International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Parent Authentication System for the Security of Pre-Basic School Pupils

Peter Awon-Natemi Agbedemnab[1], Joseph Domebale[2], Iven Aabaah[3], Gabriel Kofi Armah[4]

[1,2,3]Department of Information Systems and Technology,
[4]Department of Business Computing.
C. K. Tedam University of Technology and Applied Science,
Navrongo, Ghana.

Abstract

The safety of pupils is of uttermost concern to school authorities and especially parents in this age of rampant kidnappings and other malicious activities by unscrupulous people within the human ecosystem. In this paper, a robust security system, referred to as a Parent Authentication System (PAS) is designed and implemented using bi-modal authentication and/or verification mechanisms for the safety of pre-basic school pupils. The primary module for authentication and verification is Fingerprint (i.e. biometrics) with an alternative module of a Password which, can only be used if the primary module fails or rejects the biometrics of a particular user. The Agile System Development Life Cycle Prototyping model was leveraged to design the system; all key components responsible for the functioning of the system have been appropriately implemented and integrated resulting in a very successful and robust system. The developed system was deployed and tested at Garu Senior High School in the Upper East Region of Ghana. During the test implementation, It was a*ffi*rmed that students with issues such as scratches and dirt on their fingers were denied access and were not able to be authenticated and verified. However, after three attempts via this primary authentication module, they were able to use the alternative module, which gave them the opportunity to be authenticated and verified. As a result, a full implementation of this system will make sure only rightful parents pick up their wards from school. This system can also be deployed in other areas for attendance monitoring or personality tracking.

Keywords: Security, Fingerprint, Password, Verification, Authentication

1 Introduction

Kidnapping and stealing of school children are on the rise and a major issue in recent times making parents always worried about their children's safety and security. Keeping, managing, and monitoring the security of individuals e*ffi*ciently within the school environment is key and vital for the safety of students. Security and safety in education are important for the singular reason of eliminating any form of harm whether physical, emotional, or psychological. Over the years, research works have demonstrated that all risks relating to the learner's well-being have security implications. Researchers must therefore consider multiple angles when it comes to issues relating to the safety and security of the physical, mental, emotional, and psychological development of the learner In recent times, it has been

observed that the manual system is mostly used for monitoring in pre-basic institutions. Teachers verbally call out students to their parents and manually mark their names whenever they are brought or they are to be picked up from school. These manual processes pose a lot of stress, and security issues, time time-consuming, and are prone to some human errors by both the school authorities and parents [2]. Security systems over the years and in modern times have played a key and important role in securing areas, houses, schools, etc. against intruders and unauthorized users. This in-security issue has been handled using various security mechanisms over the years. Some examples are the fingerprint module, face recognition module, RFID, OTP modules, etc. Most researchers in solving this security problem have developed systems that use one-way, two-way, and multiple authentication and verification mechanisms. Though these systems are e*ff*ective and e*ffi*cient, they, however, does not grant a user an alternative or a second option in gaining access to a system should one authentication or verification fail. The user per the current systems is required to be authenticated by all the security verification and authentication modules before access is granted. This however creates inconveniences that may lead to denial of access and it is also time-consuming.

It is on the back of these we considered it necessary to develop a system for securing school pupils especially those in the pre-school using bi-modal authentication modules so that at any material moment the true parents/guardians will be the ones to pick up their wards from school. Lately, fingerprint verification technology is considered the most popular, reliable, and convenient means of verifying a person's identity. Also, considering biometric technologies for authentication and verification of security solutions, the fingerprint module is regarded as the best and most appropriate because as compared with other modules, it is cheaper, more convenient to use, and is also known to have a low false acceptance rate [3]. Also, the PIN/Password technology is one verification module that is very cheap, and convenient to use alongside the fingerprint module [4]. The proposed system will, therefore, ease the burden on users having to mandatorily fulfill all or various authentication modules before access is granted. The rest of the paper is organized as follows: Section 2 presents a review of existing literature on authentication systems highlighting their strengths and gaps. The methods and tools employed during the implementation of the proposed system are presented in Section 3 as the methodology. Section 4 presents the test implementation results of the proposed system as well as an evaluation of its performance on some metrics with existing systems while Section 5 concludes the paper.

