THE ICT UNIVERSITY

P.O. Box 86236, Baton Rouge, LA 70879, USA
Phone: +1 225 612-4643 FAX: +1 225 612-6994
Email: admin@ictuniversity.edu.cm
Website: http://www.ictuniversity.edu.cm

COMPUTING IN SOCIETY

PROJECT FORM

GROUPE MEMBERS :

1. NGAMENI YOUDJEU ETHEL RYAN
2. FOTSO TALA LEO
3. NJOUONWET KAMSEU JAMAL
4. NOUPOUE DE CHAMAMBE C. AUDREY
5. DJAMA'A ELIMANE LY
6. YAN MIGUEL CHIBUEZE UMEJI
7. TATSINKAM KANTE
8. NGUEMDJOP NGUEJIP GADYEL

CLASS: ICT FACULTY LEVEL 1

DATE: 2 DEC 2025

COURSE FACILITATOR: DR. EBELLE

ACADEMIC YEAR 2025-2026

TABLE OF CONTENT

PROJECT WORK

TECHNOLOGY GOVERNANCE IN SUB SAHARA AFRICAN COUNTRY (RULES AND REGULATION)

Chapter 1: Objective

The main objective of this project is to design and implement a smart, automated attendance management system for students that ensures accuracy, security, and real-time monitoring. This system integrates multiple technologies—QR code scanning, geolocation (geofencing), and cloud-based data storage (Google Sheets)—to achieve a modern solution for classroom attendance.
Specifically, the system aims to:

1. **Automate Attendance Recording:**
    - Eliminate manual roll-call and paper-based attendance sheets.
    - Reduce human errors, save teacher time, and maintain accurate records.
2. **Ensure Student Presence:**
    - Use geofencing to verify that students are physically present in the classroom.
    - Prevent students from marking attendance when absent or using fake locations.
3. **Integrate QR Code Technology:**
    - Assign a unique QR code for each course.
    - Allow students to quickly and easily mark attendance with their smartphone.
    - Ensure authentication of each attendance action.
4. **Enable Real-Time Data Management:**
    - Send attendance data instantly to Google Sheets.
    - Allow teachers and administrators to monitor attendance in real-time.
    - Track late arrivals and early departures automatically.
5. **Monitor Continuous Presence:**
    - Track the student's location during the entire class period.
    - Automatically remove students who leave the geofence area for more than 15 minutes, ensuring fairness.

Chapter 2: Main Features

QR Code Scanning for Each Course

- Every course has a **unique QR code** generated by the teacher.
- Students scan the QR code using their smartphone to mark attendance.
- Ensures **quick, easy, and secure authentication** of students.

Geofence Verification (Location-Based Access)

- The app uses **GPS and geofencing technology** to verify the student's location.
- Students can only mark attendance if they are **inside the defined classroom area**.
- Prevents cheating or marking attendance from outside the classroom.

Automatic Attendance Logging

- Once verified, the student's information and timestamp are sent **directly to Google Sheets**.
- Allows **real-time attendance tracking** for teachers and administrators.
- Eliminates the need for manual entry and reduces errors.

Continuous Presence Monitoring

- The system continuously monitors the student's location during the class.
- If a student leaves the classroom area for more than **15 minutes**, their attendance is automatically removed.
- Encourages accountability and ensures **fair monitoring** of attendance.

Secure Login and Authentication

- Students must log in using **Firebase Authentication** or email login.
- Ensures that only **authorized students** can access the attendance system.
- Enhances **security and reliability** of attendance records.

Chapter 3: Required Materials

To develop and implement the Student Attendance System, several materials and technologies are required to ensure that the system functions efficiently, securely, and in real-time.

First, **smartphones with GPS and internet connectivity** are essential for students to scan QR codes and share their location with the system. These devices serve as the primary interface for students to interact with the app, allowing them to mark their attendance and be monitored during class.

