Introduction

The integration of Internet of Things (IoT) technology in agriculture or *smart farming* is transforming the traditional farming practices. IoT refers to the network of interconnected sensors and devices that collect and exchange data over the internet thus enabling the real-time monitoring and control [1]. In agriculture this will mean that embedding farms with sensors for the soil moisture, climate, livestock trackers and automation systems to optimize the operations. These advancements will promise to enhance the productivity and resource the efficiency. For example the precision agriculture using IoT has shown improvements in the crop yields and also reduced the resource wastage [8]. This report will present a detailed network design for a smart farm scenario. The design is developed using the GNS3 network simulator. The aim of it is to demonstrate how a robust network infrastructure can support IoT devices on a farm, ensuring reliable connectivity and security for critical agricultural data.

Research on IoT in Agriculture

IoT and its Role in Modern Agriculture

IoT (Internet of Things) is a term used for the model where physical things and devices are mounted with computing and network connectivity, therefore, they can both send and receive data. This is possible with IoT in agriculture through the combination of devices and sensors that are installed together to form a so-called "smart" network that can work alone by collecting data and even manage the responses by itself [1]. Farming IoT devices include examples like soil moisture sensors, weather stations, GPS-connected farm machinery, livestock wearables, smart irrigation controllers, and IP cameras. Soil moisture probes, weather stations, GPS-enabled farm machinery, livestock wearables, smart irrigation controllers, and surveillance cameras are representative of the IoT devices used on farms.

The precision agriculture sector, which IoT technology supports, is a method that adjusts farming decisions according to very specific information. The use of sensors in the fields to determine soil conditions and plant health is enabling the irrigation and fertilization to be done in the best way for each crop zone [2]. IoT-based weather stations, moisture sensors provide automation of the irrigation systems. Thus, the crops are given water only at required times. Livestock sensors could also detect animal behavior and vital signs thus leading to better herd management and early disease diagnosis [2]. The coupling of these systems via farm networks enables operations like greenhouse climate control, automated feeding, and remote surveillance of fields.

Wireless Network Features and Constraints for IoT

A farm mostly has IoT devices that are connected wirelessly because it has to span wide areas outdoor without the need for extensive cabling. In agricultural IoT, various wireless technologies are typically used and most of them have different features and limitations. For example Wi-Fi is frequently used near farm buildings when data rate is high as For example streaming IP camera footage of a range

limited to a few hundred meters [8]. However, LoRaWAN is the one that guarantees the long-distance and low power connection which can cover several kilometers, and it is the best choice for a large number of sensors distributed in a wide area field [8].

Range and coverage are of utmost significance during the installation of wireless networks within a farm. The open-field settings allow for signals to propagate, but objects like trees, hills, or greenhouses could attenuate wireless signals. Far-off farms usually have poor internet backhaul connections because infrastructure is limited [4]. Even in the local scenario, physical barriers like crop canopies or metal walls could distort Wi-Fi signals [4]. This mirrors the need for accurate antenna placement or the employment of technologies such as LoRa or external high-gain antennas capable of penetrating obstacles. Bandwidth needs range from low, where small telemetry packets are all that simple sensors send, to significantly higher throughput for video streams or heavy telemetries such as drone data. Wireless networks need to be designed to handle the peak data rates and latency-sensitive applications.

Another constraint is power. Many IoT sensors run on battery or solar power in the field. Protocols like LoRaWAN and Zigbee are optimized for low energy usage, while a Wi-Fi can be power-hungry. In all cases, reliability is crucial. Farmers depend on these networks for timely alerts (e.g., a greenhouse temperature spike), so the network must be resilient to outages. Strategies such as using redundant communication paths or edge computing can reduce the connectivity issues [4].

Security Concerns and Vulnerabilities in IoT Network

Many IoT devices have limited processing power and also lack the robust security controls. It has been shown that security measures are often lagging behind the rapid deployment of IoT gadgets. The reason is that many devices cannot easily receive the firmware updates/patches which causes persistent vulnerabilities [5]. For example a vulnerable sensor or camera could be compromised and used to infiltrate the broader network or leak sensitive data such as farm operational data or video feeds.

