**CHAPTER 2**

**LITERATURE SURVEY**

**CHAPTER 2**

**LITERATURE SURVEY**

In this section, we present a brief overview of the related research works and discuss the key findings that support the development of our project **EDUCARE**. The reviewed literature focuses on various attendance management systems, including **manual, RFID-based, biometric, and facial recognition systems**, highlighting their advantages, limitations, and challenges in ensuring accuracy, efficiency, and data security.

Berta et al. [1] “Challenges of Manual Attendance Systems and the Need for Automation” Discussed the challenges of **manual attendance systems**, emphasizing issues like **time consumption, human error, and data inaccuracy.** The study suggested the need for **automating attendance management** to improve **efficiency, accuracy, and faster attendance marking.** The use of traditional methods like roll calls or paper-based registers was proven to be inefficient in large-scale educational environments. However, the study did not provide any automated solution to the problem.

Arab et al. [2] “Image Encryption Using Chaos Sequence and AES for Secure Data Storage” proposed an **image encryption algorithm** based on the combination of the **chaos sequence and AES encryption** to ensure high-level **data security**. The encryption key was generated using the Arnold chaos sequence, ensuring **data confidentiality**. However, the method lacked **real-time attendance marking** and required **manual data entry,** reducing overall system efficiency.

Ele et al. [3] “A Cryptographic Framework for Securing Attendance Management Systems” introduced a **cryptographic system framework** that ensures **data integrity and security** in attendance management systems. The proposed system reduced the chances of data manipulation by utilizing a strong **encryption mechanism**. However, the major limitation was the **complex coding structure** and **long processing time**, which prevented **real-time attendance management**. Additionally, the system did not focus on automating attendance marking, limiting its practical application in educational institutions.

Waters et al. [4]” Biometric Fingerprint-Based Attendance System: Challenges and Limitations” developed a **biometric fingerprint-based attendance system** aimed at minimizing **proxy attendance** and ensuring **accurate student tracking**. However, the study reported several challenges such as **hardware failure, hygiene issues, and time delay**, especially in large educational institutions. Moreover, the system required **continuous device maintenance** and was prone to **sensor malfunctions**, making it less effective for long-term use.

Xing et al. [5] “Enhancing Student Data Security with AES Encryption in Attendance Systems” explored the **Advanced Encryption Standard (AES)** for **securing student attendance data** and maintaining **high confidentiality**. The AES algorithm provided **strong data security**, making it difficult for unauthorized users to access attendance data. However, the system did not offer **real-time attendance tracking** and still required **manual input,** making it less efficient for large institutions.

Abdullah et al. [6]” Cloud-Based Attendance Management Systems: Benefits and Challenges” focused on **cloud-based attendance management systems** for educational institutions, allowing **anytime, anywhere access** to attendance records. This approach improved **data availability and accessibility,** reducing manual work for faculty members. However, the system was highly **dependent on internet connectivity**, making it **unreliable in remote areas** with poor network infrastructure. Furthermore, cloud-based systems raised **privacy concerns**, as sensitive student data was stored on external servers.

Pawar et al. [7] “RFID-Based Automated Attendance Tracking: Strengths and Weaknesses” discussed the **use of RFID cards** for automated attendance marking. RFID (Radio Frequency Identification) technology uses radio signals to detect and record student attendance. This method significantly reduced **manual errors** and ensured faster attendance tracking. However, the system faced major challenges such as **card loss, misuse, and dependency on external devices,** leading to **inaccurate attendance marking** in some cases. Additionally, students could give their cards to others, resulting in **proxy attendance.**

Ramesh et al. [8] “Data Encryption Techniques for Secure Attendance Management” explored the importance of **data encryption techniques** such as AES, DES, and Blowfish for securing attendance records. Their study highlighted that traditional attendance management systems are prone to **data breaches and manipulation**, compromising data security. However, the study did not provide any **real-time attendance solution** or address the need for **automated attendance marking.**

Dwivedi et al. [9]” A 3-Tier Security Architecture for Protecting Attendance Data” proposed a **3-tier security architecture** to protect **student attendance data** from unauthorized access. The architecture involved **data encryption, authentication, and real-time monitoring** of student records. However, the system lacked **real-time attendance marking** and required **manual intervention**, making it less practical for large institutions. Additionally, the system did not provide **student facial recognition**, limiting its automation capacity.

Shukla et al. [10] “Ensuring Data Integrity in Attendance Systems Using Secure Hash Algorithms (SHA)” explored the use of **Secure Hash Algorithms (SHA)** for ensuring **data integrity and security** in attendance management systems. SHA converts attendance data into a hash, ensuring **tamper-proof storage** of records. However, the study did not address **automating attendance marking** and still required **manual attendance input**, making the system inefficient. Moreover, the absence of **real-time attendance tracking** limited its practical usability in educational environments.

Dida et al. [11] “Web-Based Login System for Attendance Management Using MD5 Hashing” introduced a **web-based login system** that used the **MD5 hash function** for securing student attendance data. The system allowed faculty members to **login and manage attendance records.** However, the study showed significant **vulnerability to collision attacks,** where two different data inputs could generate the same hash value, compromising **data security**. Additionally, the system did not provide **real-time attendance tracking,** limiting its efficiency in educational institutions.

Imam Riad et al. [12] “AES Encryption for Secure and Confidential Student Attendance Data” discussed the importance of using the **AES encryption algorithm** to secure attendance data. The AES encryption provided **high-level security**, ensuring that **attendance records were safe from unauthorized access**. However, the system did not offer **automated attendance marking** or **real-time attendance tracking**, making it inefficient for practical use. The absence of facial recognition limited the automation potential of the system.

### ****Findings:****

Based on the above literature survey, the following findings were observed:

* Most existing attendance systems use **manual, RFID, or fingerprint-based methods,** which are prone to errors, inefficiency, and time consumption.
* Cloud-based solutions improve data accessibility but face **network dependency issues.**
* Encryption methods like **AES, DES, and 3DES** are widely used for data security but do not address **real-time attendance tracking**.
* Facial recognition technology offers a promising solution for **automated attendance management,** ensuring **accuracy, real-time data tracking, and minimal manual intervention.**

**EDUCARE** aims to overcome these challenges by developing a **web-based, real-time automated attendance system** using **facial recognition technology**. This approach minimizes **manual effort, improves accuracy, and ensures fast attendance tracking** in educational institutions.