**IT 423 Project Two White Paper**

**IT-423 Computing as a Service**

**Tatiana Epps**

**October 27, 2024**

**Project Two White Paper**

**Introduction**

YODAE's commitment to enhancing education through technology has led to the development of innovative IoT devices designed to revolutionize the classroom experience. However, the integration of IoT devices into educational environments introduces new security challenges. This white paper aims to address these challenges by providing a comprehensive overview of YODAE's IoT devices, their potential use cases, and critical security considerations.

**Technology Overview**

**IoT Devices and Their Use Cases**

1. Voice-Activated Personal Assistants (VPAs): These devices offer hands-free access to information and classroom management tools. Teachers can use VPAs to set timers, check schedules, and control smart devices in the classroom. Students can use them for research and language learning.
2. IoT Whiteboards: These interactive whiteboards enable collaborative learning and engaging presentations. Teachers can share digital content, annotate documents, and conduct interactive quizzes. Students can participate in real-time discussions and problem-solving activities.

**IoT and Cloud Computing**

IoT devices generate vast amounts of data that are often stored and processed in the cloud. This integration with cloud computing offers scalability and accessibility but also introduces security risks. Data privacy, integrity, and confidentiality are paramount concerns when handling sensitive student and staff information.

**IoT Vulnerabilities and Risks**

IoT devices are susceptible to various security threats, including:

* Insecure Default Settings: Many devices ship with weak default passwords, making them easy targets for hackers.
* Lack of Patching: Outdated firmware and software can leave devices vulnerable to known exploits.
* Data Privacy Breaches: Sensitive information, such as student records and personal preferences, can be compromised if not protected adequately.
* Physical Security Risks: Devices can be physically tampered with or stolen, leading to data breaches and unauthorized access.

**IoT Architecture**

A typical IoT architecture consists of three layers:

* Device Layer: This layer comprises the physical IoT devices, such as sensors, actuators, and gateways.
* Network Layer: This layer facilitates communication between devices and the cloud. It involves protocols like Wi-Fi, Bluetooth, and cellular networks.
* Application Layer: This layer handles data processing, analytics, and user interfaces. It often leverages cloud-based services to provide insights and automation.

**Errors in IoT Design and Potential Solutions**

**YODAE IoT Classroom Design with Security Enhancements**

**A diagram of a diagram

Description automatically generated with medium confidence**

**Confidentiality:**

Error: Lack of encryption for data transmission and storage.

Solution: Implement strong encryption algorithms (e.g., AES-256) to protect sensitive data.

**Integrity:**

Error: Weak authentication mechanisms for device access.

Solution: Utilize robust authentication methods, such as multi-factor authentication and strong password policies.

**Availability:**

Error: Single points of failure in the network infrastructure.

Solution: Implement redundancy and failover mechanisms to ensure continuous operation.

**Ethical and Societal Implications**

The deployment of IoT devices in educational settings raises ethical concerns, such as:

* Student Privacy: Collecting and analyzing student data requires careful consideration of privacy rights and data minimization principles.
* Surveillance and Monitoring: The use of IoT devices for surveillance purposes can raise concerns about student autonomy and freedom.
* Digital Divide: Ensuring equitable access to technology is crucial to avoid exacerbating existing educational disparities.

**Conclusion**

By addressing these security challenges and ethical considerations, YODAE can ensure the safe and effective integration of IoT devices into K-12 classrooms. A well-designed and secure IoT architecture will empower educators and students while safeguarding sensitive information.

**Tatiana E. Epps**

**YODAE**

**Resources**

Top IoT security challenges and best practices. (2024, October 21). Balbix. <https://www.balbix.com/insights/addressing-iot-security-challenges/>

Kananda, V. (2024, August 7). Why you should use AES 256 encryption to secure your data. Progress Blogs. <https://www.progress.com/blogs/use-aes-256-encryption-secure-data>

LAN Switching with Redundant Links | NetworkAcademy.io. (n.d.). NetworkAcademy.io. <https://www.networkacademy.io/ccna/ethernet/an-switching-redundant-links>