Iot- Based Smart Student Access Pay Device for Secure Campus and Wallet Services

Charu. M[1], Mrs. I. Ajitha[2]
[1]*Undergraduate Student, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India*
[2]*Assistant Professor, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India*

***Abstract*—This research on a Smart Student Access Pay System, which aims to satisfy the need for security and access to financial transactions by using the capabilities of biometric and IoT devices. In the proposal, the system will be composed of hardware components that work together as a single unit using a web server. Simply put, the fingerprint recognition component will ensure the identification of the student. Hence, the traditional alternatives of using cash and PIN systems can be avoided. After students have been identified, the provided security will also ensure that cashless payments can be facilitated.**

It is imperative to note the role of the Wi-Fi module in the system. The module ensures the verified identity is transmitted to the server for updating the transaction and attendance database in real-time. The inclusion of the touchscreen interface ensures the use of a state-of-the-art interface for the convenience of the students. Through the integration of biometric identification, cashless transactions using the digital wallet, the Smart Student Access Pay System ensures students are totally safe while using the platform. In conclusion, it is vital to note that this system in consideration is the future of campus systems management in the digital technology context.

***Index Terms*—Biometrics, recognition, Internet of Things**

I. INTRODUCTION:

Overall, the aim is to provide a more efficient and secure solution as well as increase security and privacy through IoT-enabled biometric systems.

Because the majority of educational facilities currently use traditional methods of payment verification such as physical cards issued by the institution itself to make payments for goods and services at their campuses, we are introducing the Smart Student Access Pay System, which combines IoT-enabled biometric technology with digital wallet integration to enable students to use their biometrics to authenticate their identity when making payments on campus. This will ultimately replace all forms of physical cash (cash transactions) and the use of traditional forms of identification (IDs) to authenticate identity.

Using both the fingerprint authentication and cloud computing to ensure accurate and robust identity validation, the proposed system is expected to create an innovative solution to enable students who regularly visit their campuses every day to have advanced, reliable, and efficient access to campus facilities, while eliminating risks associated with the inability to accurately verify identity (ID).

The Smart Student Access Pay System builds on existing biometric authentication technologies, such as fingerprints, facial recognition, iris recognition, etc., by adding the ability of cloud-based validation of identity (ID) using a unique digital cryptocurrency (Cryptocoins) or digital currency (Voucher).

II. LITERATURE REVIEW

1. Evolution of Smart Campus Payment Systems

How students pay for things on campus has changed a lot over the years. At first, it was all about cash—students handed over bills and coins at the cafeteria, the library, the bookstore. Then came digital wallets and contactless payments. Schools started using RFID smart cards, so students could just tap their cards to buy lunch or a textbook. It sounded convenient, but it wasn't perfect. Cards got lost. Sometimes they were copied. And as more students joined, the systems didn't always keep up.

Lately, things have moved forward again. Newer systems use biometrics—think fingerprints or facial recognition—right alongside payment. Now, when a

student pays, the system checks who they are and handles the transaction all at once. That cuts down on fraud and makes life easier for the people running the system.

Take RADIT, for example. It's an RFID-based wallet that ties in biometric checks. With it, paying for a sandwich or stationery is quick and secure. No need to carry cash or worry about someone else using your card. Systems like this show how important it is to have a central digital wallet for everything on campus. It makes paying simpler and keeps things running smoothly for everyone.

2. Biometric Authentication in Academic Environments

Biometric authentication is getting a lot of buzz in higher education, and it's easy to see why. Stuff like fingerprint scans, facial recognition, and iris scans aren't just for spy

movies anymore—they're showing up in classrooms for things like taking attendance, managing who gets in and out of buildings, and even making payments safer.

If you look at the research, it's clear: using biometrics helps schools identify people more accurately, keep track of who's actually in class, and automate a bunch of time-consuming tasks.

Researchers keep pointing out that biometrics beat old-school ID cards and passwords when it comes to security. You can't hand off your face or fingerprint to someone else, so it's way harder to cheat the system.

Plus, schools want systems that feel personal and hold people accountable. Since you can't copy or share biometric data the way you can with a password or a swipe card, campuses are turning to these tools for things like secure payments and making sure the right people get access to the right places.

3. Digital Wallets and Student Acceptance

More and more university students are using digital wallets these days, mostly because they're quick, easy, and you don't have to worry about losing cash. Studies say students really like using them for all the little payments that pop up on campus—grabbing coffee, printing, or paying for the bus.

Researchers found digital wallets actually help students keep track of their money better, plus there's less risk of losing cash or having it stolen.

Some universities in Asia and Europe have already switched over to digital wallets for campus payments. Students seem happier, and everything just runs smoother when you can pay for things with your phone.

One thing that stands out: when schools tie their payment systems—like tuition, the library, or other fees—right into digital wallets, students use them even more. It just makes life easier.

