as management of confirmation code in IoT environment seems to be very easy. This technique can be applied in IoT based agriculture.

IoT terminal node and platform asymmetric mutual authentication scheme that combines SHA1 and feature extraction was proposed for IoT security by [59]. The proposed scheme is highly efficient in terms of throughput with reduced computation and communication cost. This mechanism can be applied in IoT base agriculture environment.

3). Solutions to Data Confidentiality Attacks

Confidentiality in IoT based agriculture can be achieved based on cryptographic mechanism such as cipher-text based access-based mechanism. [60] used an elliptic curve integrated encryption scheme (ECDH) to provide data confidentiality and integrity through the generation of massage authentication key and encryption key in lightweight attribute-based encryption scheme. This scheme proves robust than other cryptographic mechanism that use decisional bilinear Die-Hellman exponent. This scheme is highly secure against attribute set attack and plaintext attack.

A cipher-text attribute-based encryption technique for fog enabled IoT in order to achieve data confidentiality and with variability in a case of access request from an identified IoT device was proposed by [61].

4). Solutions to Availability Attacks

Denial-of-Service (DoS) and botnet attack mainly target the availability of IoT network services. Implementation of firewall for intrusion detection and prevention system on IoT-Based farm network will keep the farm inform about any unnecessary traffic inflow. Installation of anti-DoS attack mechanism and implementation of physical security and light weight encryption algorithms in IoT nodes vicinity and light weight encryption algorithms will enable IoT devices in farm to provide undisrupted service [46] [47].

5). Solutions to Data Integrity Attack

In [49], a lightweight integrity verification security architecture (LIVE) that can be implemented for IoT based agriculture was proposed. The scheme provides content verification for named data networking. The security levels included in this architecture are non-cacheable, 1-cacheable and all cacheable. Cryptographic technique (Merkle Hash Tree algorithm) is used to produce token for signature generation.

A secure Threshold Cryptography based Group Authentication (TCGA) scheme which is capable of verifying all nodes in IoT network was proposed in [61]. This scheme proved secure and tend to reduce overhead handshake and power consumption. This security mechanism can be implemented in IoT based agriculture to protect data integrity.

A security technique based on Digital certificate with datagram transport security was proposed in [62]. In this technique, pre-shared key mechanism is replaced with digital certificate for IoT Authentication in secure communication. The authentication procedures involve; (i) client's request is sent to server (ii) Client receives server's certificate (iii) client decrypts certificate using server's public key as a means of verification (iv) sever uses same mechanism for verification and both can start communicating. Application of this communication mechanism will solve integrity problem in IoT based agriculture.

Considering data integrity protection and authentication, [63] suggested a privacy preserving protocol based on Message Authentication Code (MAC). where original IoT data carries MAC solution that can be verified by sender during communication whether data has been altered by attacker. Implementing this can protect agriculture IoT data

C. Countermeasures to Attacks Based on Architectural Layers

1). Solutions to Attacks on Physical/Sensor Layer

According to [64] applying hybrid linear combination encryption and Hash function between IoT devices communications can secure the agriculture sensor layer against impersonation and DoS attack.

According to [60] data confidentiality and integrity can be achieved against chosen plaintext and attribute set attack through the implementation of encryption mechanism using secure symmetric cryptographic system based on Lagrange secret sharing for massage exchange between IoT devices in sensor layer. Encryption keys are generated using elliptic curve cryptosystem.

A homomorphic encryption-based trust management system consisting of three entities such as node, evaluation party and authorized proxy which is used to protect IoT devices against conflict behaviour and On-off attack was discussed in [65]. This can be applied between IoT devices and an access point at agriculture sensor layer.

Applying blockchain technology in private information retrieval at sensor layer can protect IoT privacy [42].

The physical layer nodes should be protected against any form of physical and natural disaster such as fire, thunder storm, and human activities. Nodes should be equipped and protected with tamper-resistant hardware, any attempt on the node should wipe out the memory so that data will note be leaked to attacker especially secret key. Good password should be used for the bootstrap loader of IoT nodes and JTAG interface should be disabled. Sensor nodes should be routinely checked using special devices such as magnifiers and not with the human eyes alone and also be protected against attack through camouflaging.

