Securing Agri-IoT: Threat Model, Vulnerabilities and Encryption Challenges*

[1]Joshua Kweku Aidoo, [1]Solomon Nunoo, [1]Emmanuel Effah and [2]William Akotam Agangiba
[1]University of Mines and Technology (UMaT), Tarkwa, Ghana
[2]University of Cincinnati, USA

Aidoo, J. K., Nunoo, S., Effah, E. and Agangiba W. A. (2025), "Survey: Fundamentals of Agri-IoT, Security Challenges and Proposed Remedies", *Ghana Journal of Technology*, Vol. 9, No. 1, 2025, pp. 56-61.

Abstract
In the era of pervasive digital communication where many devices relate to one another, the Internet of Things (IoT) has become predominantly employed in many domains to ensure efficiency, effectiveness and automation of activities. Due to the heterogeneous nature of devices and networks in the IoT, securing devices and data has become of utmost importance. Many research works propose security services and mechanisms to counter attacks in the IoT application domains such as smart cities, smart industries, and smart healthcare. This paper seeks to highlight the security gap with respect to encryption in the application of IoT in agriculture (Agri-IoT) with some proposed future scope.

Keywords: Internet of Things (IoT), Agri-IoT, Security, Encryption, Decryption, CIA, OSI Security Architecture, Attack

1 Introduction

Internet of Things (IoT) refers to the interconnection of low-powered, low-processing devices ("things") over a network for the purpose of sensing and performing actions automatically based on sensed parameters without any human intervention (Chen *et al.*, 2017; Ferrag *et al.*, 2020; Hassija *et al.*, 2019; Islam *et al.*, 2015).

The IoT is heterogeneous in nature, that is, it is made up of several devices made by different vendors, and also, involves connection over different network architectures. The devices in IoT employ machine-to-machine (M2M) communication protocols to avoid the need for human intervention in activities. Due to the pervasive nature of IoT, it is expected that M2M connections will reach 29 billion by 2030 and a $4 trillion revenue be obtained through the use of IoT by the end of 2025 (Hassija *et al.*, 2019; Kassim, 2022).

Since its inception, many research has been done to find its possible application in a plethora of domains. These domains include smart industry, Smart Healthcare, Smart Traffic, Smart Homes, Smart Cities, Smart Grids, Smart Agriculture, among others as can be seen in Fig. 1 (Akhtar *et al.*, 2020; Orpa *et al.*, 2022; Usha *et al.*, 2020; Yue, 2021). The widespread application of IoT is owed to its ability to be contextualized to a particular domain for the purpose of ensuring efficiency, effectiveness and automation to gain profit with little to no human intervention. In the agricultural domain, where farmers performed a lot of manual work to ensure the best quality of farm produce, IoT is being employed to perform the painstaking farm activities which include irrigation, application of fertilizer, testing of soil PH, and pest control as illustrated in Fig. 2 (Kassim, 2020). This has led to the production of farm produce of the highest quality with little wastage of resources and energy, as well as saving costs (Xu *et al.*, 2022). Through IoT, farmers can remotely monitor and initiate actions on farmlands. In addition, data can be collected for data analysis and optimisation of farm activities to improve yield and productivity.

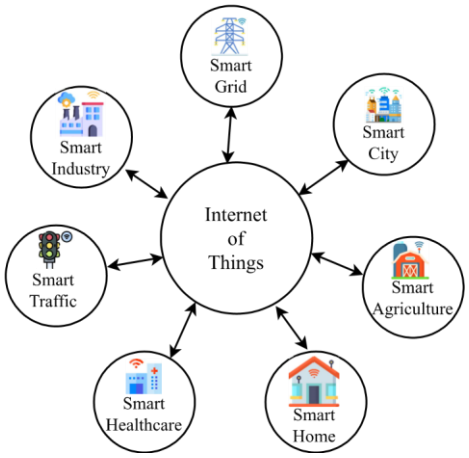

Fig. 1 IoT Domains

Urbanization of rural areas is accelerating, contributing significantly to food insecurity due to the resulting food production gap. As a result, it is projected that by 2050 (Usha *et al.*, 2020), 70% of the global population will reside in urban areas, leading to an increase in overall food consumption worldwide. Moreover, the world population is expected to reach 9 billion by 2050, hence the total amount of food production is expected to double by

*Manuscript received July 8, 2024
Revised version accepted March 20, 2025

2050 in order to meet the demand for agricultural produce (Antony *et al.*, 2020). With one-third of world population and over 70% of the African population depending on agriculture for income, it would be expected the amount of food production would be met (Abbasi *et al.*, 2019).

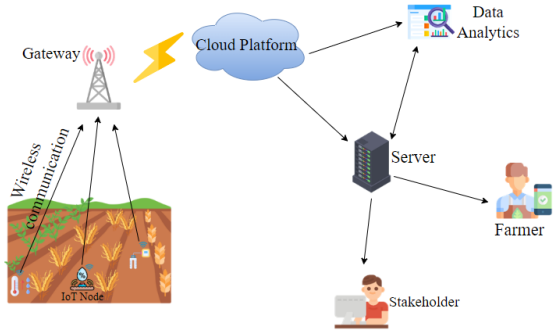

Fig. 2 Conceptual Representation of Agri-IoT

However, it might not be met because current agricultural practices depend on traditional farming methods (Effah *et al.*, 2023). In Africa, the two farming seasons has been reduced to one due to climate change which has led to the production of less farm produce and many leaving the agricultural arena resulting in food insecurity (Kristen *et al.*, 2021). This calls for a paradigm shift in farming practices. The most promising remedy is precision and greenhouse farming whose underlying technology is Agricultural Internet-of-Things Technology (Agri-IoT) (Kristen *et al.*, 2021). Thus, it is of global significance to expand research in this field since it affects a lot of the world population.

Although the adoption and adaption of IoT in agriculture offers advantages of efficiency, effectiveness and comfort of use, there are issues of security and privacy that emerge (Asif *et al.*, 2021; Kassim, 2022; Zrelli *et al.*, 2022).
Before the incorporation of IoT in farm activities, issues of security and privacy was limited to the physical farm environment. However, the incorporation of IoT introduces cyber threat to the pool of challenges regarding security and privacy in agriculture. Moreover, the heterogeneous nature of devices and networks employed provides a large attack vector for compromising security and privacy (Zimmermann *et al.*, 2022).

Therefore, a reference document that evaluates the fundamentals of Agri-IoT, encryption security challenges, and future developments in encryption mechanisms for securing the Agri-IoT environment is needed. This study fills that gap.

1.1 Architecture and Communication

Generically the architecture for the implementation of IoT in agriculture has three main layers, namely; Perception Layer, Network Layer and Application Layer (Duangphasuk *et al.*, 2020; Kaur, 2018; Sethi and Sarangi, 2017). Fig. 3 illustrates the three-layer architecture.

The perception layer is the lowest layer in the architecture, where devices ("things") employed interact directly with the physical environment. For this reason, it is also referred to as the physical layer (Sarath Chandra *et al.*, 2023; Sharma *et al.*, 2016). Devices used in this layer are low powered and have low processing capabilities. Often they rely on batteries for power, while maintaining sleep-wake cycles (Khodayer Al-Dulaimi *et al.*, 2022). The perception layer devices usually deployed on the farmlands include soil moisture sensors, humidity sensors, soil PH sensors, among others.

The network layer is the second layer in the architecture which lies between the perception and application layers. This layer serves as the layer responsible for ensuring communication (Mahajan, 2021). It transfers data from the perception layer to the application layer for processing and analysis. This layer can use diverse communication protocols for communication between the perception layer and itself and for forwarding data to the Application Layer. Protocols for communication between the application layer and the network layer include Zigbee (Pawaskar *et al.*, 2021), LoRa (Zourmand *et al.*, 2019) , Sigfox, Z-wave (Badenhop *et al.*, 2017) among others. Communication between the network layer and the application layer can be achieved through WiFi (Ejaz *et al.*, 2016), LoRa (Effah *et al.*, 2023), and Fibre (Aleksic, 2019), among others.

The application layer is the last layer of the architecture. This is the layer the end users directly interact with. It provides customised services to the end users (Ejaz, 2021). These services are provided to the users remotely, giving them information on data obtained on the farmland, providing them with results obtained after analysis of the data and finally providing an interface through which end users can remotely perform actions on the farmland. Communication within the application is through application layer communication protocols such as Message Queue Telemetry Transport (MQTT) (Alqinsi *et al.*, 2018), Constrained Application Protocol (CoAP) (Brasilino and Swany, 2019), Extensible Messaging and Presence Protocol (XMPP) (Al-Fuqaha *et al.*, 2015), Data Delivery Service (DDS) (Al-Fuqaha *et al.*, 2015), Advanced Message Queuing Protocol (AMQP) (Caiza *et al.*, 2019).

The structure of this paper is as follows. Section 2 outlines the threat model for Agri-IoT, identifying key assets and vulnerabilities. Section 3 discusses security measures and best practices. Section 4 focuses on encryption as a security remedy,

comparing conventional and IoT-based methods. Section 5 addresses ongoing challenges related to encryption and suggests areas for future research. Finally, Section 6 provides the conclusion of the study.

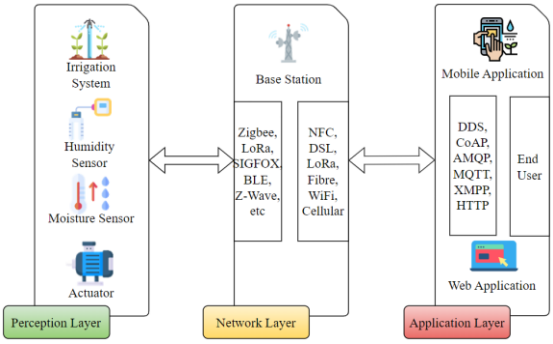

Fig. 3 Agri-IoT Architecture

2 Threat Model

Threat modeling is done to identify the assets in the system, the potential threats that the system faces and their associated risks using abstraction (Sunhare *et al.*, 2020). Through threat modeling the vulnerabilities within the Agri-IoT system is identified and the impact on the system if these vulnerabilities are exploited by malicious users of technology. Threat modeling include; identification of assets (Kristen *et al.*, 2021), identification of threat actors, threat enumeration, assessment of vulnerabilities, analysis of impact, risk prioritisation, mitigation strategies and finally, review and update as illustrated in Fig. 4.

