A Lightweight and Adaptive Logging Architecture

Students :Diala Alazzeh-Jana Abdeen-Eyad Alssouqi
Supervised by: Prof. Mohammad Alnabhan,
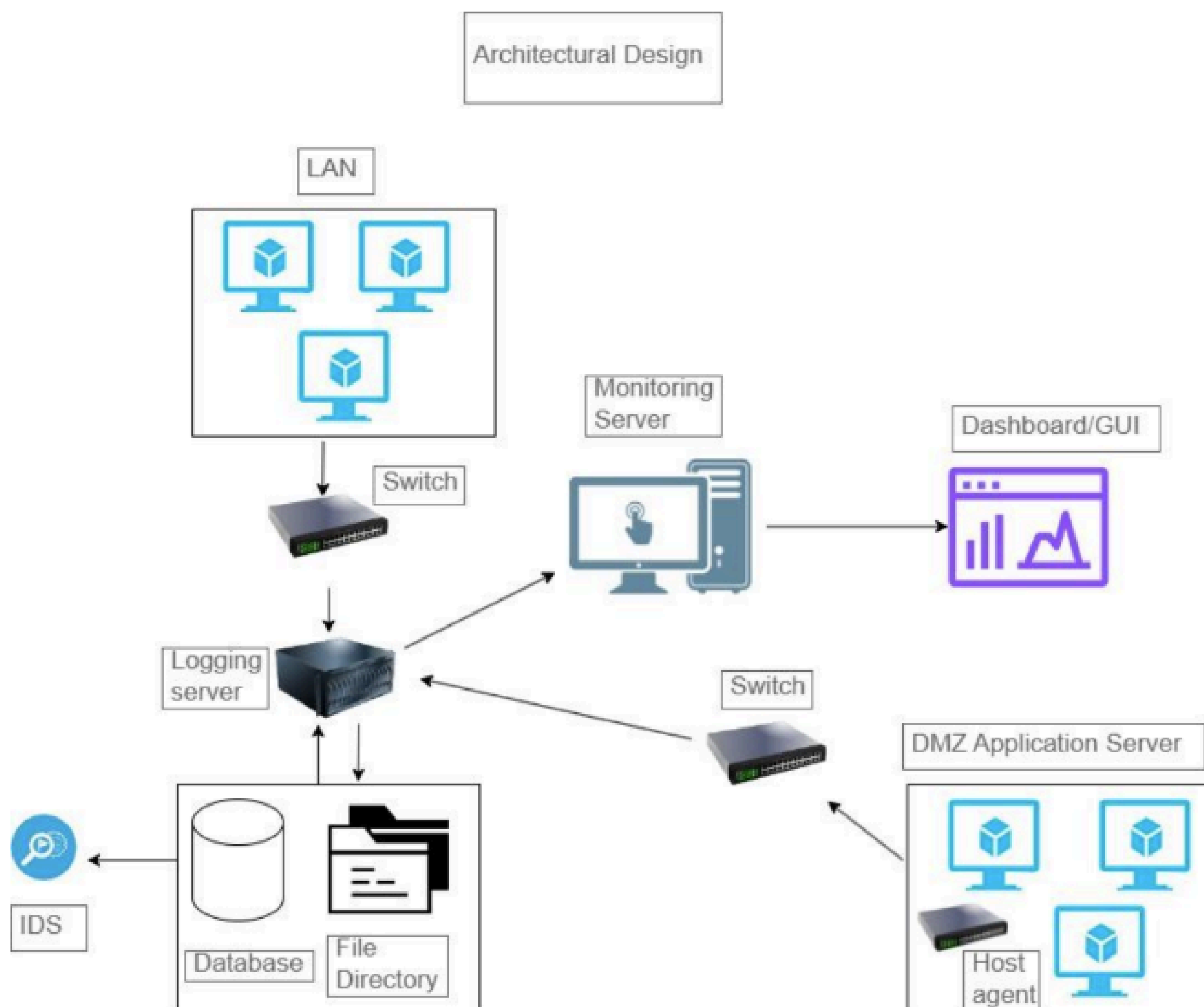Department of Cybersecurity

Princess Sumaya University for Technology
جامعــــة الأميـــرة سميّـة للتكنولوجيا

King Hussein School of Computing Sciences
كليـــة الملك الحسين لعلـــوم الحوسبــة

Abstract

Traditional logging systems are vulnerable to security threats, inconsistent formats, costly storage costs, and the destruction of crucial information. This project introduces a centralized, lightweight logging system that structures logs, filters key attributes, and integrates with an IDS for real-time threat detection. For organizations of all sizes, it presents an effective, scalable solution that minimizes complexity and strengthens security.

Architectural Design

Key Features
-Our system is integrated with an Intrusion Detection System(IDS) for enhanced monitoring.
-Logs are structured and filtered, to store only efficient attributes.
-Central server to store logs from different sources for unified and real-time analysis.

Project Goals
-Develop a scalable and lightweight centralized logging system for real time tracking.
-Design a flexible data model that simplifies log management across multiple organizational needs.
-Support security teams with a user-friendly interface and tools to detect threats efficiently.