2). Solutions to Attacks on Fog Layer

The work of [63] proposed the use of chaos-based cryptography and massage authentication code to mitigate eavesdropping attacking at the fog layer. In this technique, access point and fog node add a message authentication code to the original data to verify the integrity of the transmitted data among IoT devices.

According to [66], false data injection, Denial of Service and differential attack can be mitigated by implementing Chinese remainder theorem, homomorphic paillier encryption and one-way hash chain in the fog computing layer to filter injected false data

3). Solutions to Attacks on Network Layer

The work of [60] suggested that the network layer can be protected against chosen-plaintext attack by adapting a searchable encryption scheme based on setup, KeyGen, store, trapdoor and search.
In-depth protection against other attacks can be achieved by segmenting and segregating farm networks and functions. Limiting unnecessary lateral communication within farm network and hardening of network and network infrastructures through the installation antivirus, firewalls, intrusion prevention and detection systems can keep the network layer protected against known and unknown attack. Regular backup, implementation of adequate password policies, validation of software integrity and performing out-of-bound network management are good measures against network layer attacks.

4). Solutions to Attacks on Cloud Layer

According to [67] collision attack at the cloud layer can be overcome through proxy sever deployment and one-way anonymous key agreement protocol. Cryptographic measures such as data encryption and two step verification implemented between device and cloud interaction can provide secure device to cloud interaction. If the cloud is a hybrid cloud connected at the network layer, Virtual Private Network (VPN) implementation can encrypt traffic between agriculture device and cloud, if connected at application layer, SSL/TLS implementation can encrypt traffic between agriculture device and cloud

IV. CONCLUSION

Wide adoption of Internet of Things in agricultural have raised security and privacy issues in cyber domain. In research, application of IoT devices in agriculture is being discussed extensively with in-depth reviews of existing security and privacy solutions for IoT-based agriculture. The research also proposed a five-tire (tier) threat model for IoT-based agriculture with implementable countermeasures. This research will be beneficial to researchers (and agriculturist) intending to develop and deploy IoT devices for agriculture purposes. Future research will focus on security issues in deployment of 5G communication technologies in IoT-based farming.

V. FUNDING STATEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] O. Elijah, I. Orikumhi, T. A. Rahman, S. A. Babale, S. I. Orakwue. *Enabling smart agriculture in Nigeria: Application of IoT and data analytics*. IEEE, 2017, pp. 762–766, DOI: 10.1109/NIGERCON.2017.8281944

[2] N. Ahmed, D. De, I. Hussain, *Internet of Things (IoT) for smart precision agriculture and farming in rural areas*. IEEE Internet Things J, 2018, Vol. 5, No. 6, pp. 4890-4899

[3] G. Villarrubia, J. F. De Paz, D. H. De, La Iglesia and J. Bajo, *Combining multi-agent systems and wireless sensor networks for monitoring crop irrigation*. Sensors. 2017, Vol. 17, No. 8, pp. 1775.

[4] J. M. Talavera, L. E. Tobón, J. A. Gómez, M. A. Culman, J. M. Aranda, D. T. Parra, L. A. Quiroz, A. Hoyos and L. E. Garreta, *Review of IoT applications in agro-industrial and environmental fields*. Comput. Electron. Agriculture, 2017, No. 142, pp. 283-297.

[5] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, *IoT in agriculture: Designing a Europe-wide large-scale pilot*. IEEE Communication. Magazine, 2017, Vol. 55, No. 9, pp. 26-33.

[6] L. Li, *Application of the Internet of Thing in green agricultural products supply chain management*. In Proc. IEEE Int. Conf. Intell. Comput. Technol. Autom. (ICICTA), Shenzhen, China, 2011, No. 1, pp. 1022–1025.

[7] J. V., Stafford, *Precision Agriculture. Wageningen*. The Netherlands: Academic, 2019.