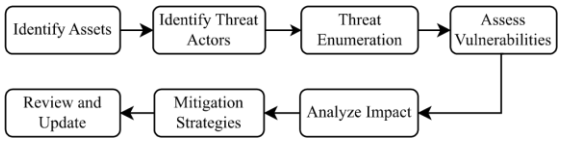

Fig. 4 Threat Model

2.1 Identification of Assets in Agri-IoT

At this stage assets in the Agri-IoT system are identified. These assets include critical components of the IoT environment which need to be available at all times with confidentiality and integrity maintained (Kristen *et al.*, 2021). These assets are the target of an attacker. Should an attacker have access to or manage to get these assets offline, the Agri-IoT system will be greatly affected.

Assets within the Agri-IoT system are distributed throughout all layers of its architecture. These assets encompass a variety of components, such as sensor devices that collect data, actuators that perform actions based on that data, network devices like routers that facilitate communication, and application services in the application layer that process and analyse the information to support decision-making. User data also forms part of the assets in the Agri-IoT system.

User data include the physical parameters collected from the farm environment (Akhter and Sofi, 2022) such as soil moisture and soil temperature. Data on user operations such as the amount of fertilizer applied by users through the IoT system, the time intervals for application, and personal information about the farmers. Hence this data can be both personal and sensitive data that keeps farmers ahead of competition. Agri-IoT infrastructure also forms part of the assets in the Agri-IoT environment. The IoT network infrastructure includes communication protocols and gateways (Chakravarthy *et al.*, 2022). Finally, there are supporting systems such as management software for the farm and services such as cloud services.

2.2 Threat Actors in Agri-IoT

Threat actors are individuals or groups who are involved in the actions performed to compromise the security of the Agri-IoT system for ideological, personal or political reasons. Threat actors identified in Agri-IoT system include cybercriminals, insider threats, cyber terrorists, thrill seekers and competitors.

Cybercriminals are individuals or groups who focus on compromising the Agri-IoT system for the purpose of obtaining money (Richet, 2022). Cybercriminals target assets such as the perception layer devices, network infrastructure and or supporting systems. Commonly, they deny the availability of devices, services or data (Aminu Ghali *et al.*, 2020) and demand ransom be paid for the release of the assets.

Insider threats refer to workers on the farm who may have limited access to the Agri-IoT system. These workers may attempt to obtain confidential data through social manipulation or tampering of IoT devices. In many instances, insider threats arise not from malicious intent but from human errors, like inadvertently installing harmful software on the system, which can lead to significant damage (Wei *et al.*, 2021).

Cyberterrorists are groups or individuals who perform cyberterrorism based on political or ideological standpoints. These terrorists aim at causing malfunction of devices or falsification of data which would lead to complete destruction of farm crops (Plotnek and Slay, 2021). In some cases, these cyberterrorists are state sponsored so they have

state of the art technology at their disposal (Durojaye and Raji, 2022).

Thrill seekers are computer users who would want to compromise the Agri-IoT environment for the fun of it (Sailio *et al.*, 2020). Often, they are computer users who are new to hacking and would want to test their skills on live technology on the internet. These users try to elevate their privileges on the system to the highest privileges and also try to obtain the most amount of data they possibly can. They attempt this using available scripts and tools on the internet designed for assessing and exploiting specific vulnerabilities in systems.

Competitors are farmers who would want to have access to farming procedures and practices performed by farmers in order to be able to dominate the market (Sachitra and Chong, 2016). Sometimes, they would want to attack the Agri-IoT system used to cause total system failure, which in turn would cause total destruction of farm produce, eliminating farmers from markets.

2.3 Threat Enumeration

In threat enumeration, the possible threats that can compromise Confidentiality, Integrity, and Availability (CIA) in the assets already identified are looked at. These threats vary in severity of damages that can be achieved. Threats can be either passive or active in its operation.

Passive attacks are attacks aimed at collecting data on a system without affecting the functioning of the system or altering anything about the system (Keerthika and Shanmugapriya, 2021). These targeted data include data on applications being used, their versions, users on the system and data on individual users such as user privileges. Passive attacks on Agri-IoT can lead to malicious users obtaining personal information about farmers, quantity and type of fertilizers used, quantity of water administered per crop daily, among others. These data may be what gives farmers the competitive advantage. Therefore, the disclosure of such data can cause farmers' sales to plummet.

Active attack on the other hand interacts directly with system component for the purpose of altering the normal functioning of the devices as well as the data provided by the device (Keerthika and Shanmugapriya, 2021). Active attacks on Agri-IoT can cause subsystems such as motors and sprinklers to malfunction. Also altering of data to be sent to the cloud can lead to false predictions and incorrect recommendations which can result in a failed farming season.

In Agri-IoT, threats can target devices at the physical layer through node tampering and physical damage, devices at the network layer through attacks such as sinkhole attacks and routing attacks and finally, the application layer through virtualization attacks, among others. Section 2.3.1 to 2.3.19 elaborates on the threats in Agri-IoT.

2.3.1 Node Tampering Threat

Node tampering is a threat to sensors and actuators of the perception layer. Attackers of the Agri-IoT environment in this case physically access the nodes (sensors, actuators) and try to alter their functioning to cause it to behave as they want it to (Butun *et al.*, 2020; Keerthika and Shanmugapriya, 2021). In some cases, attackers go as far as gaining authorization to alter configurations on the sensors and actuators. Others also may replace some components of the devices.

2.3.2 Sleep Deprivation Threat

Agri-IoT nodes are remotely deployed. In this regard they are designed with internal batteries as the power source (low- power devices). These devices are however programmed to sleep at certain time intervals. In the case where the battery of Agri-IoT devices is drained, it leads to the death of node (device). Sleep deprivation attack is aimed at causing the Agri-IoT devices to work at their maximum capacity without rest hence leading to high drainage of battery power and eventually death of node (device) (Bhattasali *et al.*, 2012; Uy and Nam, 2019).

2.3.3 Physical Damage Threat

In Agri-IoT, physical damage pertaining to the perception layer as a threat is an attempt by an attacker to put a device out of perfect working condition. This usually occurs due to lack of physical security measures put in place to prevent an attacker from gaining physical access to the IoT device. The physical damage attack differs from the node attack in the sense that the aim in this case is to impact or take away the availability of the services provided by the node (Abomhara and Køien, 2015).

2.3.4 Malicious Code Injection Threat

Malicious code injection attack is an attack that compromises the normal functioning of a node or device by injecting or introducing foreign (malicious) code into the system of the node (Obaidat *et al.*, 2020). This is usually accomplished by an attacker when they are able to gain physical access to the node. Upon gaining access an attacker introduces this foreign (malicious) code using a

device such as the USB (Dalkilic and Ozcanhan, 2021).

2.3.5 RFID Spoofing Threat

RFID spoofing is tricking an RFID reader to think a false RFID tag is an original one. Here the attacker uses a device to obtain information about an original RFID tag while it is being read by an RFID reader. Afterward, this information is written onto a false tag, enabling the attacker to trick the system using the copy of the identity written onto the false tag (Obaidat *et al.*, 2020).

2.3.6 Man-in-the-Middle Threat

Man in the Middle (MITM) threat provides an attacker the ability to eavesdrop on communication between two valid devices. As the device attempts to communicate the attacker is able to intercept the communication usually by means of special devices and gain unauthorised access to the message being communicated. The attacker may be a passive attacker, that is, the attacker only eavesdrops and gains access to the message being communicated. In some cases however, attackers are able to trick the devices to think they are the sender or the receiver, and in this case they are able to intercept, alter messages before forwarding to the intended receiver (Dalkilic and Ozcanhan, 2021).

2.3.7 Sinkhole Attack Threat

The sinkhole threat is a routing threat where an attacker can compromise a node and advertise itself as the shortest route to the base station (Butun *et al.*, 2020). This directs all traffic of neighbouring nodes to itself. The compromised node may then be used to alter messages before forwarding to the base station or perform selective forwarding of received packets.

2.3.8 Sybil Threat

Taking advantage of a sybil threat an attacker can launch an attack where a node assumes the identity of multiple nodes. The aim of this attack is to be able to obtain a majority of the network connections so as to be able to conduct illegal activities (Obaidat *et al.*, 2020). In the IoT environment for instance, assuming when multiple sensors are triggered an emergency system should implement an emergency protocol, attackers will be able to start the emergency system even though the sensor information being generated is false.

2.3.9 Traffic Analysis Threat

The traffic analysis threat is also a network layer threat. Leveraging on this threat an attacker can perform a passive attack where attackers listen on the IoT network in order to map out the locations of key nodes and in the network and ultimately the location of the base node. During a traffic analysis attack, attackers are able to find the routing table of the network and also identify the routing patterns for applications (Keerthika and Shanmugapriya, 2021). Upon gaining this information, an attacker is better positioned to launch active attacks on the IoT environment.

2.3.10 Flooding Threat

The flooding threat, also known as the denial of service threat, provides an attacker the ability to sends large amounts of traffic (usually HELLO packets) to the IoT network environment to slow down the network or prevent particular nodes or entities from functioning normally as resources will be working at peak capacities in order to handle the large amount of traffic (Aditya Sai Srinivas and Manivannan, 2020).

2.3.11 Routing Threat

This threat is a potential security risk that if exploited by an attacker the attacker can change the routing configuration on the routing table of a router. The changes to the routing configuration are done to introduce loops into the routs, forward false packets, drop packets, among others (Obaidat *et al.*, 2020).

2.3.12 Side-Channel Threat

Side channel threat is a potential risk where an attacker can obtain information or data from parameters (physical) of the working of a system such as the hardware (execution time, electromagnetic leaks, power consumption) rather than the program code. Performing the side-channel attack, attackers are able to calculate cryptographic keys (Obaidat *et al.*, 2020)

2.3.13 Cryptanalysis Threat

In IoT cryptanalysis attack is the analysis of the cryptographic method of the Agri-IoT system to identify a weakness and exploit it. Here the cryptographic algorithm used in performing the cryptography is critically analysed by an attacker with the aim of obtaining the secret key for encryption (Obaidat *et al.*, 2020). If successful, attackers can decrypt cipher text into plain text using the obtained key.

2.3.14 Structured Query Language (SQL) Threats

SQL, a language for the backend, is used for manipulating data stored in databases. An attacker can leverage SQL injection threats in Agri-IoT to

attempt to query the Agri-IoT databases and obtain unauthorised access to data using malicious code. Here, servers are tricked by inserting SQL commands into web forms, page requests, domain names, among other things, to bypass server access controls and gain access to databases (Tang *et al.*, 2020).