2 Literature Review

A survey of existing literature on one-way and multi-factor security systems for monitoring the attendance of students and sta*ff* of schools and other workplaces is presented next, focusing on fingerprint and pin code/password technologies. The work in [5] proposed and developed a system that uses the fingerprint module. The system monitors and solves attendance problems at the Bells University of Technology, Ota Nigeria. The system was able to ensure that only valid students were allowed to attend lectures by comparing their fingerprints to that of the stored information in the database system. Only valid students, meaning only students who have been able to register for their respective courses in a semester are granted access to lecture halls. However, the system is unable to take and keep records of the attendance of students. Also, the system is unable to generate attendance reports of students. Also, [6] developed a school attendance management system that uses a fingerprint module. It records the attendance of lecturers and students by matching the fingerprint image to the pre-registered fingerprints in the database. It is also built with the ability to generate reports of students and the total attendance of

lecturers weekly and monthly. It is designed to avoid impersonation from other students and also to eliminate the traditional manual way of recording students' attendance. Though it's very portable and easy to use, the following setbacks are associated with the system; it lacks GSM connectivity, and it may be prone to false rejects since it involves a single verification mechanism. Additionally, authentication issues are likely to be encountered should the user biometrics fail. In [7], they designed and developed a system for managing attendance using a fingerprint module for institutions within the educational sector. It has one fingerprint sensor and LCD screen placed at suitable places in the institution. To monitor students' attendance, students' fingerprints are captured by the biometric device and matched with the pre-stored biometrics in the system. The system was able to eliminate and reduce the energy and time spent in taking attendance of students through the traditional manual system. However, some challenges identified with the system are; that parents are not given alerts on the attendance of their children daily, but rather collated messages sent at the end of each term or semester and it employs only one authentication mechanism.

In [8], the authors proposed an attendance system with a biometric feature (fingerprint sensor) which they named the Smart Attendance System (SAS). The system was to address issues relating to time lost as a result of taking attendance of students. In the process of enrollment, fingerprint images of faculties and learners are stored in the device. Its hardware components are; the fingerprint device, an LCD Screen, and an Arduino UNO microcontroller. Though it's portable and user-friendly, it lacks GSM connectivity i.e. parents are not given alerts on the attendance of their children. A system to monitor students' attendance was designed in [9]. The proposed system uses fingerprint technology to capture students' attendance at school. With the motive of overcoming the drawbacks associated with the manual system of monitoring and keeping records of students, the system has a desktop-based application and a database server capable of registering and keeping records of attendance of students. Reports can however be accurately generated as they are needed. The system lacks GSM connectivity and may pose authentication and verification problems should a student have problems with the fingerprint image. Furthermore, [10] designed and developed a smart system to monitor students' attendance in schools. It is built with an Arduino microcontroller embedded with a GSM module. Verification and authentication are done through the matching of the fingerprints of students to the pre-registered information in the database. An automatic SMS alert is generated and sent to parents once authentication is done. It eliminates the manual system where papers and books are used to record and keep the attendance of students. presented a Smart and Secure Fingerprint attendance system using Arduino UNO with GSM alert. It employs a single authentication mechanism and comes with a number of challenges. Similarly, [11] proposed a system for taking attendance of students and lecturers in institutions using a fingerprint module. Its design comprises five components. First, the fingerprint component enables and facilitates the capturing of biometrics of users. The second component is the window application component where the biometrics of users are pre-processed and stored in a web service component. From there, the data is stored in the database component. The web application component is a secondary storage system making it the last component. With improved e*ffi*ciency and easy usability, the system had an error rate of 2.5% when it was tested and also lacked GSM connectivity. A work by [12] also developed a multi-factor system using PIN/Password technology with SMS verification technology. The system monitors and records the attendance of students and teachers in higher educational institutions in other to avoid wasting productive time in getting students and sta*ff* records. This system possesses multiple authentication mechanisms that users are required to produce before verification and gaining access. The system first

requires a password from the user which is matched with pre-stored passwords in the database to grant or deny an OTP message. If the password corresponds to database credentials, the dynamic password generator generates an OTP to the user's cell phone using an SMS gateway provider to the user grant acceptance. The system offers a robust authentication mechanism that is secure, less expensive, user-friendly, and efficient. Limitations of the system are; that it may take a long time to deliver the password to a user, and it lacks RTC.