[8] Iot in Agriculture: 5 Technology use cases for smart farming (and 4 challenges to consider). Accessed: Jul. 2, 2020. [Online]. Available: https://easternpeak.com/blog/iot-in-agriculture-5-technologyuse-cases-for-smart-farming-and-4-challenges-to-consider/

[9] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, *Internet of Things security: A survey*. Journal of network and computer applications, 2017, Vol. 88:, pp. 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

[10] L. Angelini, E. Mugellini, O. Abou Khaled and N. Couture, *Internet of tangible Things (IoTT): Challenges and opportunities for tangible interaction with IoT*. Informatics, 2018, Vol. 5, No.1, pp. 7. https://doi.org/10.3390/informatics5010007

[11] Olakunle Elijah, Tharek Abdul Rahman, Igbafe Orikumhi and Chee Yen Leow. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE internet of things journal, 2018, 5(5): 3758-3773

[12] Xiaojie Shi, Xingshuang An, Qingxue Zhao, Huimin Liu, Lianming Xia, Xia Sun and Yemin, Guo, *State of the Art: Internet of Things in protected agriculture*. Sensors, 2019, Vol. 19, pp. 1833; doi:10.3390/s19081833 www.mdpi.com/journal/sensors

[13] U. Raza, P. Kulkarni and M. Sooriyabandara, *Low power wide area networks: An overview*. IEEE Commun. Surv. Tutor, 2017, No. 19, pp. 855–873.

[14] Y. D. Beyene, *NB-IoT technology overview and experience from cloud-RAN implementation*. IEEE Wireless Communication., 2017, Vol. 24, No. 3, pp. 26–32.

[15] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, *IoT middleware: A survey on issues and enabling technologies*. IEEE Internet Things Journal, 2017, Vol. 4, No. 1, pp. 1–20.

[16] X. Chen, Q. Shi, L. Yang, and J. Xu, *Thrifty Edge: Resource-efficient edge computing for intelligent IoT applications*. IEEE Network, 2018, Vol. 32, No. 1, pp. 61–65.

[17] J. I. Rubala and D. Anitha, Agriculture field monitoring using wireless sensor networks to improving crop production. International Journal of Engineering and Science, 2017, Vol. 52, No. 16, pp. 5216–5221.

[18] M. Odema, I. Adly, A.Wahba, and H. Ragai, *Smart aquaponics system for industrial Internet of Things (IIoT)*. in International Conference on Advanced Intelligent Systems and Informatics. Cairo, Egypt: Springer, 2017, 844–854.

[19] T. A. Shinde and J. R. Prasad, *IoT based animal health monitoring with naive Bayes classification. International* Journal Emerging Trends in Technology, 2017, Vol. 1, No. 2, pp. 252–257.

[20] Olakunle Elijah, Tharek Abdul Rahman, G. Orikumhi, and Suleiman Aliyu Babale, *Enabling smart agriculture in Nigeria: Application of IoT and data analytics*. 2017, DOI: 10.1109/NIGERCON.2017.8281944 https://www.researchgate.net/publication/323067309

[21] S. Li, M. Li, H. Xu, and X. Zhou, Searchable encryption scheme for personalized privacy in IoT-based big data. Sensors, 2019, 19(5): 1059.

[22] Z. Wang, K. B. Walsh, and B. Verma. On-tree mango fruit size estimation using RGB-D images, Sensors, 2017, 17(12): 27-38.

[23] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, *Design of secure user authenticated key management protocol for generic IoT networks*. IEEE Internet Things Journal, 2018, Vol. 5, No. 1, pp. 269-282.

[24] Mohamed Amine Ferrag, Lei Shu, Xing Yang, Abdelouahid Derhab, *Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges*. IEEE Access, 2020, DOI: 10.1109/ACCESS.2020.2973178

[25] R. R. Shamshiri, F. Kalantari, K. C. Ting, K. R. Thorp, I. A. Hameed, C. Weltzien, D. Ahmad, and Z. M. Shad, *Advances in greenhouse automation and controlled environment agriculture: A transition to plant factories and urban agriculture*. Int. J. Agricult. Biol. Eng, 2018, Vol. 11, No. 1, pp. 122.

[26] K. Benke and B. Tomkins, *Future food-production systems: Vertical farming and controlled-environment agriculture. Sustainability*. Sci., Pract. Policy, 2017, Vol. 13, No. 1, pp. 1326.

[27] M. Mukherjee, R. Matam, L. Shu, L. Maglaras and M. A. Ferrag, N. Choudhury, and V. Kumar, *Security and privacy in fog computing: Challenges*. IEEE Access, 2017, No. 5, pp. 19293-19304.