2.3.15 Virus

A virus in Agri-IoT is program code written by a malicious user to cause malfunctions in the operation of Agri-IoT devices, networks, or applications. When a virus is executed, it modifies certain target computer programs by inserting its own code. Whenever the genuine program is run, it will execute the virus, causing more harm to the computer. In this case, we say the program executing the virus is a host program.

2.3.16 Denial of Service (DoS) Threat

DoS threats allow an attacker to send large volumes of traffic or send data that would cause the system to malfunction, crash and render the system unable to perform services. In the application layer of the Agri-IoT, DoS attacks cause the applications to crash making them unable to render services (Abomhara and Køien, 2015; Dalkilic and Ozcanhan, 2021)

Table 1 provides a summary of the attacks the Agri-IoT system is vulnerable to.

Table 1 Summary of Attacks Agri-IoT System is Vulnerable to

Threat	Active	Passive	Confidentiality	Integrity	Availability	Perception	Network	Application
Node Tampering (Deogirikar and Vidhate, 2017)	✓		✓	✓	✓	✓		
Sleep Deprivation (Sah *et al.*, 2022)	✓				✓			
Physical Damage (Andrea *et al.*, 2015)	✓				✓			
Malicious Code Injection (Noman and Abu-Sharkh, 2023)	✓		✓	✓	✓	✓		✓
RFID Spoofing (Noman and Abu-Sharkh, 2023)	✓		✓	✓			✓	
Sybil Attack (Feng *et al.*, 2021)	✓			✓	✓		✓	
Traffic Analysis Attack (Hafeez *et al.*, 2019)		✓	✓				✓	
Flooding Attack (Gajbhiye *et al.*, 2020)	✓				✓		✓	
Selective Forwarding (Jiang and Liu, 2022)	✓		✓	✓	✓		✓	
Side-Channel Attack (Prates *et al.*, 2020)		✓	✓			✓		
Cryptanalysis Attack (Muthavhine and Sumbwanyambe, 2022)		✓	✓				✓	
SQL Injection (Kareem *et al.*, 2021)	✓		✓	✓			✓	✓
DOS Attack (Lee *et al.*, 2022)	✓				✓		✓	✓
DDOS Attack (Ibrahim *et al.*, 2022)	✓				✓		✓	✓

2.3.17 Distributed Denial of Service Threat

This threat is similar to that of the Denial of Service (DoS) threat. That is, attackers flood the applications working at the application layer with traffic causing the application to crash and unable to render services. The DDoS attack however achieves its aim by using multiple machines (botnets) to flood the application with large volumes of requests (Aldaej, 2019).

2.3.18 Virtualisation Threats

Virtualization threats in Agri-IoT provide the attack surface for attacks that target applications running in a virtual environment. If the Agri-IoT system has some applications running on virtual machines, they

can be subject to virtualization attacks. Virtualization attacks are conducted by malicious users by compromising the hypervisor (virtual machine monitor (VMM)), the application that enables the host computers to support virtual machines. Upon compromising the hypervisor, the attacker can take control of the virtual machine.

2.3.19 Third Party Relationships Threats

Applications at the application layer may have relationships with other applications outside the Agri-IoT network. These external applications provide services to the Agri-IoT applications or vice versa. Attackers to gain unauthorised access to the Agri-IoT applications may go ahead to compromise the external applications with which the IoT applications have relationship. Through the compromised third-party application, an attacker can gain unauthorised access to the Agri-IoT applications hence compromise them as well.

2.4 Assessing Vulnerabilities

Vulnerability assessment in the Agri-IoT system involves identifying defects and assigning severity levels to the identified issues within the system. This can be done manually or through software and codes that run automated checks on the system with varying degrees of rigor. Vulnerabilities that can be identified in the Agri-IoT system include lack of physical security for devices, insecure software running on Agri-IoT devices, authentication and authorisation vulnerabilities in protocols/APIs, insecure network/no encryption, no monitoring for anomaly detection, untrained staff, no contingency measures.

2.4.1 Physical Device Security

Agri-IoT devices are typically deployed in agricultural fields, utilizing microcontrollers to process data from various sensors, including pH sensors, humidity sensors, and moisture sensors. These devices work together to monitor environmental conditions and optimize farming practices. In some farms hedges or fences are not built around fields to serve as a layer of physical security to protect devices deployed from individuals with intentions of inflicting physical damage, stealing devices or connecting foreign devices to devices deployed on the farm for the purpose of installing dangerous software which can affect IoT system functionality.

2.4.2 Insecure Firmware on Devices

After IoT system has been setup and configured for farms, they start operation. In many cases, after setup and configuration, farmers do no perform regular update and upgrade of firmware on devices. After security issues are found in device firmware, patches are uploaded on company websites. However as long as devices on farms have not been updated and upgraded the vulnerabilities in the firmware will persist.

2.4.3 Authentication and Authorisation

Authentication is used to determine if a user of the Agi-IoT system is who they claim to be. Authentication can be in the form of username and passwords, using smart cards, NFC, RFID cards among others. Authorization is used to determine the level of access and control users have in the system. It ensures users have authority to view and perform actions that are privileged to that particular user and nothing more. Authorisation and authentication are generally used to ensure only the right people can have access to the system, view data and perform actions. In cases where the Agri-IoT systems have no authentication and authorisation mechanisms in place or they are poorly implemented, the system is vulnerable to cyber-attacks.

2.4.4 Vulnerabilities in Protocols

Protocols used to facilitate the transfer of data from M2M and also from one layer to another within the Agri-IoT layered architecture can have some vulnerabilities. Vulnerabilities can be found in certain versions of the protocols used for ensuring communication and data transfer. Attackers and malicious users can take advantage of these vulnerabilities to obtain unauthorised access to devices and data within the Agri-IoT system. Attackers can also leverage APIs to infiltrate the Agri-IoT system to gather data and compromise the integrity of both system and data.

2.4.5 Unencrypted or Weakly Encrypted Data

Data in transit can be collected by malicious users through eavesdropping, among other methods. If the data is encrypted, attackers cannot read it. However, if the data is unencrypted, attackers can view it in plain text. Also, when encryption mechanisms used for encryption are weak, cybercriminals can easily perform reverse engineering to decrypt the data to obtain plain text.

2.4.6 No Monitoring for Anomaly Detection

The establishment of a monitoring subsystem is key in Agri-IoT systems. This subsystem monitors packets shared, sessions established, and communication duration, among other things, to identify anomalies within the system and isolate involved parties. The unavailability of a monitoring

subsystem means an attacker can attempt to compromise security several times without being isolated. Additionally, once cybercriminals gain access to the Agri-IoT environment, they can carry out abnormal activities within the network without being detected or isolated.

2.4.7 Untrained Staff

Untrained staff at the farm who have access to the IoT system on the farm can also be the point of vulnerability through which cybercriminals can gain access to the system. In cases where staff are not trained to use long passwords that include numbers and special characters, and also cases where staff are not trained how insecure it is to write usernames and passwords on sticky notes to be put on their desks. Also, some staff are not aware they are not supposed to send or share usernames and passwords with others. Some system users also aren't aware of how security can be breached by clicking on links sent from unknown or untrusted individuals and companies. In other cases, staff are not aware of how cybercriminals can obtain their username and password in public while they attempt to log into their accounts by looking over their shoulder.

2.4.8 No Cyberattack Contingency Plan

The absence of a contingency plan for breached security is also a vulnerability. Without a contingency plan, when security in the Agri-IoT system is breached, there are no plans or measures in place to backup data and isolate the intrusion to prevent its escalation to the point where recovery becomes impossible.

2.5 Analysis of Impact

Analysis of impact is performed to determine the severity of damage that can be done to the Agri-IoT system should an attacker exploit any of the possible vulnerabilities in the system. The impact can be categorized into disconnection of nodes from the network, unauthorised access to data operation of system based on false data and total system shutdown

2.5.1 Loss of Nodes/Disconnection of Nodes from Network

When the physical security of a node is compromised, in a way that causes physical damage to the node, it can lead to damage to electrical circuits or wifi module which in turn results in the loss or disconnection of node from the Agri-IoT network. Also, attacks such as sleep deprivation attacks can cause nodes to be active for long hours to the extent that they run out of battery and die.

2.5.2 Unauthorised Access to Data

Malicious users can obtain confidential data which makes the produce from the farm top grade. Passive attacks such as eavesdropping and traffic analysis attacks can result in malicious users gaining unauthorized access to critical or highly confidential data. These data such as the formular for the fertilizer applied to crops can be what takes away the competitive advantage farmers have resulting in few sales.

2.5.3 Operation Based on False Data

Malicious users exploiting vulnerabilities that allow for code injection can jeopardize the Agri-IoT system by exposing it to the risk of operating on false data. For example, the irrigation system can be reprogrammed to send data affirming that it has sprinkled water on crops while it has not done so.

2.5.4 Total System Shutdown

The presence of multiple vulnerabilities in the Agri-IoT system means attackers can gain elevated privileges. With the elevated privilege, the risk of a total system shutdown becomes evident and high. Should the attacker decide to totally shut down the system, then the risk of total crop destruction can be achieved should contingency measures prove ineffective.

2.6 Prioritisation of Risk

The severity of various threats to the Agri-IoT system is assessed, and they are prioritized according to the impact they have on the system. Degree of impact of threats has been illustrated in Fig. 5.

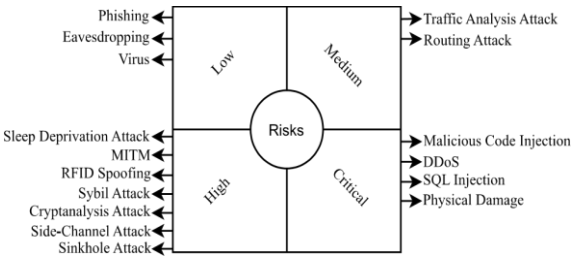

Fig. 5 Severity of Various Attacks on Agri-Iot

2.7 Mitigation Strategies

Mitigation strategies are employed to minimize the impact of risks and enhance the overall security of the system. Key strategies include regular firmware and application software updates, the installation of patches for communication protocols, and the implementation of physical security measures. Notably, encryption of data stands out as a critical strategy, as it helps protect sensitive information and

secure communications, addressing approximately 35% of potential threat which includes node tampering, RFID spoofing, man-in-the-middle, traffic analysis and cyrptanalysis threats. Together, these measures create a comprehensive security framework for Agri-IoT systems.

2.8 Review and Update of Mitigation Strategies

As technology advances and better ways of securing systems and data arise, the mitigation measures employed in the Agri-IoT system need to be revised and the needed updates applied accordingly to reduce the risk of attack.