From the above literature, it is observed that there are some limitations associated with the systems as proposed by various researchers. The proposed system seeks to contribute in this regard especially for schools in this part of the world, to design and develop a robust security system to monitor how and who comes to drop off children and pick them up in their various schools when they close. Combining fingerprint technology (primary authentication module) with PIN technology (secondary authentication module) is, therefore, a justifiable approach since it will also incorporate GSM connectivity where SMS will be sent to registered parents/guardians in the database. Primarily, the system seeks to avoid and eradicate challenges encountered in the implementation of departure verification and authentication systems. The system is very simple and not costly with the ability to keep the attendance and departure records of students and parents who come to pick up their children from school.

3 Methodology

The methods and tools employed during the design and implementation of the proposed system are presented next.

3.1 System Design

The primary objective of the proposed system is to add another layer to a single-layer authentication and verification module by granting users a secondary option for authentication and verification should the primary authentication and verification module fail or encounter a problem. The system was programmed and developed using Microsoft C# language. The user's fingerprint images which comprise a primary parent and three other relatives, and other information about these people are captured and pre-stored in the database with the respective name(s) of their children attached. This data is then stored in a Microsoft SQL Server for processing and matching purposes. Figure 1 is a schematic diagram of the system architecture.

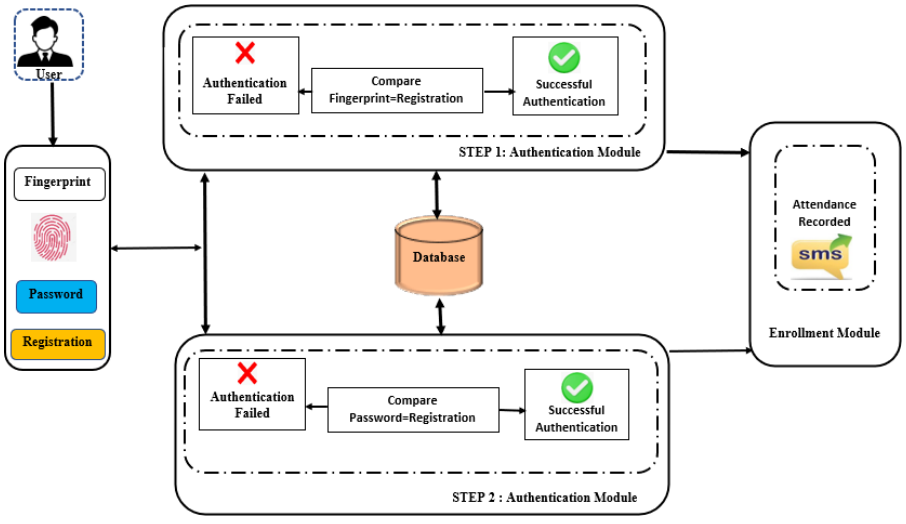

Figure 1: System Architecture

To be granted access to pick up your child from the school, you need to first verify your identity primarily via fingerprint. If the fingerprint image matches with what is stored in the database, a window is displayed with the picture of the verified person, and an alert sent to the primary parent via SMS indicating the time and the person who is picking up the child. But if the fingerprint image does not match the pre-stored data after three attempts, the person is redirected to use the PIN/Password option. The processes involving how the system works are explained using the flowchart in Figure 2.

3.2 System Implementation

The system is developed and coded using C# programming language and MySQL. C# is used for the creation of the application interface which is linked to the parent's and pupils' databases handled by MySQL. Additionally, fingerprint and password modules are embedded in the system for primary and secondary authentication purposes respectively. Meanwhile, an API module using an SMS gateway provider (InnotechIT Bulk SMS) is embedded also for sending messages to parents.

