KN University Network Design

COIT13236 – Cyber Security Project

Document Title	IoT Integration Plan
Document Type	Technical Artefact
Document Status	Completed
Document Version	V_2.01
Group No	02
File name	group02-IoT-integration-plan.docx
Created By	Narayan Parajuli (12144248)
Create Date	01/08/2024
Reviewed By	Krishan Himesh Abeyrathne (12217274)
Reviewed Date	15/08/2024

Table of Contents

IoT Integration Plan

IoT Integration Plan:

Integrate IoT gadgets to upgrade student and campus experiences while staying aware of network security and execution. Exhaustive Coordination of IoT gadgets across college workplaces, including study halls, homes, libraries, sporting facilities, and authoritative buildings.

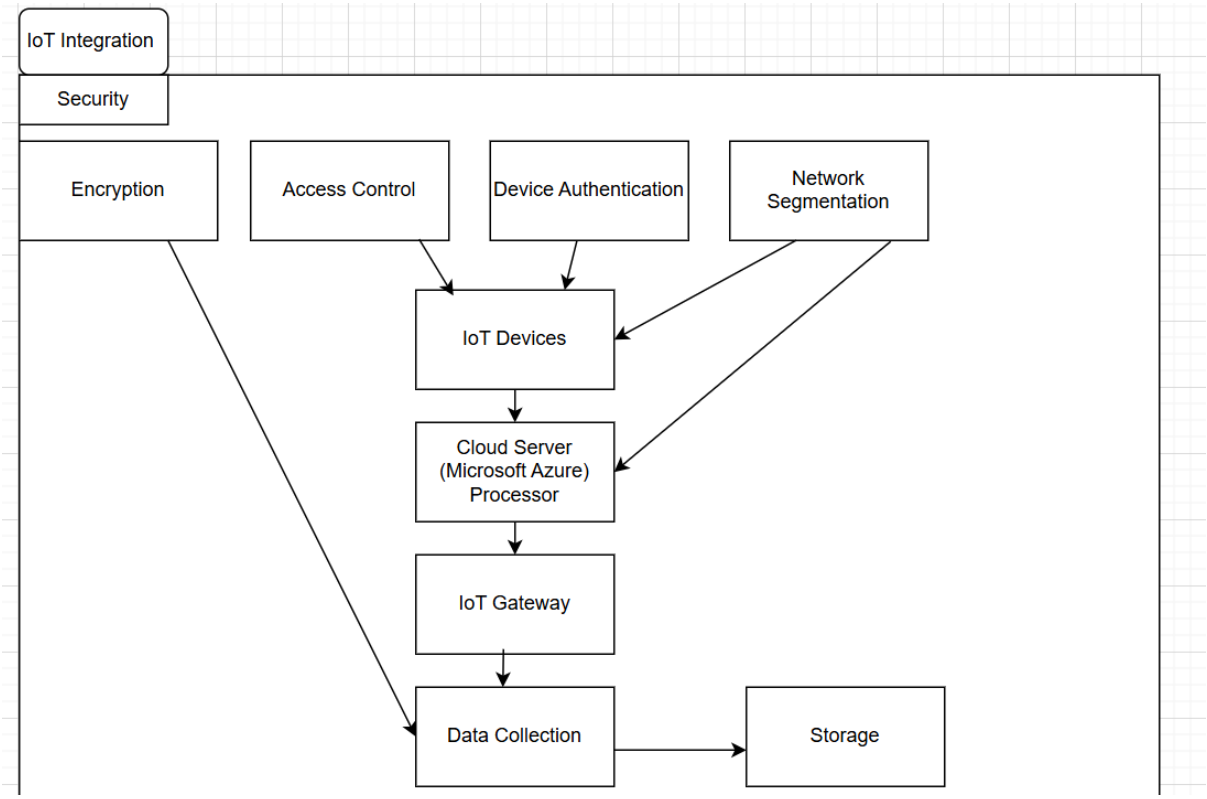

Fig: IoT Integration Plan

The security architecture for consolidating Internet of Things (IoT) gadgets into KN University's network is shown in the diagram. Access control to ensure that main approved clients can collaborate with the system, gadget verification to affirm that only authentic gadgets interface with the network, and encryption to shield information from unapproved access are safety efforts for KN University IoT integration. By disengaging IoT gadgets, network segmentation further develops security by decreasing the impact of expected interruptions. This multitude of steps cooperate to ensure the protected handling of the information created by IoT gadgets and their protected activity all through the campus.

