Cryptographic and Automatic Attendance System Using RFID Cards and PSoC Technology

ICTU Student 209
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student209@ictu.edu.vn

***Abstract*—The thesis proposes a card-based password and attendance system using RFID and PSoC technology. Its stated aim is to associate each student or employee with one card code and use that code across identification and attendance functions. The available source introduces the institutional motivation and describes parts of a communication protocol between a computer and reader modules, including start and stop markers, module addresses, data, and a checksum. These are design elements. The excerpt does not contain a conclusion, trial results, measured efficiency, or evidence that a complete system was installed. The summary therefore records the proposed architecture and protocol without claiming successful deployment or validated security.**

***Index Terms*—RFID, PSoC, password system, automatic attendance, communication protocol**

I. Introduction

The project addresses a practical identification problem in an academic department that handles student and staff records. The author proposes using a single RFID card identifier for each person rather than several disconnected identifiers. PSoC is chosen as part of the electronic design, and the system is intended to support password-related access and automatic attendance. The source presents these as the motivation and intended functions of the thesis. It does not show that the proposed arrangement improved administrative efficiency or replaced an existing deployed system [1]. Published books on the methods and subject of this project provide context for this English summary [2].

II. Methods

The document reviews RFID and PSoC and specifies a communication format between a computer and reader modules. A computer-to-module frame begins with a start marker, carries a module address and data, includes a checksum, and ends with a stop marker. The reverse direction uses a different start marker so that the receiver can distinguish messages. The design also allows an address used for broadcast handling. These details describe a protocol for a proposed attendance application. The excerpt does not provide a documented test procedure for card reading, access control, or communication reliability [1].

Supervisor: Lê Hùng Linh, Thai Nguyen University of Information and Communication Technology (lhlinh@ictu.edu.vn).

III. Results

The available material establishes the intended one-card identification concept and provides concrete protocol specifications for communication between the computer and modules. It explains how the start marker distinguishes message direction, how the address selects a recipient, and how the checksum can detect transmission errors. The text also describes the use of data and stop fields in each frame. Those specifications are the results that can be checked in the excerpt. No completed attendance records, measured read rates, security assessment, or deployment observations are supplied, so such outcomes are not attributed to the thesis [1].

IV. Discussion

A unified RFID identifier could simplify attendance and access workflows, but the source presents that benefit as a goal. The protocol design anticipates addressing, framing, and error detection, all necessary parts of communication with multiple modules. A checksum alone, however, is not proof of confidentiality or authentication. The available excerpt lacks test logs and a final evaluation of the proposed system. It therefore supports discussion of architectural choices and implementation requirements, while leaving practical reliability and institutional impact unverified [1].

V. Conclusion

The thesis describes a proposed RFID and PSoC attendance and password system centered on one card code per person. The source excerpt contains the rationale for the design and a detailed computer-to-module communication format, including start and stop markers, addresses, data, and checksums. It does not include a final assessment, measured outcomes, or evidence of an operational deployment. This summary treats the protocol as documented design work and avoids presenting intended administrative benefits or secure operation as findings already demonstrated by the manuscript [1].

References

[1] ICTU Student 209, ”Cryptographic and Automatic Attendance System Using RFID Cards and PSoC Technology,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2010.

[2] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms, 2nd ed. MIT Press, 2001. ISBN 9780262032933.