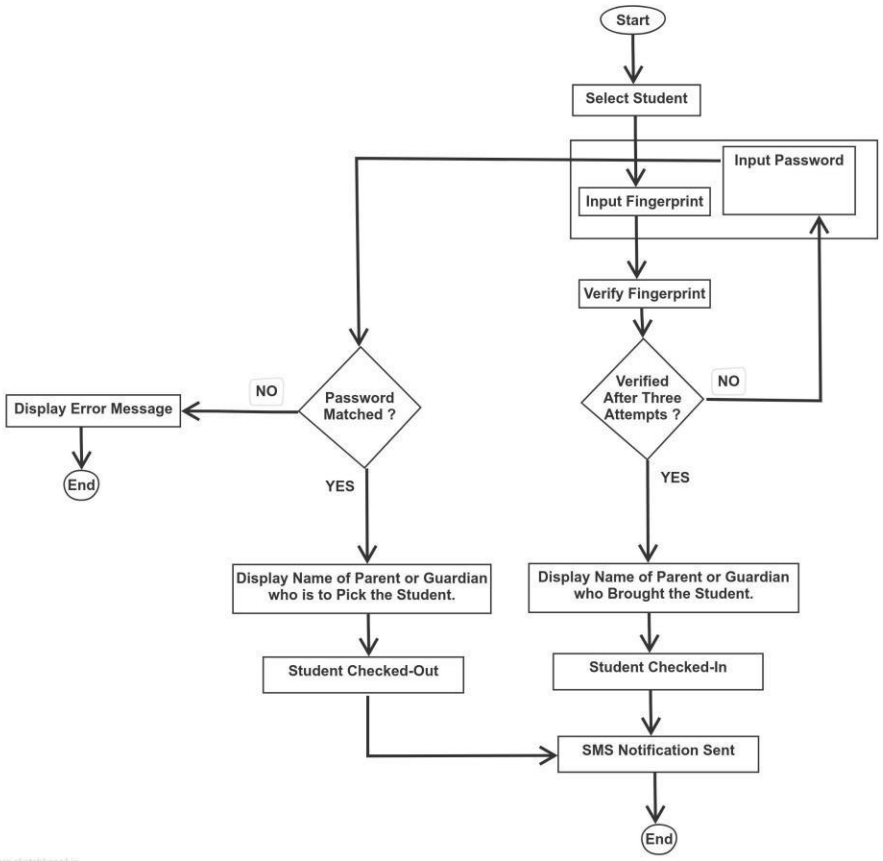

Figure 2: Flowchart of the Proposed Authentication System

3.2.1 Fingerprint Module

The fingerprint technology is used in this paper to develop the system. This is for identification and authentication purposes and it is the primary authentication and verification mechanism for granting access. Research indicates that every human being has a unique fingerprint that is permanent and di*ff*erent from other people which is for a whole life. Hence, there are no two di*ff*erent people with the same fingerprint based on these unique characteristics, It is concluded that fingerprint is a secure, e*ffi*cient, and reliable mechanism for forensic biometric applications and for personal identification systems [13]. In the proposed system, the DigitalPersona U.are. U 4500 scanner is used as shown in Figure 3. The device is

an optical sensor type with USB 2.0 which can reject latent fingerprints. It has a sensor coating made up of silicon that makes it able to read fingerprints of varied ranges at a faster rate no matter the angle of placement. For verification, a red "Flash" shows a fingerprint image is successfully captured. It captures fingerprint images at a faster rate with excellent quality images and encrypts them.

Figure 3: DigitalPersona U 4500 Fingerprint Scanner

3.2.2 Database

Microsoft SQL which is an open-source database system is used to handle the database of the whole system. Additionally, the logical database method and design are used. This scheme helps to transform data that is represented in high-level into structures of database management systems. Data query, data manipulation, data identity, and data access control are some of the key operations associated with MySQL [14]. This system's database is made up of various tables responsible for storing records that correspond to all authorised users accessing the system. The database server aids C# and Apache to work collaboratively in helping access and display information and data in a format that can be read. Information like first name, last name, passwords, usernames, phone numbers, and email addresses of users are handled and stored in the database.

3.2.3 Password Module

The system is designed to use a secondary authentication and verification module. The password module is likely to be required as a fallback if the primary authentication module (fingerprint module) encounters authentication and verification challenges and other security issues. Passwords play a very important security role by ensuring that data and devices can only be accessed by authorised users and those who have permission to use them [15]. Various forms of passwords can be grouped into; Advance Encryption Standard, Triple Data Encryption Standard [16], Encryption and Decryption, [17], and One-Time Password (OTP), [18]. The Password Authentication Protocol (PAP) which is an internet standard (RFC 1334), Password-based verification and authentication protocol is used as the secondary authentication mechanism. PAP is a client-server authentication protocol that is simple and easy to implement, [19].

3.2.4 SMS Module (API Technology)

During the development of the system, the Application Programming Interface (API) technology was used and incorporated into the whole system setup for communication purposes. Application Programming Interface (API) is a programming code that makes it possible for two di*ff*erent applications

to be able to communicate, [20]. Considering this, the API acts as an intermediate layer between the server and the client aiding in the exchange of data. In designing and implementing APIs for the Web, there are several types involved, some examples are; Open/Public APIs, Partner APIs, Composite APIs, etc. For this work, the Private/Internal APIs are used. Additionally, API o*ff*ers high-security protection between users or systems by providing security layers that can secure data during communications. It provides users with security and privacy protection since additional protection features are provided thereby allowing the user to deny or grant requests, [21].