Next, a **computer equipped with Android Studio or Flutter and python language** is necessary for developing the mobile application. Android Studio allows developers to create robust native Android apps, while Flutter provides a cross-platform solution that can run on both Android and iOS devices and python language will permit us to develop the backend of the application. These development environments include all the tools needed to design, code, test, and debug the application.

For secure authentication, the system uses **Firebase Authentication**, which allows students to log in safely using their email or Google account. This ensures that only authorized users can access the system, preventing unauthorized attendance marking.

The attendance data is stored and managed using the **Google Sheets API or in MySQL**, which provides a cloud-based solution for real-time data storage. As students check in or leave the class, the system updates the attendance records instantly, enabling teachers and administrators to monitor attendance remotely from any device.

Additionally, a **QR code generator** is required to create unique QR codes for each course. These QR codes act as the key for students to mark their attendance, ensuring that the system identifies each class session accurately.

Finally, the **Google Maps Geofencing API** is used to define classroom boundaries. This technology allows the app to check whether a student is within the designated area before marking attendance. It is also responsible for monitoring continuous presence during class hours and triggering automatic removal from the attendance list if a student leaves for more than 15 minutes.

Together, these materials and technologies form a complete ecosystem that ensures the Student Attendance System is accurate, secure, and easy to use.

Each component plays a crucial role, from device hardware to cloud services, making the project reliable and efficient for modern educational environments.

Chapter 4: How it works

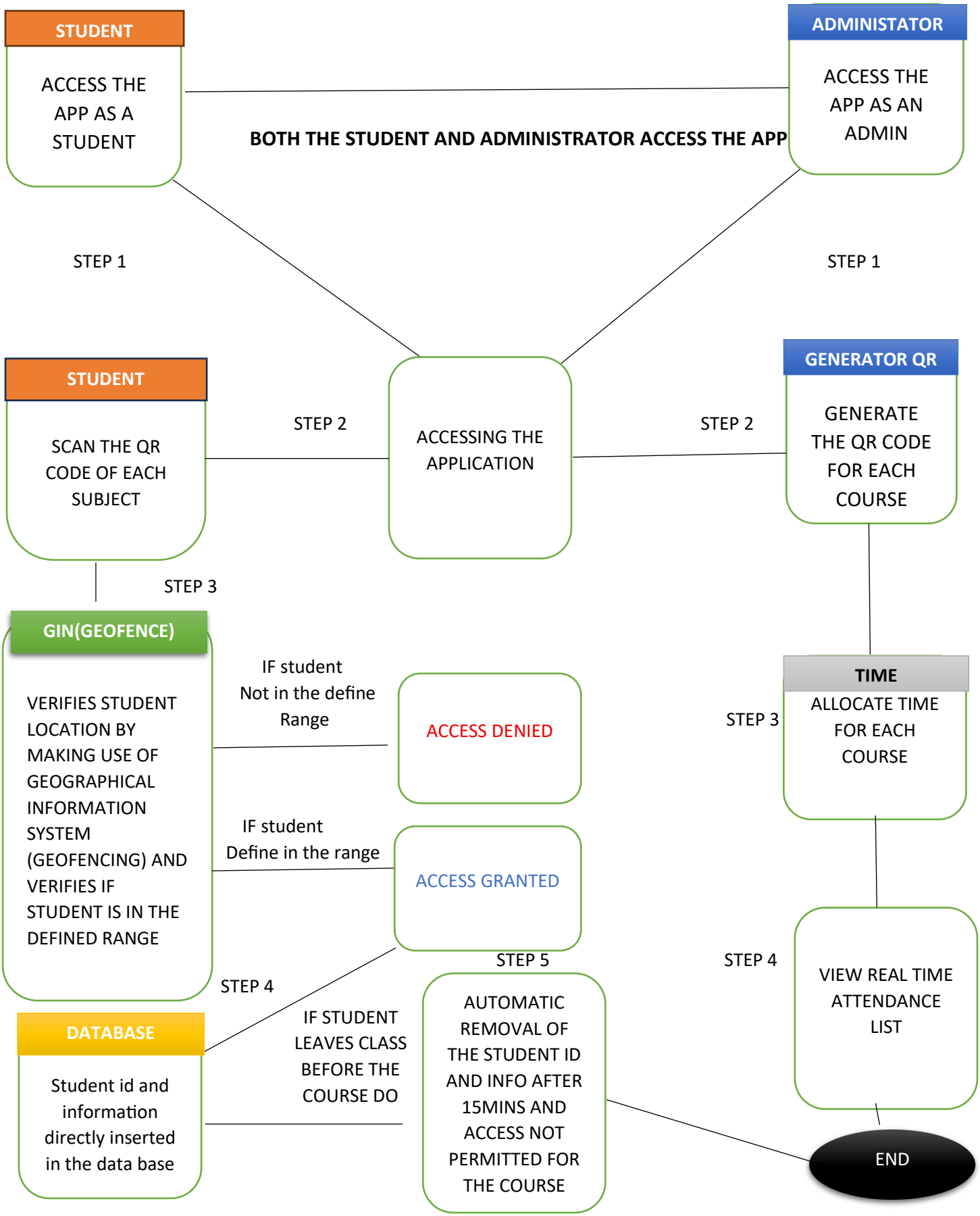
The Student Attendance System operates as an **integrated flow of actions** between the student, the mobile application, and the cloud system. When a student enters the classroom, the system first identifies the course session through a **unique QR code**, which acts as a digital key.