3 Security

Although security in IoT has received a lot of attention such as in vehicular IoT, Industrial IoT, smart cities, this paper is of the view that Agri-IoT needs some security because not all Agri-IoT data must go unprotected. Agri-IoT is merging with agribusiness. Therefore, it is not just about production but from production to the end user, which means the information that goes through. This makes agricultural security very important. Security of Agri-IoT system is the protection of the system against unauthorised access and modification to devices and data while in processing, transit or storage. There are a number of Security models used for determining security measures needed for providing security in systems such as the CIA and the OSI.

3.1 CIA Triad

The Confidentiality Integrity Availability (CIA) triad is widely known when it comes to ensuring the security of systems. Every attack on a system focuses on compromising one or more of the three areas in the triad; confidentiality, integrity and availability (Kumar *et al.*, 2022).
Therefore measures implemented to ensure confidentiality, integrity and availability of devices and data while maintaining balance between them as shown in Fig. 6 ensures the security of Agri-IoT system without compromising on operation (Aminzade, 2018).

Confidentiality ensures unauthorised users do not have access to data and devices in order to prevent the disclosure of data. Here the devices and data should be accessible to authorised persons only and kept secret from all others as well as have measures put in place to prevent accidental disclosure of data (Kumar *et al.*, 2022; Obaidat *et al.*, 2020).

Integrity seeks to keep unauthorised modification of data and devices in order to prevent devices from sending false data as well as prevent the alteration of data stored on devices or in the process of transmission. In Agri-IoT, false data can cause the destruction of a whole plantation, such as data that causes the application of more fertilizer than needed (Kumar *et al.*, 2022; Obaidat *et al.*, 2020)

In an attempt to ensure the confidentiality, and integrity of data and devices, availability of both data and devices can be compromised (Obaidat *et al.*, 2020)Therefore. It is important to ensure the availability of devices, services and data. Authorised persons should have access to devices and data anytime they need it. Unauthorised users on the other had should not be able to access devices and data. In addition, they should not be able to prevent authorized persons from accessing devices and services (Kumar *et al.*, 2022)

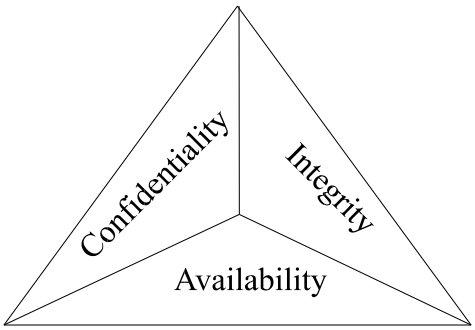

Fig. 6 CIA Triad

3.2 OSI Security Architecture

According to the OSI security architecture, provided there are security attacks, security mechanisms and Security services can be employed to protect and safeguard systems and the data as shown in Fig. 7.

Security services are services employed to ensure the security and safety of data and systems. They include authentication, access control, data confidentiality, data integrity and non-repudiation.

Security mechanisms are built into systems to identify or prevent security breaches. They can be implemented to provide confidentiality, integrity, and availability to protect systems, networks, or node devices. Security mechanisms that can be employed to ensure security include encipherment (encryption), digital signature, traffic padding, and routing control, among others. However, this paper focuses on encryption security mechanisms employed to safeguard Agri-IoT systems against attacks.

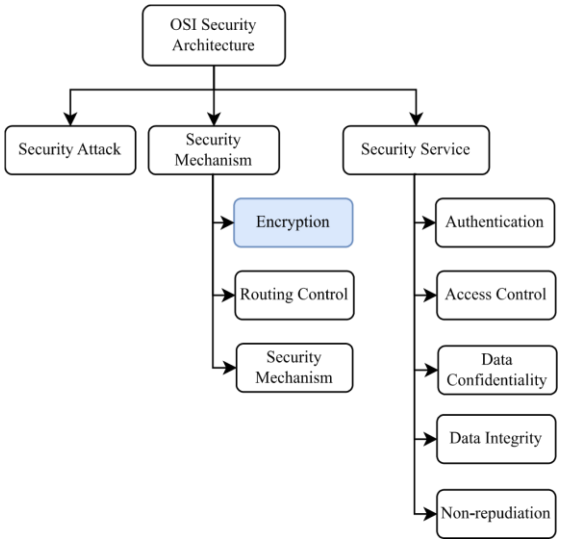

Fig. 7 OSI Security Architecture

4 Encryption Security Mechanism

In light of the numerous vulnerabilities that can be subjected to exploitation by the many threat actors, taking into consideration the risks exploitation of these vulnerabilities pose to the Agri-IoT system it is of utmost importance security measures are put in place to ensure the confidentiality, integrity and availability of data in a balanced manner, eventually making the operational efficiency of the Agri-IoT system in terms of data dissemination and processing as well as security sure. There are several security mechanisms available for ensuring security in IoT based systems. However, these mechanisms are context relevant. These mechanisms include intrusion detection and prevention systems, blockchain mechanisms, encryption algorithms, software defined networking, Data privacy and consent, access controls. However, this paper focuses on encryption as a security mechanism for Agri-IoT systems. The literature review was done using papers from reputable databases. These include IEEE Xplore, SpringerLink, ScienceDirect, and ACM Digital Library. Much focus was given to papers within the last 5 years. For inclusion criteria, performance, cost, and scalability were taken into consideration, while papers published before 2019, and non-peer-reviewed-sources formed part of the exclusion criteria.

Data within the Agri-IoT system can be made secure for transmission using the encryption cryptography technique. Encryption refers to the process of securing plain text (message) through conversion of the data into hidden text (ciphertext). The process of converting the ciphertext back to plain text is decryption. In the encryption and decryption process, strings of numbers (keys) are used. Without, the key, it should be extremely difficult for ciphertext to be decrypted. Fig. 8 illustrates the general process of encrypting and decrypting data (Alenezi *et al.*, 2020). There are two types of encryption techniques. These the depend the type of key being used. That is, whether the key for encryption and decryption is symmetric or asymmetric.

Conventional encryption algorithms, both symmetric and asymmetric, present computational challenges for Agri-IoT applications. Symmetric algorithms, while generally faster, still require significant processing power, which can strain the limited resources of IoT devices in agricultural settings. Asymmetric algorithms, on the other hand, demand even more computational resources due to their complex key management and encryption processes, making them slow and inefficient for real-time applications as explained in section 4.1 and 4.2.

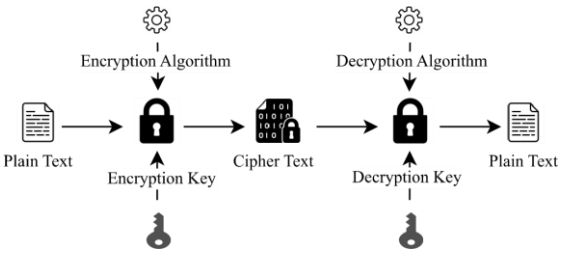

Fig. 8 Illustration of Encryption and Decryption

4.1 Symmetric Key Encryption and Decryption

Symmetric encryption is a type encryption, where a single key is used for both encryption and decryption of plain text to ciphertext and decryption of ciphertext to plain text. The encryption and decryption key, known as the private key is shared over a secure channel to avoid unauthorised access (Alenezi *et al.*, 2020). Symmetric key encryption can be categorised under block cipher, and stream cipher. In the block cipher, the data is divided into blocks, after which every block will be encrypted to obtain ciphertext for each block. Finally, all the cyphertext is put together to obtain the final ciphertext. The size of blocks used in block cipher is usually 64-bit. However, more recent ones use 128-bit blocks. In stream cipher every bit is combined with a pseudorandom key to encrypt the data in a bit-by-bit manner. Fig. 9 illustrates the process of performing symmetric encryption and decryption. Examples of block cipher symmetric encryption algorithms include DES, IDEA, Blowfish, among others. Examples of stream cipher include RC4, TKIPP, among others.

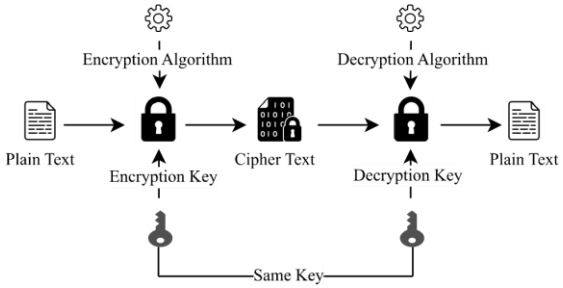

Fig. 9 Illustration of Symmetric Encryption

4.1.1 Data Encryption Standard (DES)

DES is a symmetric key block cipher that uses both substitution and transposition operations. The DES algorithm is used for encrypting 64-bit blocks of plain text at a time. It also uses a 56-bit key, of which 8 bits for checking parity is added to make it 64 (Alenezi *et al.*, 2020). However, it is not counted as part of the length of the key. Since the key is 56-bit, the number of ways that exist to find the right key is 2^{56}. From the 56-bit key, 16-bit round keys (k_i) are generated to be used in all the 16 rounds of encryption. Beginning the encryption, the 64-bit text is subject to permutation at the initial permutation (IP) stage. Where bits are replaced with other bits within the 64-bit plain text. For example, the 5th bit will be replaced with the 32nd bit. After this, the Feistel network rounds begin, and the permutated plain text is divided into two 32-bit halves (L_i and R_i). The right half (R_i) would then be fed as input to the Feistel function (F) along with round key (K_i) the result XORed is with the left half (L_i). Fig. 10 illustrates how the F function works in DES. Afterwards, the new left half is equal to the right half, and the right half is equal to the values obtained after the XORing operation. This process is repeated for the 16 rounds after which the final permutation (FP) is performed to produce the 64-bit ciphertext. However, when a weak key is used, DES is prone to bruteforce key attacks (Paradesi Priyanka *et al.*, 2022). Fig. 11 illustrates the process of converting plain text to ciphertext using DES.

2.1.2 Advanced Encryption Standard (AES)

AES is a block cipher encryption algorithm designed to replace DES and 3DES. AES can use one out of three (3) lengths of key. That is 128, 192 and 256. Based on the length of keys used the encryption will be stronger or weaker (Alenezi *et al.*, 2020). This is because the longer the length of key the stronger the encryption. The block size of data to be encrypted is fixed in AES, usually 128 bits with the rounds for encryption being either 10, 12 or 14. The main operations performed in each round is; byte substitution, row shifting column mixing and addition of round key. However, in the final round column mixing operation is not performed.