4 Results, Testing, and Discussion

Results from the test implementation of the developed system are discussed next in this section.

4.1 Results

To evaluate the functions of the system, the software after its development was tested on the following aspects:

- The ability for a parent to be authenticated and verified.
- The ability to send SMS notifications.
- Ability to view students' attendance/departure status.

Table 1 shows the testing that has been carried out in the system development and the results.

S/N	Tested Data	Expected Results	Actual Results
1	Administration Login	Expected to log in only if it is the administrator	Was able to log in due to the correct credentials
2	SMS notification	Expected to send reports to parents via SMS	Was successful
3	Verification	Expected to verify parents correctly without errors	Was able to verify parents correctly without errors
4	View of Reports	To see if reports and records of all students can be viewed	Was successful
5	Queries	Expected to see user's information	Was successful

Table 1: System Evaluation Results

Observations from Table 1 indicate that the developed system has addressed the outlined specifications. Moreover, Figure 4 to Figure 7 present a pictorial view of some of the interfaces of the developed system. Next, are some interfaces of the developed system: Figure 4 is the User Sign Up/registration screen where the particulars of new parents such as phone number, name, preferred password, etc. including the biometric data are captured into the database. Before a parent takes the child from school, he/she would be verified and authenticated by the system. This is first done through the fingerprint module but if that fails the parent will then use the password module. This is shown in Figure

5. Figure 6 is the interface of a successful verification and authentication process, after which, an SMS notification will be sent to the primary parent indicating the person who has come to pick up the child with a times- tamp. Figure 7 is a screenshot of a report of registered pupils which, contains relevant information for school administration.

4.2 Testing and Discussion

To evaluate the e*ff*ectiveness and usability of the proposed system (i.e. Parent Authentication System), various sets and series of experiments needed to have been conducted on the system. Hence, the system was experimented with and evaluated through usability testing (Biometric E*ffi*ciency Test) and Speed Testing. This technique ensures that only intended and authorised users of the system will be able to perform and execute the intended activities e*ff*ectively and successfully.

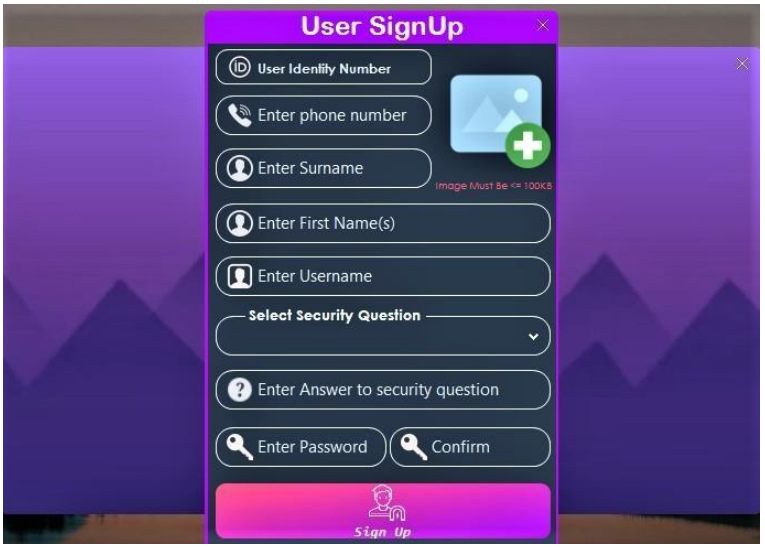

Figure 4: Sign-Up Page

Figure 5: Verification Before Departure

4.2.1 Biometric E*ffi*ciency Test

In order to test for the e*ff*ectiveness and consistency of a system regarding its error rates, there is the need to consider the False Acceptance Rate (FAR) and False Reject Rate (FRR) [22]. These error rates are measured with the following metrics;

- **False Accept:** This occurs when an illegitimate/unauthorized user's fingerprint is accepted as valid and granted access in the verification process.
- **False Reject:** This occurs when a legitimate or authorised fingerprint of a user is denied access to a

system.

- **True Accept:** This is a situation whereby the fingerprint image of an authorised user matches the stored fingerprint in a system.
- **True Reject:** This is a situation where the fingerprint image of an unauthorised user is rejected by a system due to a mismatch.