[28] M. Mukherjee, L. Shu, and D. Wang. *Survey of fog computing: Fundamental, network applications, and research challenges*. IEEE Commun. Surveys Tuts., 2018. Vol. 20, No. 3, pp. 1826-1857.

[29] K.P. Ferentinos, N. Katsoulas, A. Tzounis, T. Bartzanas and C. Kittas, *Wireless sensor networks for greenhouse climate and plant condition assessment*. Biosyst. Eng. 2017, No. 153, pp. 70–81.

[30] J. I. Rubala and D. Anitha, *Agriculture field monitoring using wireless sensor networks to improving crop production*. International Journal of Engineering and. Science, 2017, Vol. 52, No. 16: pp. 5216–5221.

[31] D. García-Lesta, D. Cabello, E. Ferro, P. López, and V. M. Brea. *Wireless sensor network with perpetual motes for terrestrial snail activity monitoring*. IEEE Sensors Journal, 2017, Vol. 17, No. 15, pp. 508–5015.

[32] M. Roopaei, P. Rad, and K. K. R. Choo, *Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging*. IEEE Cloud Computing, 2017, Vol. 4, No. 1, pp. 10–15.

[33] S. Sharma, K. Chen, and A. Sheth, *Toward practical privacy preserving analytics for IoT and cloud-based healthcare systems*. IEEE Internet Comput., 2018, Vol. 22, No. 2, pp. 42–51.

[34] L. Chen, *Robustness, security and privacy in location-based services for future IoT A survey*. IEEE Access, 2017, Vol. 5, pp. 8956–8977.

[35] P. Varga, S. Plosz, G. Soos, and C. Hegedus, *Security threats and issues in automation IoT*. In Proc. IEEE 13th Int. Workshop Factory Commun. Syst. (WFCS), 2017, pp. 1–6.

[36] A. Bothe, J. Bauer, and N. Aschenbruck, *RFID-assisted continuous user authentication for IoT-based smart farming*.. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA), 2019, pp. 505-510.

[37] M. Abdelsalam, R. Krishnan, Y. Huang, and R. Sandhu. *Malware detection in cloud infrastructures using convolutional neural networks*. In Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), 2018, pp. 162-169.

[38] B. Ali and A.I. Awad, *Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors*, 2018, Vol. 18, No. 3, pp. 1–17.

[39] S. C. Cha, T. Y. Hsu, Y. Xiang, and K. H. Yeh, *Privacy enhancing technologies in the Internet of Things: Perspectives and challenges*. IEEE Internet Things Journal, 2019, Vol. 6, No. 2, pp. 2159-2187.

[40] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. *A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications*. IEEE Internet Things Journal, 2017, Vol. 4, No. 5, pp. 1125-1142.

[41] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. A survey on security and privacy issues in Internet of Things. IEEE Internet Things Journal, 2017, 4(5): 1250-1258.

[42] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, *PTAS: Privacy preserving thin-client authentication scheme in blockchain-based PKI*. Future Gener. Comput. Syst., 2019, Vol. 96, pp. 185-195.

[43] S. Li, M. Li, H. Xu, and X. Zhou. *Searchable encryption scheme for personalized privacy in IoT-based big data*. Sensors, 2019, Vol. 19, No. 5, pp. 1059.

[44] U. E. Chinanu, O. E. Oche and J. O. Okah-Edemoh, *Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures.* Academic Research Publishing Group Scientific Review, 2018, Vol. 4, No. 10, pp. 80-89, 2018 URL: https://arpgweb.com/journal/journal/10 DOI: https://doi.org/10.32861/sr.410.80.89

[45] O. Novo. *Blockchain meets IoT: An architecture for scalable access management in IoT*. IEEE Internet Things Journal, 2018, Vol. 5, No. 2, pp. 1184-1195.

[46] T. Tyagi. Botnet of things: *Menace to Internet of Things.* In Proc. 3rd Int. Conf. Computer., Communication and Network Security, 2018, pp. 1-5.

[47] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu. *LIVE: Lightweight integrity verification and content access control for named data networking.* IEEE Trans. Inf. Forensics Security, 2015, Vol. 10, No. 2, pp. 308-320.

[48] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu. APPA: An anonymous and privacy preserving data aggregation scheme for fog enhanced IoT. J. Netw. Comput. Appl., 2019, No. 125, pp. 82-92.