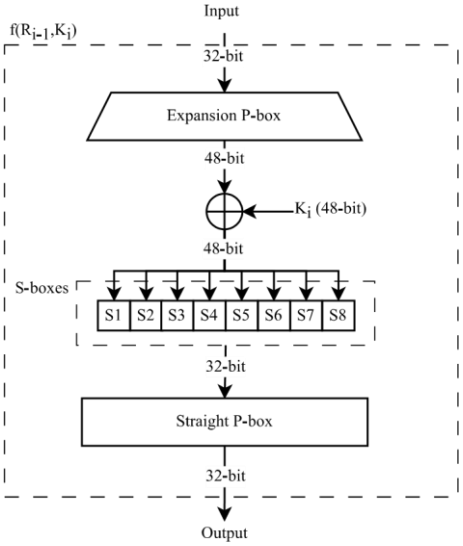

Fig. 10 Illustration of F Function of DES

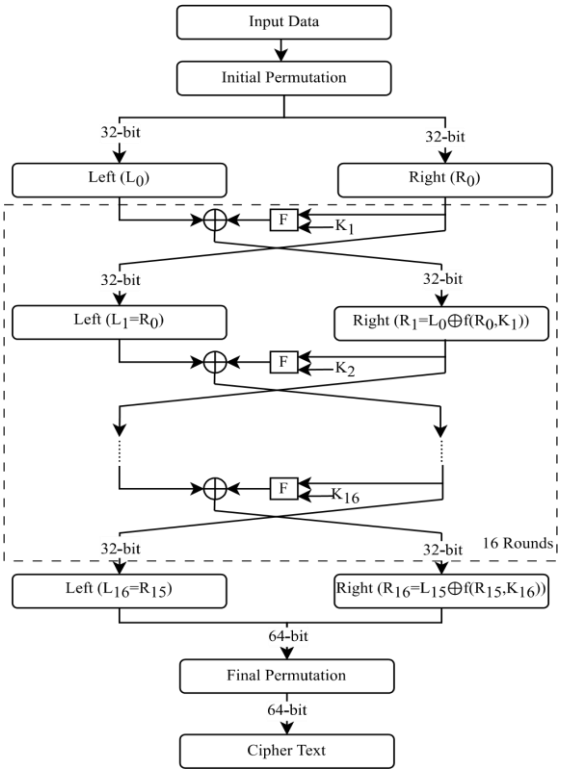

Fig. 11 Illustration of DES Encryption

At the byte substitution stage, every byte in the block is substituted with another byte from a fixed substitution table called the S-box. In the row shifting, the rows are shifted to the left. Here, the first row is not shifted (Alenezi *et al.*, 2020). However, the shifting of the rows depends on the rows. The second row is shifted by one, the third row is shifted by two, and the fourth row is shifted by three. Column mixing is used to introduce confusion by multiplying the mix column input matrix by a predetermined matrix. Finally, at the add round key stage the round key is added through bitwise XOR operation of the block with the round key. AES is

not suitable for Agri-IoT due to its computational intensity and resource demands. The encryption and decryption processes can require significant processing power and memory, which many resource-constrained Agri-IoT devices lack. The operation of AES is illustrated in Fig. 12.

4.1.3 International Data Encryption Algorithm (IDEA)

IDEA is a symmetric block-based cipher that encrypts 64-bit blocks of data at a time using a 128-bit key size. Each 64-bit of data is divided into four 16-bit sub-blocks. It uses mathematical operations including modular arithmetic, XOR and bit shifting to convert the 64-bit plain text to ciphertext (Alenezi *et al.*, 2020). The number of rounds for encryption is 8. For each round six sub-keys generated from 128-bit key size is used. The output obtained from each round serves as input for the next until all 8 rounds are completed. The output for the final round undergoes transformation to output the ciphertext as illustrated in Fig. 13. IDEA is not optimised for better performance like AES. As a result, it is much more resource-intensive and unsuitable for Agri-IoT.

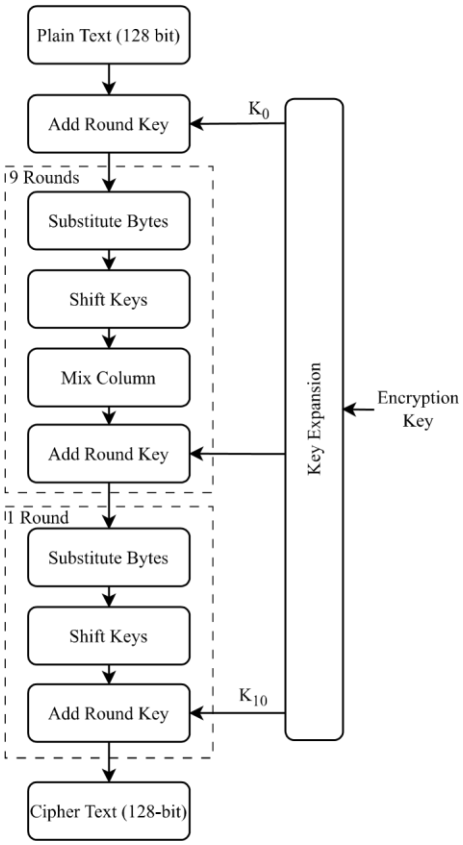

Fig. 12 Illustration of AES

4.1.4 RC4

This is a symmetric stream cipher where encryption is performed on a character at a time. It is usually employed in wireless routers. In RC4, the length of the key ranges from 40 to 2048 bits. However, 16-byte keys are effective for robust text encryption. Here, the blocks of data are XORed with keystream bytes, which are obtained through a pseudorandom key generator that outputs the ciphertext.

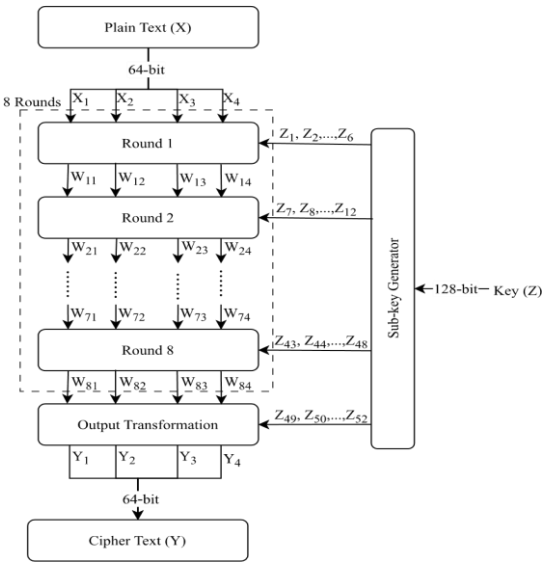

Fig. 13 Illustration of IDEA Encryption

In its working permutation, numbers from 0 to 255 are used to generate an s-block of 8*8 size, and a 256-byte long table is also initialised with a variable key length from 1 to 256 bytes.
Using the provided encryption key the entries in the s-box is shuffled by using the bytes in the key and their position. This is achieved through the key-scheduling algorithm. After which, a pseudorandom generation algorithm will be used to generate a pseudo-random key stream from the permutated s-box, all the while iteratively swapping elements in the s-box. Afterward, the keystream is XORed with the corresponding plain text byte to obtain the ciphertext, as shown in Fig. 14. RC4 is not suitable for Agri-IoT due to several significant vulnerabilities such as key recovery vulnerabilities and output biases. These make it susceptible to various attacks, compromising data integrity and confidentiality.

4.1.5 BlowFish

The BlowFish algorithm is an encryption algorithm whose key length varies from 32-bit to 448 bits. It is a block-based encryption algorithm. Each block of data contains 64 bits of data. The number of rounds involved in the encryption process is 16. It uses both permutation and substitution methods in the encryption process through P-block and S-block respectively, where the P-block contains 18 subkeys with each subkey being 32-bit and the number of S-blocks being 4 with each having 256 entries of 32-bit each.

To encrypt a 64-bit data it is divided into two halves of 32 bit each (L_i, R_i). The left (L_i) is then XORed with P_i, after which the output is fed as input to the BlowFish function (F) where it will be divided into 4 subblock of 8 bits each.

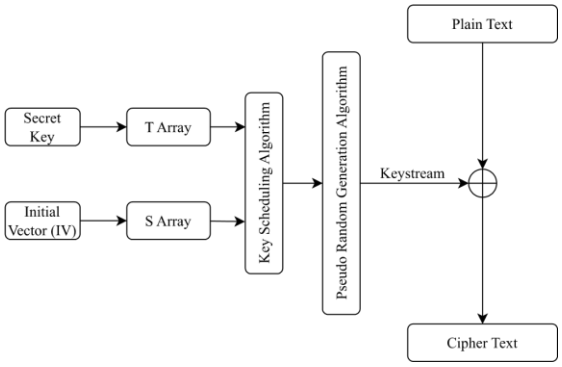

Fig. 14 Illustration of RC4 Function

Then bytes within each block is substituted with values from a corresponding S-block through using the byte as an index to retrieve the value from the corresponding S-box. The output from the substitution is 32-bits. Modular addition will be performed on two of outputs and XORed with the third output. The output from that is also added to the final one through modular addition to obtain the final output F as illustrated in Fig. 15. The output F is then XORed with R_i to obtain a new R_i. After which L_i and R_i are swapped. This process is done for all the 16 rounds. After the 16 rounds are completed, L_i and R_i are swapped again and P_{17} is XORed with R_i and P_{18} XORed with L_i. The resulting L_i and R_i are combined to give the ciphertext as illustrated in Fig. 16. Blowfish however requires more memory for its internal state and key scheduling making it unsuitable for Agri-IoT.

4.1.6 3DES

Three DES is a block cipher algorithm which is based on DES. In order to enhance the security of data the DES cipher applied to each block of data to be encrypted 3 times (Alenezi *et al.*, 2020). Hence the strength of the encryption is three times that of DES. The length of key used in 3DES is 112 bits or 168 bit and the data blocks of 64 bit each. 3DES was developed to be stronger than DES since the 56-bit key employed in DES could be subject to a successful brutefore attack. Hence, 3DES basically performs the same encryption steps as DES, however, this is done thrice. Given a 64-bit block plain text message, DES encryption is performed using a first key, the resulting ciphertext is also encrypted using a second key, and finally a third and final key is used to encrypt the resulting ciphertext after the second encryption. However, due to the repeated encryption process the average time of encryption and resources used is higher (Paradesi Priyanka *et al.*, 2022). Since applies the DES encryption algorithm to the data 3 times, it is computationally intensive and unsuitable for Agri-IoT.