Hence, to evaluate and determine the performance of fingerprint systems, there are two accepted performance evaluation indexes. These are;

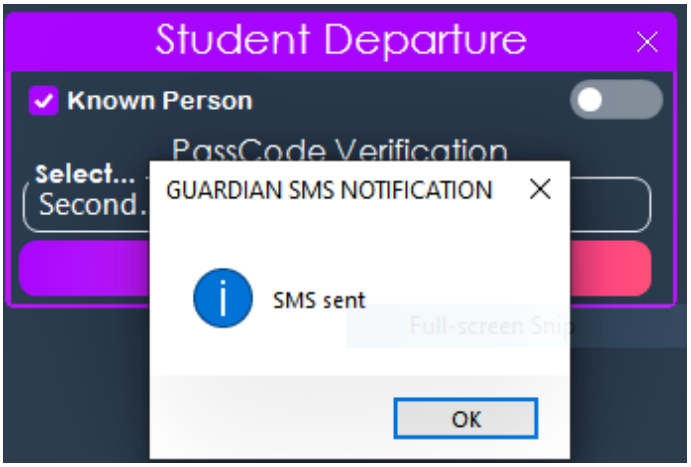

Figure 6: SMS Notification

Figure 7: Admission Report

(a) False Rejection Rate (FRR): It is a situation where a legitimate or authorised user is denied access to a system as a result of system failure. It is known as a Type 1 error by security analysts because it poses no security threats.

FRR (%)

$$FRR = \frac{FR}{N} \times 100$$

FR = Number of False Incidents rejected

N = Number of samples

(b) False Accept Rate (FAR): This is a situation where an illegitimate/unauthorised user somehow is granted access to a system as a result of systemic failure. It is known as a Type II error by security professionals because it poses a lot of security threats and it's not acceptable.

FAR (%)

$$FAR = \frac{FA}{N} \times 100$$

FA = Number of False Incidents Accepted

N = Number of samples

The system was tested at Garu Senior High School for a week in five classes, one class a day. Students were registered in the system by capturing the bio-data and other details for verification purposes. Students acted as parents and would have to be authenticated through either the fingerprint module or the password module. The table below shows the results of authentication and verification processes carried out using the fingerprint module.

Date	No. Of Students	False Accepts	False Rejects	True Accepts	True Rejects	FAR (%)	FRR (%)
24-04-2023	60	0	0	49	11	0.00%	0.00%
25-04-2023	40	0	0	26	14	0.00%	0.00%
26-04-2023	25	0	0	18	7	0.00%	0.00%
27-04-2023	32	0	0	23	9	0.00%	0.00%
28-04-2023	30	0	0	24	6	0.00%	0.00%

Table 2: False Accept and False Reject using The Primary Verification Module

From Table 2, the error rate used in measuring the e*ffi*ciency of the system can be inferred and concluded as:

False Accept Rate (FAR) = 0.00% False Reject Rate (FRR) = 0.00%

It's also observed that users with unclean fingers or scratched fingerprints were blocked and denied access as shown in the results for True rejects. Table 3 shows the results of parents using the second authentication module (Password) for authentication and verification.

Date	No. Of Students	False Accepts	False Rejects	True Accepts	True Rejects	FAR (%)	FRR (%)
24-04-2023	60	0	0	60	0	0.00%	0.00%
25-04-2023	40	0	0	40	0	0.00%	0.00%
26-04-2023	25	0	0	25	0	0.00%	0.00%
27-04-2023	32	0	0	32	0	0.00%	0.00%
28-04-2023	30	0	0	30	0	0.00%	0.00%

Table 3: False Accept and False Reject using Secondary Verification Module

From Table 3, it can be deduced that the proposed system is very efficient and effective considering the error rate.

False Accept Rate (FAR) = 0.00%. False Reject Rate (FRR) = 0.00%.

However, inferring from Table 3, parents who were blocked and denied access as a result of unclean and scratched fingerprints have now gained access and authenticated successfully via the secondary authentication module. This implies the proposed system has been able to address the major objective of the system i.e., a secondary module for verification to augment the primary module in case of failure and accidents.