Once the QR code is scanned, the system **validates the student's presence within a defined boundary** using geolocation. If the student is inside the classroom area, the system registers the attendance and updates the **centralized database** in real-time.

Throughout the session, the system continues to **monitor the student's presence**, ensuring continuous compliance with the classroom rules. If the student exits the designated area for a defined period, the system automatically adjusts the attendance status, reflecting absence.

The system abstracts all complex operations into **three main layers**: the student interface, the validation and monitoring logic, and the centralized data storage. These layers work in harmony to provide a **seamless, automated, and secure attendance management experience** for both students and educators.

CHAPTER 5: UML DIAGRAM QR VEFICATION CODE PROCEDURE



Chapter 7: Summary / Conclusion

In summary, this project demonstrates how **technology can streamline educational processes**, enhance accountability, and create a more efficient and reliable system for both students and educators. It provides a **scalable, flexible, and user-friendly platform** that can be adapted for multiple courses, classrooms, and even campuses, making it a **valuable tool for modern educational environments**.

TECHNOLOGY GOVERNANCE IN THE SUB-SAHARAN COUNTRY

Chapter 1: What is Technology governance?

Technology governance means *creating and enforcing rules* that guide how digital technologies should be used in a country.
It tells people, companies, and the government what they must do, can do, and must not do when using technology.

You can think of it as instructions for managing technology, including:

1. **Protect people's data** –
   Make sure personal information is collected, stored, and shared safely.
2. **Stop cybercrimes** –
   Create laws to punish hacking, online fraud, scams, and harmful digital behavior.
3. **Regulate telecom networks** –
   Set rules for mobile companies, internet providers, SIM registration, and network quality.
4. **Guide digital businesses** –
   Tell apps, websites, fintechs, and platforms how to operate legally and protect users.
5. **Ensure digital safety** –
   Make rules for online content, child protection, and misinformation control.
6. **Support innovation** –
   Create policies that help digital startups grow while staying safe and legal.