Data security is an important concern in the smart agriculture because of the volume and value of data collected from sensors and cameras. Making sure the privacy and integrity and secure transmission of this data is important so as to prevent the unauthorized access and breaches [8]. Key security considerations include the encryption of data communication e.g., using WPA2/WPA3 for Wi-Fi networks, or AES encryption in Zigbee/LoRaWAN, authentication of devices to prevent spoofing, and network access control. To handle these risks, modern network design principles recommend segmenting IoT devices onto separate network segments or VLANs isolated from the core business network [7].

Commercial and Environmental Impacts of IoT Adoption

Investing in IoT technology in agriculture has the commercial benefits and environmental implications. From a business standpoint the data-driven approach of IoT can greatly improve the operational efficiency and crop yield. By applying water and fertilizer and pesticides only as needed and in precise amounts, the farmers can reduce the waste and input costs while maintaining or improving output.

Traditional farming often suffers from inefficiencies and studies indicate that roughly 30% of the irrigation water is lost because of evaporated or not using it and up to 50% of the fertilizers ends up polluting the waterways rather than aiding crops [8]. Such waste directly erodes profitability and harms the environment through water scarcity and pollution. IoT-based solutions directly address these issues, for example smart irrigation systems use the soil moisture sensor data to irrigate only when and where necessary, preventing overwatering.

IoT can lower the labor and operating costs. Automation like autonomous tractors can reduc the manual workload. Energy savings are realized by optimizing pump and equipment usage. Even though implementing IoT infrastructure can require a high amount of upfront investment the long-term returns justify the cost. In many cases, farmers see a return on investment within just 1–3 years due to the combined savings from water, energy, and labor, coupled with higher revenues from better yields [9]. Additionally, external factors like government incentives for precision agriculture and sustainability initiatives can subsidize the adoption of IoT, further improving the commercial case [9].

Network Design and Implementation

Smart Farm Scenario Overview and Requirements

The network is designed for a diversified farm that includes the market garden with greenhouses, a pick-your-own(PYO) field area with a kiosk, a farm shop, a cafe and office facilities based on our given scenario. All these are located on the same site of almost 5 hectares with the main buildings clustered around a central yard of around 1 hectare. The networks support a variety of connected devices:

- **Office and Management:** Desktop PCs for staff. Approximately 4 in a general office and 1 in the manager's office and networked printers.
- **Farm Shop:** Four point-of-sale (POS) terminals (cash register systems) and an integrated scale/label printer and several smart refrigerators/freezers that report temperature data online.
- **Café:** Two POS terminals in the café and maybe tablets or devices in the kitchen area.
- **Greenhouses:** Environmental control systems and IP cameras for monitoring.
- **PYO Field Kiosk:** A scale and ticket printer at the kiosk where visitors weigh their picked produce.
- **Security Cameras:** Several surveillance cameras around the premises which stream video to a storage server or cloud.
- **Internet Connectivity:** The farm is in a semi urban area with the grid power and a broadband internet connection. Internet is required for functions like cloud backups, remote monitoring and electronic payment processing.

From these requirements, it's clear the network must handle both wired **and** wireless connections.

Network Topology and VLAN Segmentation

A segmented star topology was chosen which is centered around the core switch in the main building. The high-level topology is as follows:

- A single edge router connects the farm's network to the Internet This router serves as the gateway for all internal subnets.
- The router connects to a central switch that distributes connections to different areas like office, shop, greenhouse etc. Since multiple network segments are needed, VLANs are configured on this switch to logically separate the traffic types.
- VLAN 10 – Office Network: for office PCs and printers (administrative network). This VLAN holds the sensitive business data and is isolated from IoT devices.
- VLAN 20 – Point of Sale Network: for all payment terminals and shop/café devices. These are segregated to protect financial transactions (and could be subject to PCI-DSS security standards).
- VLAN 30 – IoT Sensors & Devices: for greenhouse sensors, environmental controllers, freezer monitors, and IP cameras. This network is kept separate to contain the potential security issues from IoT devices and to prevent their traffic from overwhelming other systems.
- VLAN 40 – Guest/Customer Wi-Fi (optional): if the farm offers public Wi-Fi that would be on its own VLAN with internet-only access.