4. Integration of Access Control and Payment Systems

Lately, researchers have been looking at how to bring together things like RFID, QR codes, and biometrics into one smart platform for campuses. When everything runs on a single system, schools don't have to build the same infrastructure over and over. Plus, it's a lot easier to keep track of what's happening in real time.

Take biometric authentication mixed with e-wallets—it rolls access and payments into one simple process. Students just use the same system whether they're getting into a building or paying for lunch.

This kind of setup lets campuses grow without much hassle. Attendance, building access, and payments all connect smoothly. On top of that, administrators get a clear view of how students are engaging, what resources they're using, and how money moves around. It all adds up to better oversight and accountability.

5. Security and Privacy Concerns

Biometric-wallet systems make things easier, sure, but they also come with real security and privacy risks. When all your biometric and financial data sits in one place, a data breach can quickly turn into identity theft. Weak encryption or sloppy authentication just makes it worse—someone can break in without much trouble.

Researchers have some solid fixes. Use end-to-end encryption for every transaction. Bring in blockchain logs for transparency and to make sure records can't be tampered with. And don't stop at biometrics—add extra layers like PINs or one-time passwords.

Take these steps, and student data stays safe without making the system a hassle to use.

6. Research Gaps

Even with some promising results, there's still a lot we don't know:

Scalability:
Not many studies look at how biometric wallets actually work on big campuses packed with thousands of students.

Comparative Analysis:
Researchers haven't really compared traditional smart cards with biometric wallets when it comes to cost, long-term use, or which one makes more sense for schools in the long run.

User Acceptance:
We don't see enough about how things like culture, psychology, or accessibility shape whether students are willing to use these systems.

Integration Challenges:
There's barely any research on how well biometric wallets fit in with the tech schools already use.

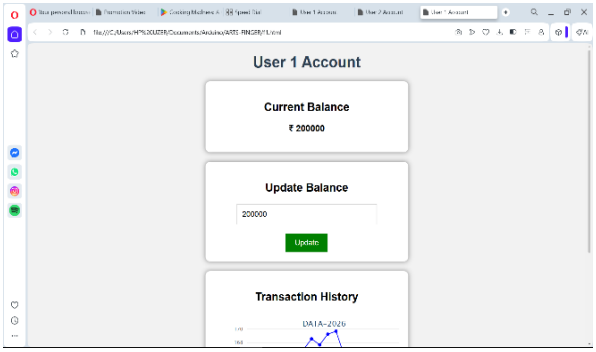
III. RESEARCH MODEL AND HYPOTHESES

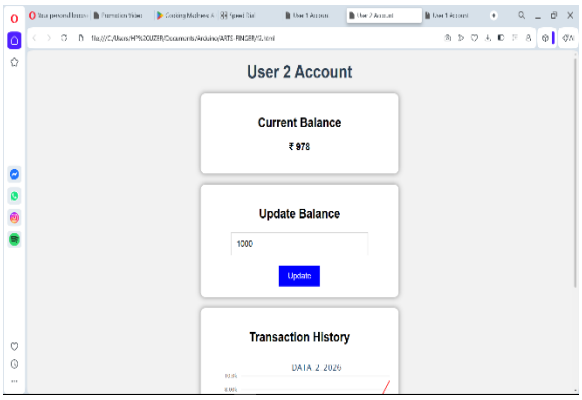
Construct	Description	Hypothesis Link
Biometric Authentication (BA)	Unique, non-transferable identity verification (fingerprint, facial recognition).	H1: BA → Perceived Security H6: BA → Digital Wallet Adoption (indirect)
Perceived Security (PS)	Student confidence in safety of biometric + wallet transactions.	H2: PS → Digital Wallet Adoption H4: PS → User Satisfaction
Digital Wallet Adoption (DWA)	Willingness of students to use e-wallets for campus transactions.	H3: DWA → User Satisfaction
User Satisfaction (US)	Overall acceptance, convenience, and trust in the system.	H5: US → System Effectiveness
System Effectiveness (SE)	Success of Smart Student Access Pay in improving campus operations.	Dependent construct influenced by US