4.2.2 Speed Test

The speed or rate of throughput test purposely measures the time taken to authenticate a parent using the proposed system. Using the various authentication modules, the proposed system, Parent Authentication System (PAS) was compared with similar existing systems that utilise the fingerprint module for verification and authentication for attendance based on the average time for execution. Table 4 is a comparison of PAS with the work by [23] which, utilises the fingerprint module for authentication and verification for attendance using the same sample size. From Table 4, the average time taken per student

		eduTAMS		PAS	
Sample	**No. Of Students**	**Total Time**	**Average Time**	**Total Time**	**Average Time**
1	48	5minutes 41 seconds	7.11 seconds	4minutes 46 seconds	5.96 seconds
2	52	6minutes 5 seconds	7.01 seconds	5minutes 1 second	5.79 seconds
3	58	6minutes	6.22 seconds	5minutes 25 seconds	5.60 seconds
4	55	5minutes 50 seconds	6.40 seconds	5minutes 5 seconds	5.54 seconds

Table 4: Speed Test Comparison

using eduTAMS is 6.65 seconds whilst that of PAS is 5.72 seconds. This shows that the proposed PAS is faster than that of eduTAMS. Figure 8 is a graphical group chart of the speed evaluation. From the bar chart, it is observed that the average time taken to authenticate the attendance of users using the PAS is about **5.72 seconds** compared to about **6.65 seconds** when using the eduTAMS. Hence, an average time of **0.93 seconds** has been saved. This time saved can be used effectively in enhancing instructional activities.

5 Conclusion

In this paper, a robust parent authentication system was designed and implemented using bi-modal authentication approaches for the primary purpose of securing the safety of pre-basic school children. In

addition to security, the proposed system is able to keep records of attendance. Additionally, parents can monitor the person who comes to pick up their child(ren) from school and the specific time the child(ren) is picked up through an SMS alert. The proposed system can be replicated in other sectors for attendance monitoring and issues relating to security. In future work, multiple fingers can be considered to enhance reliability.