Each VLAN corresponds to a separate IP subnet. For example we use private IPv4 addressing:

- **VLAN 10 (Office):** 192.168.10.0/24 (gateway 192.168.10.1)
- **VLAN 20 (PoS):** 192.168.20.0/24 (gateway 192.168.20.1)
- **VLAN 30 (IoT):** 192.168.30.0/24 (gateway 192.168.30.1)
- **VLAN 40 (Guest):** 192.168.40.0/24 (gateway 192.168.40.1)

Using VLANs creates isolated broadcast domains and security zones within the farm's network. For example, a broadcast storm or malware outbreak in the IoT network (VLAN 30) will not directly reach the office network (VLAN 10). Inter-VLAN traffic is routed through the router, which can enforce access control between segments. This segmentation aligns with best practices to limit the attack surface available to an adversary [7]. In implementation, the main switch will have ports assigned to the appropriate VLAN for each connected device A trunk link carries multiple VLANs between the core switch and the router, allowing the router to perform inter-VLAN routing.

Wireless integration: The greenhouses and the PYO kiosk require the wireless connectivity. A wireless access point (AP) is deployed to cover the greenhouse area, configured to serve the IoT. Modern APs can map different SSIDs to VLANs for example an SSID "FarmIoT" for sensors mapped to VLAN 30. This ensures that even though sensors connect wirelessly, their traffic is tagged and isolated like wired IoT devices. If needed, another SSID "FarmShop" on the AP could be mapped to VLAN 20 for any wireless

POS devices. All APs then link back to the wired over 802.1Q trunk links or dedicated VLAN access ports as appropriate.

GNS3 Implementation Steps

The network was built and simulated in GNS3. The following steps were carried out to implement the design:

1. **Device setup in GNS3:** A new GNS3 project was created and a virtual router, switch, and multiple virtual PCs (VPCs) were added to represent the network components. For the router, a Cisco IOS image provided routing functionality. A GNS3 Ethernet switch with VLAN support was used as the core switch. Each VPC node simulated an end device To simulate internet connectivity the GNS3 Cloud/NAT node was connected to the router's WAN interface.
2. **Switch configuration (VLANs):** On the virtual switch, VLANs were defined corresponding to the design. This involved using the switch's CLI to create VLAN 10, 20, 30 and assigning switch ports to the appropriate VLAN.
3. **Router configuration (routing and DHCP):** On the router, the interface connecting to the switch was configured for *802.1Q trunking* with subinterfaces for each VLAN. For example:
    - Interface Fa0/0.10 was created for VLAN 10, with encapsulation dot1Q 10 and IP address 192.168.10.1/24 (gateway for the office network).
    - Interface Fa0/0.20 for VLAN 20 with IP 192.168.20.1/24.
    - Interface Fa0/0.30 for VLAN 30 with IP 192.168.30.1/24 (and similarly Fa0/0.40 if applicable).

These subinterfaces act as default gateways for their respective VLANs, enabling inter-VLAN routing. The router's second physical interface was connected to the "Internet" node and given an IP configuration (or obtained one via DHCP from the NAT cloud) to simulate an ISP link.

Next, DHCP pools were configured on the router for each internal subnet. This meant setting up a DHCP scope for 192.168.10.0/24 (with default gateway 192.168.10.1) for VLAN 10 and similarly for VLAN 20 and 30. As a result any of the device connecting to the network in those VLANs will automatically receive an IP address, the correct subnet mask, the gateway and the DNS server from the router. This simplifies host configuration.