[49] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, *Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment*. IEEE Internet Things Journal, 2019, Vol. 6, No. 3, pp. 5791-5802.

[50] K. Gai, K.-K.-R. Choo, M. Qiu, and L. Zhu, Privacy-preserving content oriented wireless communication in Internet-of-Things, IEEE Internet Things J., 2018, vol. 5, no. 4, pp. 30593067.

[51] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos. Two schemes of privacy preserving trust evaluation, Future Gener. Comput. Syst., 2016, 62: 175-189.

[52] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, LIVE: Lightweight integrity verification and content access control for named data networking, IEEE Trans. Inf. Forensics Security, 2015, Vol. 10, No. 2, pp. 308-320.

[53] P. Gope, R. Amin, S. K. Hafizul Islam, N. Kumar, and V. K. Bhalla, *Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment*, Future Gener. Comput. Syst., 2018, Vol. 83, pp. 629-637.

[54] X. Zhang, C. Liu, S. Poslad, and K. K. Chai, *A provable semi outsourcing privacy preserving scheme for data transmission from IoT devices*. IEEE Access, 2019, Vol. 7, pp. 87169-87177.

[55] J.Y. Lin and W.C. Huang, *A lightweight authentication protocol for internet of things*. In Proceedings IEEE International Symposium on Next-Generation Electronics, Kwei-Shan, Taiwan, 2014, pp.1–2.

[56] P. K. Sharma, S. Singh, Y.S. Jeong, and J. H. Park, *DistBlockNet:A distributed blockchains-based secure SDN architecture for IoT networks*. IEEE Communication Magazine, 2017, Vol. 55, No. 9, pp. 7885.

[57] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, *A survey on security and privacy issues in Internet of Things*. IEEE Internet Things Journal, 2017, Vol. 4, No. 5, pp. 1250-1258.

[58] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang. *A practical and compatible cryptographic solution to ADS-B security*. IEEE Internet Things Journal, 2019, Vol. 6, No. 2, pp. 3322-3334.

[59] Inayat Ali, Sonia Sabir and Zahid Ullah, *Internet of Things Security, Device Authentication and Access Control: A Review*, International Journal of Computer Science and Information Security (IJCSIS), 2016, Vol. 14, No. 8, pp. 56-60.

[60] M. Panwar, and A. Kumar, *Security for IoT an effective DTLS with public certificates. International conference on advances in Computer Engineering and application (ICACEA)*, 2015.

[61] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng. *A privacy preserving communication protocol for IoT applications in smart homes*. IEEE Internet Things Journal, 2017, Vol. 4, No. 6, pp. 1844-1852.

[62] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen.,*CPAL: A conditional privacy-preserving authentication with access link ability for roaming service.* IEEE Internet Things Journal, 2014, Vol. 1, No. 1, pp. 46-57.

[63] W. L. Chen, Y. B. Lin, Y. W. Lin, R. Chen, J. K. Liao, F. L. Ng, Y. Y. Chan, Y.-C. Liu, C. C. Wang, C.-H. Chiu, and T. H. Yen, *AgriTalk: IoT for precision soil farming of turmeric cultivation*. IEEE Internet Things Journal, 2019, Vo. 6, No. 3, pp. 5209-5223.

[64] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, *A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT*. IEEE Access, 2017, No. 5, pp. 3302-3312.

[65] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, *Efficient and privacy preserving access control scheme for fog-enabled IoT*. Future Generation Computing System, 2019, No. 99, pp. 134142.

AUTHORS

First Author – ONOJA, Emmanuel Oche. MTech. Department of Cyber Security Federal University of Technology Minna, Nigeria. onoskiss@gmail.com
Second Author – SULEIMAN, Muhammad Nasir. MTech. Computer Science Department, Federal Polytechnic Nasarawa Nigeria. suleimanmohdnasir@fedpolynas.edu.ng.
Third Author – ALHASSAN Hauwa Muhammed. Computer Science Department, Federal Polytechnic Nasarawa Nigeria. hauwama@yahoo.com

Correspondence Author – ONOJA, Emmanuel Oche. onoskiss@gmail.com, eonoja1@yahoo.com. +2348064474211

http://dx.doi.org/10.29322/IJSRP.10.08.2020.p10494