4.1.7 TwoFish

This is also a block-based cipher for encrypting 128-bit block size. Key sizes used for encryption are 128, 198 or 256. The number of rounds used in for encryption is 16 (Alenezi *et al.*, 2020). Before the rounds begin the plaintext goes through input whitening where it is XORed with additional subkeys generated from 4 blocks of 32-bit after which they

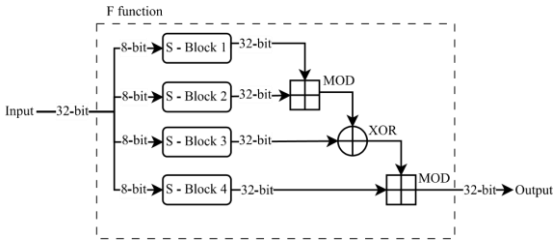

Fig. 15 BlowFish F Function

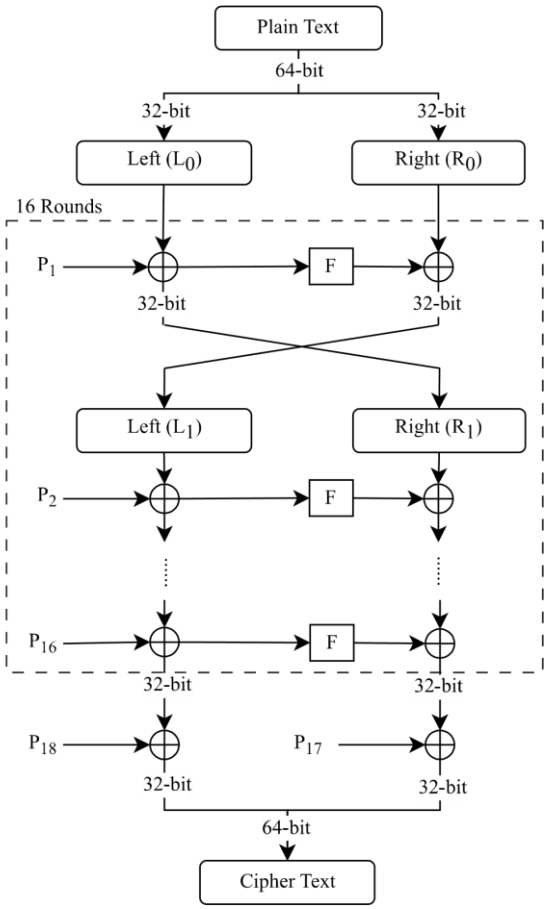

Fig. 16 Illustration of BlowFish

By dividing the original key (X, Y, Z, W). After whitening two data blocks (X and Y) are fed as input to the F function. In the function F, where they are divided into four bytes and they go through four corresponding key-dependent s-boxes. The maximum Distance Separable (MDS) matrix is used to combine the output of the four s-boxes to form a word of 32-bits. The output from the MDS matrix is combined using two round subkeys. The result is XORed with the second half of the text. Before performing the XOR operation 1-bit rotation is performed, likewise after the XOR operation.
After the 16 rounds are completed, the last swap is undone, and post-whitening is performed by XORing the output with additional subkeys to obtain the final ciphertext. Twofish is resource-intensive and has limited adoption and support, making it unsuitable for Agri-IoT.

4.2 Asymmetric Key Encryption and Decryption

Asymmetric key encryption is an encryption that uses two keys. Here, public and private key is used. The public key is known by all devices on the network. However, the private key for each device is known by that device only. In order to transmit data, the sender's public key is used to encrypt the data for transmission. After the data is received by the recipient, it is decrypted using the recipient's private key. Examples of asymmetric algorithms include RSA, DSA, ECC and Delfie Helman. Fig. 17 gives an illustration of the process of encrypting and decrypting data using asymmetric key (Alenezi *et al.*, 2020).

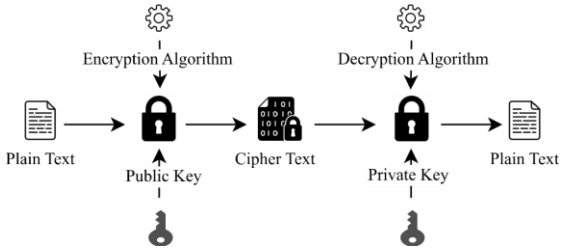

Fig. 17 Illustration of Asymmetric Encryption

4.2.1 Rivest-Shamir-Adleman

RSA is a cryptosystem that utilizes the asymmetric key. That is, it is public-key based. Hence it uses one key for encryption (public key) and another for decryption (private key). The factoring problem associated with prime numbers forms the basis for this encryption algorithm (Alenezi *et al.*, 2020). That is, the difficulty in finding the factors of a number which is the product of two prime numbers. In its operation n is the product of two prime numbers p and q which in turn will be used as the modulo for the public and private keys. The totient of n is given as $\phi(n) = (p-1)(q-1)$. After which a prime number greater than 1 however less than $\phi(n)$, that is $(1 < e < \phi(n))$. Usually, *65537* is used as the value for e. That is $e = 2^{16} + 1 = 65537$, since its modular exponentiation is efficient. Once e is obtained d can be calculated for as $(d * e), \phi(n) = 1$. Finally, we have the public key as (e, n) and the private key as (d, n). Therefore, in order to encrypt plain text message M to a ciphertext C and back to plain text message again, the following equations are used respectively.

$$C = M^e (mod\ n) \quad (1)$$

$$M = C^d (mod\ n) \quad (2)$$

Where M < n. Should the plain text message be greater than n ($M > n$), it is viewed as a concatenation of plain text messages and each part is encrypted separately.

However, if p and q used to generate the key is small, the cipher can easily be decrypted. On the other hand, if p and q have large lengths then the challenge of time inefficiency arises (Paradesi Priyanka *et al.*, 2022). Additionally, the computational requirement and key size (2048-bit) of RSA it is unsuitable for Agri-IoT.

5 Open Issues

This paper has firmly established the importance of the incorporation of IoT in agriculture to meet the current food demand and expected food production demand in the near future. In light of this, a steep rise is expected in the role IoT plays in producing food products of the highest quality with little human efforts. However, there are some open issues regarding Agri-IoT:

- The field of Agri-IoT has not received enough research on the potential vulnerabilities in the system and the cyber threats it faces.
- Enough research has not been done on the risk of food insecurity and its economic impact on society should Agri-IoT systems come under attack.
- Existing conventional encryption, such as AES and DES, are resource and time-intensive. That is, they require a lot of processing power and electrical power and take quite some time to encrypt data, which is not suitable for resource-constrained, low-power devices that are used for obtaining and transmitting real-time data in Agri-IoT. Researchers have proposed alternative encryption models for resource-constrained IoT applications, targeting general IoT or specific domains such as smart health and smart cities. However, these approaches have limitations that render them unsuitable for Agri-IoT applications, as highlighted in Table 2.

Table 2 Comparative Analysis of Proposed Encryption Algorithms

Paper	Technology Used	Motive	Domain	Strength	Limitations
(Sharma and Purushothama, 2023)	Multiple multicast encryption	Enable and ensure secure communication across multiple multicast groups	General IoT	Allows for communication across multiple groups	Storage cost for multiple secrets is high
(Ettiyan and V., 2023)	DNA-based encryption system	Secure data from the monitoring system	Smart Healthcare	Confidentiality, Integrity, Authenticity	High computational cost, High computational overheads
(Yousefi and Jameii, 2017)	Hybrid encryption	Secure data using encryption with less computational complexity with speed	General IoT	Data confidentiality, computationally efficient	Difficulty in integration with existing networks
(Tawalbeh *et al.*, 2022)	Enhanced AWSIoTAC model	Provide a latent and energy-efficient IoT model	Smart Healthcare	Confidentiality, Integrity	Power consumption can be reduced further using machine learning
(Kiran *et al.*, 2023)	Discrete-time chaotic maps	Provide a lightweight encryption mechanism for robots	Smart Industry	High-rate image encryption per second	High-end hardware requirement for computation
(Medileh *et al.*, 2020)	Flexible Encryption Technique (FlexenTech)	Protect data in storage and transit	General IoT	Low energy consumption, less computation time, confidentiality, integrity	Variable rounds hence rounds may be set to be computationally intensive or may be inadequate for efficient encryption
(Sheikhpour *et al.*, 2021)	low-cost attack resilience AES encryption	Provide 32-bit architecture for encryption for resource constraint applications	General IoT	Can detect almost all injected faults	Has error detection capability for only AES
(Karati *et al.*, 2019)	Generalized Signcryption With Public Verifiability	To ensure authenticity and confidentiality of data between two parties	General IoT	Confidentiality, Authenticity	Less secure due to un-forgeability
(Ahirwal *et al.*, 2013)	Encryption and decryption that utilizes Signcryption Scheme that incorporates Elliptic Curve	Secure transmission of data	Not domain specific	Less time than RSA	The number of ECPM operations is more therefore it is less efficient

6 Conclusion

This paper discusses the increasing predominance of IoT technology in the world, giving insight to the application areas of IoT. The need for the incorporation of IoT into agriculture. The cyber threats Agri-IoT faces through using the threat model, the impact, associated risks and encryption as a mitigation. This paper highlighted popular encryption algorithms and the associated limitations that makes their incorporation in Agri-IoT unsuitable. A comparative analysis of proposed encryption models is also performed to highlight the gap in secure resource-efficient encryption models in Agri-IoT.

Acknowledgement

We are grateful to The Agri-IoT Project and the University of Mines and Technology (UMaT) for their support.

References

A J. S., Chakravarthy R. and L M. L. (2022), "An Experimental study of IoT-Based Topologies on MQTT protocol for Agriculture Intrusion Detection", *Measurement: Sensors*, Vol. 24, p. 100470, doi: https://doi.org/10.1016/j.measen.2022.100470.

Abbasi M., Yaghmaee M.-H. and Rahnama F. (2019), "Internet of Things in agriculture: A survey", pp. 1–12, doi: 10.1109/IICITA.2019.8808839.

Abomhara M. and Køien G. M. (2015), "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks", *Journal of Cyber Security and Mobility*, Vol. 4, No. 1, pp. 65–88, doi: 10.13052/jcsm2245-1439.414.

Aditya Sai Srinivas T. and Manivannan S. S. (2020), "Prevention of Hello Flood Attack in IoT using combination of Deep Learning with Improved Rider Optimization Algorithm", *Computer Communications*, Vol. 163, pp. 162–175, doi: 10.1016/j.comcom.2020.03.031.

Ahirwal R., Jain A. and Jain Y. (2013), "Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation", *International Journal of Computer Applications*, Vol. 62, pp. 41–48, doi: 10.5120/10112-4777.