The router was also configured with Network Address Translation (NAT) to allow all these internal subnets to access the internet via the router's single WAN link. This allowed devices on the farm to share the one public IP on the router when communicating outbound. **Wireless network simulation:** While GNS3 cannot simulate wireless signal propagation, we modeled the presence of wireless segments by connecting devices to the appropriate VLANs as if through an access point.

Security configuration: Several security measures were implemented in the network configuration:

- **Network segmentation and ACLs:** The VLAN structure itself is a security measure. Also on the router, an access control list was applied to restrict IoT network traffic.

- **Device security:** We documented the use of strong wireless security (WPA2/WPA3) for the Wi-Fi networks to prevent unauthorized access.

4. **Device addressing and configuration:** With the network infrastructure in place, all the end devices in the simulation were set to use DHCP. Each VPC, upon startup, issued a DHCP request and obtained an appropriate IP address We verified these addresses and their default gateways. Testing and Simulation

Connectivity tests:

- **Within VLAN:** Devices on the same VLAN were tested to ensure they could reach each other. For example, one office PC pinged another office PC on VLAN 10; similarly, two sensor nodes on VLAN 30 exchanged pings. These tests were successful and confirming that intra-VLAN switching was correctly configured and that no unintended isolation existed within each group.
- **Inter-VLAN (allowed traffic):** We tested cross VLAN communication where it was intended to be allowed. For example an office PC in VLAN 10 pinged the IP address of the farm's environmental server Also, a POS terminal in VLAN 20 was able to ping the router gateways showing that the router was routing properly.
- **Internet access:** We pinged an external IP from a sample device in each VLAN. The replies confirmed that devices could reach the internet via the router's NAT. We also tested DNS resolution by pinging a domain name from a PC and confirming the DNS server (8.8.8.8 configured via DHCP) was reachable and working.

DHCP checks: All client devices were observed to receive appropriate network configurations from the router's DHCP service. Using the show ip dhcp binding command on the router, we saw leases for each MAC address in the correct pools.

VLAN isolation and security: An important part of testing was to ensure that the VLAN segmentation and ACLs were enforcing the intended isolation:

- From a device in the IoT VLAN (greenhouse sensor node), we attempted to ping an office PC in VLAN 10 and a POS terminal in VLAN 20. As expected, these pings failed or timed out, indicating that the IoT device could not reach into those networks. This confirms that the ACL blocking IoT-to-office or POS traffic was effective.
- From an office PC we attempted to reach a sensor device or the greenhouse controller. This was permitted in our design (since the ACL was unidirectional) and yes the office PC could ping the sensor's IP successfully. Thus, authorized access from the trusted network to the IoT network was working likr intended.
- We also confirmed that the guest network had no access to internal resources by trying to ping internal addresses from a "guest" VPC. Those attempts were blocked ensuring that any guest Wi-Fi users would be isolated to internet-only usage.

Analysis and Evaluation

Analysis

The smart farm network design meets the key requirements of supporting diverse IoT and business devices with reliability and security. The segmented architecture proved effective in handling the mix of traffic. One major strength is the use of VLAN segmentation, which achieved both performance and security benefits. By splitting the network, broadcast traffic is confined within each VLAN, reducing unnecessary load on devices elsewhere.

Another strength is the network's scalability and flexibility. The star topology with a central switch allows easy expansion: new devices or even new VLANs can be added with minimal disruption. The IP addressing scheme provides ample room for growth in each subnet (up to 254 devices each, far more than the current needs). The use of DHCP means adding or replacing devices is plug-and-play, simplifying network management for the farm staff. The design also seamlessly integrates wired and wireless segments under the same unified infrastructure.

The network is also well-suited to support the farm's IoT applications. The bandwidth provided by wired Gigabit Ethernet and modern Wi-Fi standards is sufficient for typical IoT data and even multiple HD camera streams. Latency within the LAN is low, which is important for any control =The design centralizes routing and management at the router, simplifying the topology and ensuring that all inter-VLAN traffic can be monitored or filtered in one place.