Chapter 2: Rules and Regulation in the sub sahara countries

A. Nigeria

Main Laws

1. Nigeria Data Protection Act (2023)
2. Cybercrimes (Prohibition & Prevention) Act (2015)
3. Nigerian Communications Act – telecom regulation
4. Digital Financial Services Guidelines – for fintech

Main Regulators

- Nigeria Data Protection Commission (NDPC)
- Nigerian Communications Commission (NCC)
- Central Bank of Nigeria (CBN) for digital finance
- NITDA for ICT policy

How it works

- Any company collecting personal data must follow strict privacy rules (consent, breach notification, etc.).
- NDPC can investigate and fine companies for data misuse.
- Cybercrime law allows the government to arrest hackers, scammers, and fraudsters.
- Telecom rules ensure SIM registration, quality of service and fair competition.
- Fintechs must get CBN approval before offering digital payments.

B. Kenya

Main Laws

1. Data Protection Act, 2019
2. Computer Misuse and Cybercrimes Act, 2018
3. Kenya Information and Communications Act (KICA)
4. National ICT Policy (2020)

Main Regulators

- Office of the Data Protection Commissioner (ODPC)
- Communications Authority of Kenya (CAK)
- National Kenya Computer Incident Response Team (KE-CIRT)

How it works

- Organizations must register as data controllers/processors.
- ODPC regularly audits companies and orders them to stop illegal data collection.
- Cybercrime law covers mobile money fraud, online harassment, and hacking.
- Kenya is very advanced in digital ID, mobile money oversight, and ICT innovation regulation.
- Telecoms are strictly supervised to protect consumers and ensure fair pricing.

C. South Africa

Main Laws

1. POPIA (Protection of Personal Information Act)
2. Electronic Communications and Transactions Act
3. Cybercrimes Act (2021)
4. National Integrated ICT Policy

Main Regulators

- Information Regulator (IRSA)
- Independent Communications Authority of South Africa (ICASA)
- Cyber Response Committee

How it works

- POPIA is one of the strongest privacy laws in Africa — companies must prove their compliance.
- The regulator can issue investigations, compliance orders, and penalties.
- Cybercrimes Act criminalizes unlawful access, fake messages, and harmful digital content.
- Telecom operators must follow licensing, spectrum allocation, and service-quality rules.
- South Africa has strong digital consumer protection rules.

GH D. Ghana

Main Laws

1. Data Protection Act, 2012 (Act 843)
2. Electronic Transactions Act (2008)
3. Cybersecurity Act (2020)
4. National Communications Authority Regulations

Main Regulators

- Data Protection Commission (DPC)
- National Communications Authority (NCA)
- Ghana Cyber Security Authority

How it works

- Organizations must register with the Data Protection Commission.
- The Cybersecurity Act sets up national teams to handle cyber incidents.
- Online platforms must follow rules for security, consumer protection, and lawful content.
- Telecom rules focus on SIM registration, mobile money security, and network quality.
- Ghana conducts nationwide cybersecurity awareness and monitoring.

Common Patterns Across Sub-Saharan Africa

Strengths

- Most countries now have **modern data privacy laws**.
- Cybercrime acts exist almost everywhere.
- Governments are investing in national digital identity systems.
- ICT regulators actively monitor telecom operators.

Challenges

- Enforcement is sometimes slow due to limited resources.
- Cross-border data transfer rules are not harmonized.
- Many small businesses do not understand compliance requirements.
- Digital literacy gaps create risks for citizens.

CONCLUSION

Technology governance in Sub-Saharan Africa has made significant progress over the past decade, with most countries adopting modern laws on data protection, cybersecurity, and digital communications. Nigeria, Kenya, South Africa and Ghana each provide strong examples of how governments are building legal and institutional frameworks to protect personal data, fight cybercrime, regulate telecoms, and guide the growth of digital markets.

Although enforcement capacity and regional harmonization still need improvement, these countries show a clear commitment to creating safer and more reliable digital ecosystems. As digital technologies become central to education, finance, health, and governance, strong regulatory systems are essential to protect citizens' rights while encouraging innovation.

Overall, Sub-Saharan Africa is steadily moving toward a more structured, secure, and coordinated digital future—one where technology is governed responsibly to support development, trust, and economic growth.