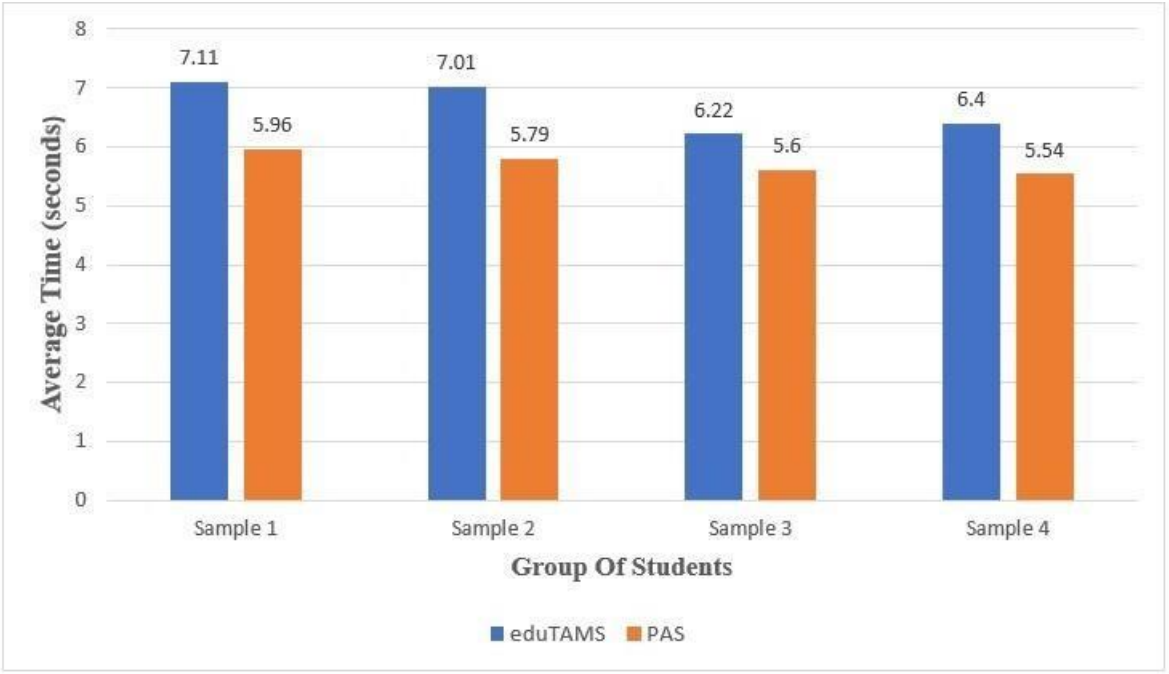

Figure 8: Group Bar Chart of Speed Test

References

1. Elda de Waal and M. M. Grösser. Safety and security at school: A pedagogical perspective. *Teaching and Teacher Education*, 25(5):697–706, 2009.
2. Hitesh Walia, Neelu Jain, et al. Fingerprint based attendance systems-a review. *International Research Journal of Engineering and Technology*, 3(5):1166–1171, 2016.
3. Acroprint Time and Recorder Company. Frequently Asked Questions About Biometrics for Time and Attendance. 2005.
4. Krishna Prasad and PS Aithal. Abcd analysis of fingerprint hash code, password and otp based multifactor authentication model. *Saudi Journal of Business and Management Studies*, 3(1):65–80, 2018.
5. B Kokumo. Lecture attendance system using biometric fingerprint. *B. Tech Dissertation, Department of Computer Science and Technology, Bells University of Technology, Ota, Nigeria*, 2010.
6. Oluwagbemiga Shoewu and OA Idowu. Development of attendance management system using biometrics. *The Pacific Journal of Science and Technology*, 13(1):300–307, 2012.
7. N Swathi, Ch Padmaja, Y Sharvani, Ranganath Kanakam, and P Ramchandar Rao. Tracking and security system for school van. In *AIP Conference Proceedings*, volume 2418, page 030019. AIP Publishing LLC, 2022.
8. Swarnendu Ghosh, Shafi KP Mohammed, Neeraj Mogal, Prabhu Kalyan Nayak, and Biswajeet Champaty. Smart attendance system. In *2018 international conference on smart city and emerging technology (ICSCET)*, pages 1–5. IEEE, 2018.

9. Blessed Olalekan Oyebola, Kayode Oluwabukola Olabisi, and Oyerinde Solomon Adewale. Fingerprint for Personal Identification : A Developed System for Students Fingerprint for Personal Identification : A Developed System for Students Attendance Information Management. (January), 2018.
10. Ritam Dutta, Tenzing Tamang, Pranoy Paul, Nitesh Kumar, Chandan Chetri, and Pradip Kumar Dutta. Smart and Secure Fingerprint Attendance System using Arduino UNO with GSM Alert. In *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, pages 1086–1090. Institute of Electrical and Electronics Engineers Inc., dec 2020.
11. Huda Basloom, Sahar Bosaeed, and Rashid Mehmood. Hudhour: A fuzzy logic based smart fingerprint attendance system. In *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 331–336. IEEE, 2020.
12. Abimbola Rhoda Iyanda and Mayokun Ebenezer Fasasi. Development of two-factor authentication login system using dynamic password with sms verification. 2022.
13. Upasana Ghosh Dastidar, Nikhita Jogi, Milan Bansod, Payal Madamwar, and Priyanka Jalan. Fingerprint sensor based attendance system using atmega 328 and esp8266. *Int J Res Sci Eng*, 3(2):471–475, 2017.
14. Siti Maesaroh, Heru Gunawan, Agung Lestari, Muhammad Sufyan Ats Tsaurie, and Mohamad Fauji. Query optimization in mysql database using index. *International Journal of Cyber and IT Service Management*, 2(2):104–110, 2022.
15. A Stein. What is password hacking?, 2022.
16. Gurpreet Singh. A study of encryption algorithms (rsa, des, 3des and aes) for information security.
17. *International Journal of Computer Applications*, 67(19), 2013.
18. Obaida Mohammad Awad Al-Hazaimeh. A new approach for complex encrypting and decrypting data. *International Journal of Computer Networks & Communications*, 5(2):95, 2013.
19. John Jacob, Kavya Jha, Paarth Kotak, and Shubha Puthran. Mobile attendance using near field communication and one-time password. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pages 1298–1303. IEEE, 2015.
20. Hsien-Chu Wu, Min-Shiang Hwang, and Chia-Hsin Liu. A secure strong-password authentication protocol. *Fundamenta Informaticae*, 68(4):399–406, 2005.
21. Li Gong, Gary Ellison, and Mary Dageforde. *Inside Java 2 platform security: architecture, API design, and implementation*. Addison-Wesley Professional, 2003.
22. Tamar Sharon. Blind-sided by privacy? digital contact tracing, the apple/google api and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 23(Suppl 1):45– 57, 2021.
23. Matteo Golfarelli, Dario Maio, and D Malton. On the error-reject trade-off in biometric verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7):786–796, 1997.
24. Aderonke Justina Ikuomola. Fingerprint-based authentication system for time and attendance man- agement. *British Journal of Mathematics & Computer Science*, 5(6):735, 2015.