Areas for Improvement

Redundancy: The current design has single points of failure in the router and main switch. Implementing a backup switch, standby router or secondary ISP (e.g., 4G/LTE) would enhance the reliability and ensuring critical systems remain operational during outages.

Security Enhancements: Adding a firewall appliance for deep packet inspection and Network Access Control (NAC) for authentication and segmenting the IoT devices into separate VLANs would further strengthen protection.

Monitoring & Management: A centralized network monitoring solution could track device status, bandwidth usage, and anomalies, reducing manual checks. An IoT dashboard would provide real-time insights and alerting farmers to sensor failures or connectivity issues.

Bandwidth Management: Link aggregation (combining switch ports) and upgrading to 10 Gbps fiber may be needed to prevent congestion from high-bandwidth devices like HD cameras, video calls.

Future-Proofing: Enabling IPv6 would accommodate the growing number of IPv6-capable IoT devices.

Conclusion

In analyzing the solution, we found that the network achieves a strong balance of performance and security for the smart farm scenario. Its strengths lie in segmentation, scalability, and alignment with

best practices (such as limiting the attack surface via network isolation [7] and using automation like DHCP for easy management). The network enables the farm to harness IoT capabilities – from automated greenhouse management to real-time inventory tracking which is translating into commercial gains and environmental benefits

References

[1] Omnitron Systems. *"IoT in Smart Agriculture Networks."* Omnitron Blog, 2023. Overview of IoT and its applications in agriculture, including definitions and examples of smart farming use cases.

[2] Omnitron Systems. *"What is IoT, and How Does it Fit into Agriculture?"* (Section in *IoT in Smart Agriculture Networks*). Explains the concept of IoT in agriculture and discusses various sensor and device applications on farms.

[3] Hardesty, George. *"Agriculture IoT: Wireless Technologies for Ag Internet of Things."* Data-Alliance Blog, Nov. 5, 2023. Details common wireless technologies (Wi-Fi, Bluetooth, LoRaWAN, NB-IoT, Zigbee, etc.) used for IoT in agriculture and their characteristics (range, power, bandwidth).

[4] Owade, Atula. *"Three major obstacles for IoTs in agriculture."* CGIAR Big Data in Agriculture Blog, Oct. 11, 2018. Describes challenges such as poor connectivity in rural farms and how innovative solutions (e.g., TV white spaces, drones) can overcome them.

[5] Kim, Hee-Hyun, and Jinho Yoo. *"Analysis of Security Vulnerabilities for IoT Devices."* **Journal of Information Processing Systems**, vol. 18, no. 4, 2022, pp. 489–499. Academic study highlighting common IoT device security issues (e.g., lack of timely patching) and the growing number of vulnerabilities as IoT expands.

[6] Data Alliance. *"Challenges and Future Outlook"* (section of *Agriculture IoT: Wireless Technologies for Ag IoT*). Emphasizes the importance of data security in smart agriculture, noting the need to ensure privacy, integrity, and protection of IoT-collected data.

[7] Infosec Institute. *"VLAN Network Segmentation and Security."* (Olzak, Tom, 2021). Explains VLAN segmentation fundamentals and notes that proper network segmentation can reduce attack surfaces and limit unauthorized access in networks.

[8] Hashstudioz (Shivam Rathore). *"From Waste to Wealth: How IoT Sensors Help Farmers Save Water & Fertilizer?"* Feb. 16, 2024. Provides statistics on resource waste in traditional farming and improvements achieved with IoT sensors (e.g., 15% yield increase, 20% less water usage).

[9] Nichols, Justin. *"The economic benefits of IoT-driven smart irrigation systems."* Smart Water Magazine, Aug. 9, 2024. Discusses cost savings and return on investment for IoT-based irrigation, noting that farmers often see ROI within 1–3 years due to water savings, labor reduction, and yield gains.