Akhtar M., Raffeh M., ul Zaman F., Ramzan A., Aslam S. and Usman F. (2020), "Development of congestion level based dynamic traffic management system using IoT", *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pp. 1–6, doi: 10.1109/ICECCE49384.2020.9179375.

Akhter R. and Sofi S. A. (2022), "Precision agriculture using IoT data analytics and machine learning", *Journal of King Saud University - Computer and Information Sciences*, Vol. 34, No. 8, Part B, pp. 5602–5618, doi: https://doi.org/10.1016/j.jksuci.2021.05.013.

Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M. and Ayyash M. (2015), "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Communications Surveys and Tutorials*, Vol. 17, No. 4, pp. 2347–2376, doi: 10.1109/COMST.2015.2444095.

Aldaej A. (2019), "Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)", *IEEE Access*, pp. 1–1, doi: 10.1109/access.2019.2893445.

Aleksic S. (2019), "A Survey on Optical Technologies for IoT, Smart Industry, and Smart Infrastructures", *Journal of Sensor and Actuator Networks*, Vol. 8, No. 3, doi: 10.3390/jsan8030047.

Alenezi M., Alabdulrazzaq H. and Mohammad N. (2020), "Symmetric Encryption Algorithms: Review and Evaluation study", *International Journal of Communication Networks and Information Security*, Vol. 12, p. 256.

Alqinsi P., Matheus Edward I. J., Ismail N. and Darmalaksana W. (2018), "IoT-Based UPS Monitoring System Using MQTT Protocols", *Proceeding of 2018 4th International Conference on Wireless and Telematics, ICWT 2018*, IEEE, doi: 10.1109/ICWT.2018.8527815.

Aminu Ghali A., Ahmad R. and Alhussian H. S. A. (2020), "Comparative Analysis of DoS and DDoS Attacks in Internet of Things Environment", in Silhavy, R. (Ed.), *Artificial Intelligence and Bioinspired Computational Methods*, Springer International Publishing, Cham, pp. 183–194.

Aminzade M. (2018), "Confidentiality, integrity and availability – finding a balanced IT framework", *Network Security*, Vol. 2018, No. 5, pp. 9–11, doi: https://doi.org/10.1016/S1353-4858(18)30043-6.

Andrea I., Chrysostomou C. and Hadjichristofi G. (2015), "Internet of Things: Security vulnerabilities and challenges", *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180–187, doi: 10.1109/ISCC.2015.7405513.

Antony A. P., Leith K., Jolley C., Lu J. and Sweeney D. J. (2020), "A Review of Practice and Implementation of the Internet of Things (IoT) for Smallholder Agriculture", *Sustainability*, Vol. 12, No. 9, doi: 10.3390/su12093750.

Asif M. R. Al, Hasan K. F., Islam M. Z. and Khondoker R. (2021), "STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems", *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, pp. 1–6, doi: 10.1109/STI53101.2021.9732597.

Badenhop C., Graham S., Ramsey B., Mullins B. and Mailloux L. (2017), "The Z-Wave routing protocol and its security implications", *Computers \& Security*, Vol. 68, doi: 10.1016/j.cose.2017.04.004.

Bhattasali T., Chaki R. and Sanyal S. (2012), "Sleep Deprivation Attack Detection in Wireless Sensor Network", *International Journal of Computer Applications*, Vol. 40, No. 15, pp. 19–25, doi: 10.5120/5056-7374.

Brasilino L. R. B. and Swany M. (2019), "Low-Latency CoAP Processing in FPGA for the Internet of Things", *Proceedings - 2019 IEEE International Congress on Cybermatics: 12th*

IEEE International Conference on Internet of Things, 15th IEEE International Conference on Green Computing and Communications, 12th IEEE International Conference on Cyber, Physical and So, IEEE, pp. 1057–1064, doi: 10.1109/iThings/GreenCom-/CPSCom/SmartData.2019.00182.

Butun I., Osterberg P. and Song H. (2020), "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures", *IEEE Communications Surveys and Tutorials*, Vol. 22, No. 1, pp. 616–644, doi: 10.1109/COMST.2019.2953364.

Caiza G., Llamuca E. S., Garcia C. A., Gallardo-Cardenas F., Lanas D. and Garcia M. V. (2019), "Industrial Shop-Floor Integration Based on AMQP protocol in an IoT Environment", *2019 IEEE 4th Ecuador Technical Chapters Meeting, ETCM 2019*, IEEE, doi: 10.1109/ETCM48019.2019.-9014858.

Chen L., Thombre S., Järvinen K., Lohan E. S., Alén-Savikko A., Leppäkoski H., Bhuiyan M. Z. H., *et al.* (2017), "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey", *IEEE Access*, Vol. 5, pp. 8956–8977, doi: 10.1109/ACCESS.2017.2695525.

Dalkilic H. and Ozcanhan M. H. (2021), "Strong Authentication Protocol for Identity Verification in Internet of Things (IoT)", *2021 6th International Conference on Computer Science and Engineering (UBMK)*, IEEE, pp. 199–203, doi: 10.1109/ubmk52708.2021-.9559010.

Deogirikar J. and Vidhate A. (2017), "Security attacks in IoT: A survey", *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 32–37, doi: 10.1109/I-SMAC.2017.8058363.

Duangphasuk S., Duangphasuk P. and Thammarat C. (2020), "Review of Internet of Things (IoT): Security Issue and Solution", *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 559–562, doi: 10.1109/ECTI-CON49241.2020.9157904.

Durojaye H. and Raji O. (2022), "Impact of State and State-Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure", doi: 10.13140/RG.2.2.364-53.06883.

Effah E., Thiare O. and Wyglinski A. M. (2023), "A Tutorial on Agricultural IoT: Fundamental Concepts, Architectures, Routing, and Optimization", *IoT*, Vol. 4, No. 3, pp. 265–318, doi: 10.3390/iot4030014.

Ejaz W., Anpalagan A., Imran M. A., Jo M., Naeem M., Qaisar S. B. and Wang W. (2016), "Internet of Things (IoT) in 5G Wireless Communications", *IEEE Access*, Vol. 4, pp. 10310–10314.

Ettiyan R. and V. G. (2023), "A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems", *Healthcare Analytics*, Vol. 3, p. 100149, doi: https://doi.org/10.1016/j.health.2023.100149.

Feng Y., Huang W., Wang S., Zhang Y. and Jiang S. (2021), "Detection of RFID cloning attacks: A spatiotemporal trajectory data stream-based practical approach", *Computer Networks*, Vol. 189, p. 107922, doi: https://doi.org/-10.1016/j.comnet.2021.107922.

Ferrag M. A., Shu L., Yang X., Derhab A. and Maglaras L. (2020), "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges", *IEEE Access*, Vol. 8, pp. 32031–32053, doi: 10.1109/ACCESS.2020.2973178.

Gajbhiye A., Sen D., Bhatt A. and Soni G. (2020), "DPLPLN: Detection and Prevention from Flooding Attack in IoT", *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 704–709, doi: 10.1109/ICOSEC49089.2020.9215381.

Hafeez I., Antikainen M. and Tarkoma S. (2019), "Protecting IoT-environments against Traffic Analysis Attacks with Traffic Morphing", *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 196–201, doi: 10.1109/PERCOMW.2019.8730-787.

Hassija V., Chamola V., Saxena V., Jain D., Goyal P. and Sikdar B. (2019), "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", *IEEE Access*, Vol. 7, pp. 82721–82743, doi: 10.1109/ACCESS.2019.2924045.

Ibrahim R., Abu Al-Haija Q. and Ahmad A. (2022), "DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology", *Sensors*, Vol. 22, p. 6806, doi: 10.3390/s22186806.

Islam S. M. R., Kwak D., Kabir M. D. H., Hossain M. and Kwak K.-S. (2015), "The Internet of Things for Health Care: A Comprehensive Survey", *IEEE Access*, Vol. 3, pp. 678–708, doi: 10.1109/ACCESS.2015.2437951.

Jiang J. and Liu Y. (2022), "Secure IoT routing: Selective forwarding attacks and trust-based defenses in RPL network", *ArXiv Preprint ArXiv:2201.06937*.

Karati A., Fan C.-I. and Hsu R.-H. (2019), "Provably Secure and Generalized Signcryption With Public Verifiability for Secure Data Transmission Between Resource-Constrained IoT Devices", *IEEE Internet of*

Things Journal, Vol. 6, No. 6, pp. 10431–10440, doi: 10.1109/JIOT.2019.2939204.

Kareem F., Ameen S., Ahmed A., Salih A., Ahmed D., Kak S., Najat Z., *et al.* (2021), "SQL Injection Attacks Prevention System Technology: Review", *Asian Journal of Research in Computer Science*, doi: 10.9734-/AJRCOS/2021/v10i330242.

Kassim M. R. M. (2020), "IoT Applications in Smart Agriculture: Issues and Challenges", *2020 IEEE Conference on Open Systems, ICOS 2020*, pp. 19–24, doi: 10.1109-/ICOS50156.2020.9293672.

Kassim M. R. M. (2022), "Applications of IoT and Blockchain in Smart Agriculture: Architectures and Challenges", *2022 IEEE International Conference on Computing (ICOCO)*, pp. 253–258, doi: 10.1109/ICOCO56118.2022.10031697.

Kaur K. (2018), "A Survey on Internet of Things – Architecture, Applications, and Future Trends", *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 581–583, doi: 10.1109-/ICSCCC.2018.8703341.

Keerthika M. and Shanmugapriya D. (2021), "Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures", *Global Transitions Proceedings*, Vol. 2, No. 2, pp. 362–367, doi: 10.10-16/j.gltp.2021.08.045.

Khodayer Al-Dulaimi O. M., Hassan Al-Dulaimi M. K. and Khodayer Al-Dulaimi A. M. (2022), "Analysis of Low Power Wireless Technologies used in the Internet of Things (IoT)", *2022 2nd International Conference on Computing and Machine Intelligence (ICMI)*, pp. 1–6, doi: 10.1109/ICMI55296.2022.-9873714.

Kiran H. E., Akgul A., Yildiz O. and Deniz E. (2023), "Lightweight encryption mechanism with discrete-time chaotic maps for Internet of Robotic Things", *Integration*, Vol. 93, p. 102047, doi: https://doi.org/10.1016/j-.vlsi.2023.06.001.

Kristen E., Kloibhofer R., Hernández V. and Castillejo P. (2021), "Security Assessment of Agriculture IoT (AIoT) Applications", *Applied Sciences*, Vol. 11, p. 5841, doi: 10.3390/app11135841.