The picture above basically shows how KN College utilizes segmentation, access control, validation, and encryption related to cloud computing and safe information storage to ensure the security and fitting administration of its IoT gadgets and the information they produce.

Components:

1. **IoT Device Types:**

   i. Smart Lighting: Computerized and energy-proficient lighting frameworks.

   ii. Natural Sensors: Temperature, humidity, and air quality sensors. Example: D23-NB NB-IoT Waterproof Temperature Sensor with cost $179

   iii. Smart Lock Frameworks: Access control for buildings and rooms. Example: Igloohome Bluetooth Smart Deadbolt 2S Dark Grey Airbnb with cost $279

   iv. Study hall management: Smart projectors, intuitive whiteboards, and attendance systems. Example: BenQ MX560 High Brightness High Contrast Projector with cost $649

2. **Network Division:**

   i. Dedicated IoT VLAN: By isolating IoT traffic from the main network and preventing potential attacks from spreading, KN University's advancement of a specific VLAN for IoT gadgets further develops security. By better controlling transfer speed, this segmentation guarantees that significant applications are not disturbed and augments execution. It likewise makes managing IoT gadgets simpler by empowering the utilization of customized approaches without obstructing other network segments.

   ii. Firewall Rules: Firewall rules are utilized at KN University to restrict collaboration, and lower security risks by forestalling communication between the IoT VLAN and significant network segments. By restricting the assault surface and allowing just fundamental communication and prohibiting superfluous protocols, these principles force severe security guidelines. To protect imperative network services, high level firewall runs likewise consider the checking and location of anomalous IoT traffic, the setting of cautions, and the restricting of suspicious movement.

3. **Information Collection and Management:**

   i. IoT Gateway: To guarantee that main the vital data is moved to the data centre or cloud, the KN University IoT gateway fills in as a solitary hub point for gathering data from different IoT gadgets. It does this by doing preliminary handling like filtering and conglomeration. Moreover, it changes over numerous communication protocols into a common format and use gadget authentication and encryption to defend data transmission.

ii. Data Storage: KN University stores IoT gadget information in protected, adaptable data sets that can oblige expanding information volumes. These data sets can be situated on-site or in the cloud. Encryption and access limitations are utilized to save information security and consistence; cloud administrations give additional safety efforts including computerized reinforcements. The tasks and decision-production of the university can then be advanced through analysis of the recorded information.

4. Safety measures:

i. Device Verification: To ensure that main approved gadgets associate with the network, authenticate and authorise IoT gadgets ahead of time. Lay out a registration strategy, track and oversee gadgets utilizing exceptional identifiers, and approve the authenticity of the gadgets with secure onboarding procedures like multi-factor or certificate-based authentication.

ii. Encryption: To stay away from unwanted access, encode data is moved between Internet of Things gadgets and network endpoints utilizing conventions like TLS. Solid algorithms like AES are utilized to encode information while it's being sent and ensure it encrypted the entire way through with the goal that main the planned recipient can decrypt it. Encryption principles frequently is refreshed to keep security and handle newfound blemishes.

5. Checking and Maintenance:

i. IoT Monitoring Apparatuses: High level monitoring tool, for example, Azure IoT Hub is introduced to watch out for the usefulness and general wellbeing of IoT gadgets all through the campus. This includes watching out for study hall the management frameworks, ecological sensors, smart locks, and smart lighting. This apparatus recognizes any issues from the get-go by giving constant information on gadget status, availability, and functional proficiency.

ii. Regular Updates: Lay out a timetable for upgrading the IoT gadgets' firmware and software that are utilized across the campus. To determine weaknesses and further develop usefulness, this interaction includes applying security refreshes, bug fixes, and execution upgrades. Test overhauls in a protected setting to forestall obstruction with fundamental college capabilities.

References

SANS Institute (2024) Network Security Policy. Available at: https://www.sans.org/security-resources/policies/network-security-policy (Accessed: 3 August 2024).