Kumar A., Saha R., Conti M., Kumar G., Buchanan W. J. and Kim T. H. (2022), "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions", *Journal of Network and Computer Applications*, Vol. 204, p. 103414, doi: https://doi.org/10.1016/j.jnca.2022.103414.

Lee S.-H., Shiue Y.-L., Cheng C.-H., Li Y.-H. and Huang Y.-F. (2022), "Detection and Prevention of DDoS Attacks on the IoT", *Applied Sciences*, Vol. 12, No. 23, doi: 10.3390/app122312407.

Mahajan P. (2021), "Internet of things revolutionizing Agriculture to Smart Agriculture", *2021 2nd Global Conference for Advancement in Technology (GCAT)*, pp. 1–6, doi: 10.1109/GCAT52182.2021.9587896.

Medileh S., Laouid A., Nagoudi E. M. B., Euler R., Bounceur A., Hammoudeh M., AlShaikh M., *et al.* (2020), "A flexible encryption technique for the internet of things environment", *Ad Hoc Networks*, Vol. 106, p. 102240, doi: https://doi.org/10.1016/j.adhoc.2020.102240.

Muthavhine K. D. and Sumbwanyambe M. (2022), "Preventing Differential Cryptanalysis Attacks Using a KDM Function and the 32-Bit Output S-Boxes on AES Algorithm Found on the Internet of Things Devices", *Cryptography*, Vol. 6, No. 1, doi: 10.3390-/cryptography6010011.

Noman H. A. and Abu-Sharkh O. M. F. (2023), "Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations", *Sensors*, Vol. 23, No. 13, doi: 10.3390/s-23136067.

Obaidat M. A., Obeidat S., Holst J., Hayajneh A. Al and Brown J. (2020), "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures", *Computers*, Vol. 9, No. 2, doi: 10.3390/computers9020044.

Orpa T. H., Ahnaf A., Ovi T. B. and Rizu M. I. (2022), "An IoT Based Healthcare Solution With ESP32 Using Machine Learning Model", *2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI)*, pp. 1–6, doi: 10.1109/STI5-6238.202-2.10103231.

Paradesi Priyanka M., Kaur N., Nazir N., Ali Khan A., Vikram Singh M., Kaur M., Behera T., *et al.* (2022), "A Comparative Review between Modern Encryption Algorithms viz. DES, AES, and RSA", *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, pp. 295–300, doi: 10.1109/C-ISES54857.2022.9844393.

Pawaskar M., Aneesh S., Sharma D., Sawale P., Sharma R. and Sharma A. (2021), "IoT enabled Smart Dustbin using Zigbee Network", *2021 International Conference on Advances in Computing, Communication, and Control (ICAC3)*, pp. 1–4, doi: 10.1109/-ICAC353642.2021.9697275.

Plotnek J. J. and Slay J. (2021), "Cyber terrorism: A homogenized taxonomy and definition", *Computers \& Security*, Vol. 102, p. 102145,

doi: https://doi.org/10.1016/j.cose.2020.102145.

Prates N., Vergütz A., Macedo R. T., Santos A. and Nogueira M. (2020), "A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic", *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pp. 1–6, doi: 10.1109/GLOBECOM42002.2020.9322070.

Purnama A. and Nashiruddin M. I. (2020), "SigFox-based Internet of Things Network Planning for Advanced Metering Infrastructure Services in Urban Scenario", pp. 15–20, doi: 10.1109/IAICT50021.2020.9172022.

Richet J.-L. (2022), "How cybercriminal communities grow and change: An investigation of ad-fraud communities", *Technological Forecasting and Social Change*, Vol. 174, p. 121282, doi: https://doi.-org/10.1016/j.techfore.2021.121282.

Sachitra V. and Chong S.-C. (2016), "Firm Level Competitive Advantage in the Agricultural Sector: A Research Agenda", *British Journal of Economics, Management, and Trade*, Vol. 12, pp. 1–12, doi: 10.9734/BJEMT/-2016/24152.

Sah D. K., ravindra C., Cengiz K., Alshehri Y., Alnazzawi N. and Ivković N. (2022), "Early alert for sleep deprivation using mobile sensor data fusion", *Computers and Electrical Engineering*, Vol. 102, p. 108228, doi: https://doi.org/10.1016/j.compeleceng.2022.1 08228.

Sailio M., Latvala O.-M. and Szanto A. (2020), "Cyber Threat Actors for the Factory of the Future", *Applied Sciences*, Vol. 10, p. 4334, doi: 10.3390/app10124334.

Sarath Chandra D. V., Kaur G. and Bhattacharya M. (2023), "Smart Irrigation Management System for Precision Agriculture", *2023 International Conference on Advances in Intelligent Computing and Applications (AICAPS)*, pp. 1–5, doi: 10.1109/AICA-PS57044.2023.10074171.

Sethi P. and Sarangi S. R. (2017), "Internet of Things: Architectures, Protocols, and Applications", *Journal of Electrical and Computer Engineering*, Vol. 2017, pp. 1–25, doi: 10.1155/2017/9324035.

Sharma P. and Purushothama B. R. (2023), "Generalization of multicast encryption for Internet of Things deployment", *Journal of Information Security and Applications*, Vol. 77, p. 103571, doi: https://doi.org/10.10-16/j.jisa.2023.103571.

Sharma S. K., Bogale T. E., Chatzinotas S., Wang X. and Le L. (2016), "Physical layer aspects of wireless IoT", pp. 304–308, doi: 10.1109/ISWCS.2016.7600919.

Sheikhpour S., Ko S.-B. and Mahani A. (2021), "A low cost fault-attack resilient AES for IoT applications", *Microelectronics Reliability*, Vol. 123, p. 114202, doi: 10.1016/j.mic-rorel.2021.114202.

Sunhare P., Chowdhary R. R. and Chattopadhyay M. K. (2020), "Internet of things and data mining: An application oriented survey", *Journal of King Saud University - Computer and Information Sciences*, The Authors, No. xxxx, doi: 10.1016/j.jksuci.2020.07.002.

Tang P., Qiu W., Huang Z., Lian H. and Liu G. (2020), "Detection of SQL injection based on artificial neural network", *Knowledge-Based Systems*, Vol. 190, p. 105528, doi: 10.1016/j.knosys.2020.105528.

Tawalbeh L., Muheidat F., Tawalbeh M., Quwaider M. and Abd El-Latif A. A. (2022), "Edge enabled IoT system model for secure healthcare", *Measurement*, Vol. 191, p. 110792, doi: https://doi.org/10.1016/j.mea-surement.2022.110792.

Usha B. A., Sangeetha K. N., Suchit T. E., Shyam A. and Suryanarayanan A. (2020), "Comprehensive Review of Smart Cities using IOT", *2020 8th International Conference on Reliability, Infocom Techn-ologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 367–371, doi: 10.1109/ICRITO48877.2020.9197792.

Uy N. Q. and Nam V. H. (2019), "A comparison of AMQP and MQTT protocols for Internet of Things", *Proceedings - 2019 6th NAFOSTED Conference on Information and Computer Science, NICS 2019*, IEEE, pp. 292–297, doi: 10.1109/NICS48868.2019.9023812.

Wei Y., Chow K.-P. and Yiu S.-M. (2021), "Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation", *Forensic Science International: Digital Investigation*, Vol. 38, p. 301126, doi: https://doi.org/1-0.1016/j.fsidi.2021.301126.

Xu J., Gu B. and Tian G. (2022), "Review of agricultural IoT technology", *Artificial Intelligence in Agriculture*, Vol. 6, pp. 10–22, doi: https://doi.org/10.1016/j.aiia.2022.01.-001.

Yousefi A. and Jameii S. M. (2017), "Improving the security of internet of things using encryption algorithms", *2017 International Conference on IoT and Application (ICIOT)*, pp. 1–5, doi: 10.1109/ICIOTA.2017.8073627.

Yue Q. (2021), "Research on Smart City Development and Internet of Things Industry Innovation in the 'Internet +' Era", *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 28–31, doi: 10.1109/ICIRC-A51532.2021.9545028.

Zimmermann T., Lanfer E. and Aschenbruck N.

(2022), “Developing a Scalable Network of High-Interaction Threat Intelligence Sensors for IoT Security”, *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, pp. 251–253, doi: 10.1109/LCN53696.2022.9843744.

Zourmand A., Kun Hing A. L., Wai Hung C. and AbdulRehman M. (2019), “Internet of Things (IoT) using LoRa technology”, *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, pp. 324–330, doi: 10.1109/I2CA-CIS.2019.8825008.

Zrelli A., Nakkach C. and Ezzedine T. (2022), “Cyber-Security for IoT Applications based on ANN Algorithm”, *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–5, doi: 10.1109/ISNCC55209.2022.9851715.

Authors

Joshua Kweku Aidoo is a PhD Candidate in the Computer Science and Engineering Department at the University of Mines and Technology, Tarkwa, Ghana. He holds a Bachelor's degree in Computer Science from the Ghana Institute of Management and Public Administration. His research interests include the Internet of Things, Cyber Security and Machine Learning.

Solomon Nunoo is an Associate Professor in Electrical Engineering at the University of Mines and Technology, Tarkwa, Ghana. He holds a PhD in Electrical Engineering from Universiti Teknologi Malaysia, Skudai, an MPhil degree in Electrical and Electronic Engineering from the University of Mines and Technology (UMaT), Tarkwa, and a BSc degree in Electrical Engineering from Western University College of KNUST, now UMaT. His research interest is energy management, and signal processing for wireless communications with emphasis on adaptive filtering and compressive sampling.

Emmanuel Effah is a Senior Lecturer at the Department of Computer Science and Engineering, UMaT, Ghana. Effah received his PhD in Computer Science in the field of IoT from Gaston Berger University, Senegal His research interests include wireless sensor networks (WSNs), Agricultural-Internet-of-Things (Agri-IoT), IoT-based surveillance Systems, smart systems design technology, and machine learning.

William Akotam Agangiba holds a PhD in Computer Science and Engineering from the University of Mines and Technology (UMaT), Tarkwa, Ghana and MSc and BSc degrees in Information Systems and Technologies from Tver State Technical University, Tver, Russia. He is an Assistant Professor at the School of Information Technology, University of Cincinnati, USA. He has several publications in international journals and conferences to his credit. His research interests are Data Analytics, Expert Systems and Logics (Fuzzy Logic, Propositional Logic and First Order Logic). He is a Member of the Institute of Electrical and Electronics Engineering (IEEE) and a Professional Member of the Institution of Engineering and Technology (IET). He is also a member of the International Association of Engineers.