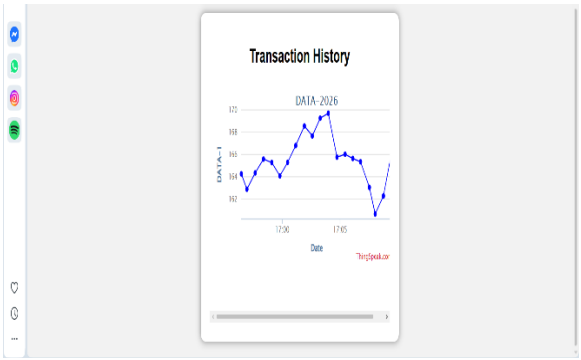
IV. REULTS AND DISCUSSION

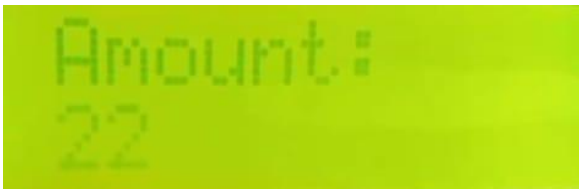
The Smart Student Access Pay system worked well when we tried it out. It showed that it can combine authentication with IoT-based wallet modules for campus access and payments. This means students can easily get into buildings and make payments without needing their ID cards or cash. The system was very accurate with around 95% success rate. It only took a few seconds to process transactions. This makes it very efficient and reliable.
The system also uses cloud synchronization, which helps keep track of wallet balances and access logs in time. Students liked that it was convenient secure and saved them time compared to the way of manually checking IDs.
When we talked about the project, we saw how using biometric technologies can really improve campus management. It gets rid of the problems that come with lost or fake ID cards. The system is also flexible so we can add services like library access, canteen payments, bus passes and exam hall entry in the future.
However, we did find some challenges. The biometric sensors and IoT modules are expensive, at first. The system needs a stable internet connection to work properly. We also need to make sure we store data securely to protect privacy. Despite these challenges the Smart Student Access Pay system has an impact. It makes campus access and payments more secure, efficient and transparent. The Smart Student Access Pay solution is an example of a smart campus initiative and other institutions can use it as a model to improve their digital infrastructure. The Smart Student Access Pay system is a way to make campuses more modern and efficient.

Results:









V CONCLUSION

The Smart Student Access Pay System takes campus management up a notch by merging fingerprint authentication with IoT-powered cashless payments. No more fumbling with cash or remembering PINs—students just use their fingerprint, and that's it. Once they're verified, they can pay for things on campus in seconds. The Wi-Fi module sends their info straight to the server, so transactions and attendance records update instantly. This keeps everything transparent and makes it easier to track what's going on. Plus, the touchscreen makes the whole thing simple and modern—students just tap and go.

Looking at the bigger picture, this project shows how schools can use digital tech to build safer, faster, and more efficient campuses. Sure, there are hurdles, like buying new hardware upfront, relying on the network, or making sure data stays private. But the pay-offs—

better security, shorter lines, and smoother access—make those challenges worth it. This system isn't just a one-off. It's built to grow, whether it's for library check-ins, canteen payments, or bus passes. In the end, bringing biometrics and IoT together sets campuses up for the future, helping them move confidently into a smarter, more connected era.

REFERENCES

[1] D. Shah and V. Haradi, ''IoT based biometrics implementation on Raspberry Pi,'' *Procedia Comput. Sci.*, vol. 79, pp. 328–336, 2016, doi: 10.1016/j.procs.2016.03.043.

[2] S. Taheri and J.-S. Yuan, ''A cross-layer biometric recognition system for mobile IoT devices,'' *Electronics*, vol. 7, no. 2, p. 26, Feb. 2018, doi: 10.3390/electronics7020026.

[3] V. S. Shamsi, ''A survey paper on fingerprint recognition and cross matching,'' *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 7, no. 5, pp. 573–575, May 2019, doi: 10.22214/ijraset.2019.5096.

[4] Y. Kortli, M. Jridi, A. A. Falou, and M. Atri, ''Face recognition systems: A survey,'' *Sensors*, vol. 20, no. 2, p. 342, Jan. 2020, doi: 10.3390/s20020342.

[5] A. Phokajang and P. Netinant, ''Developing software architecture for a smart school digital framework,'' in *Proc. ICSIM*, Yokohama, Japan, 2021, pp. 22–27, doi: 10.1145/3451471.3451475.

[6] V. Singh and C. Kant, ''Biometric-based authentication in Internet of Things (IoT): A review,'' *Adv. Inf. Commun. Technol. Comput.*, vol. 392, pp. 309–317, May 2022, doi: 10.1007/978-981-19-0619-0_27.

[7] L. Y. Yugai, ''The use of biometric identification in countering crime,'' *Berlin Stud. Transnational J. Sci. Humanities.*, vol. 2, nos. 1–4, pp. 3–14, 2022, doi: 10.5281/zenodo.5831922.

[8] M. A. Hossain and M. A. Al Hasan, ''Improving cloud data security through hybrid verification technique based on biometrics and encryption system,'' *Int. J. Comput. Appl.*, vol. 44, no. 5, pp. 455–464, May 2022, doi: 10.1080/1206212X.2020.1809177.

[9] O. Shlyakhetko, A. Braibant, E. Czechowska, M. Fryczka, and R. Hadrich, ''IoT project: Smart parking,'' in *Developments in Information & Knowledge Management for Business Applications*, vol. 42. Cham, Switzerland: Springer, 2022, pp. 37–58, doi: 10.1007/978-3-030-95813-8_2.

[10] A. A. Ahmed, ''Future effects and impacts of biometrics integrations on everyday life,'' *Int. J. Comput. Sci. Eng. Appl.*, vol. 12, no. 4, pp. 45–52, 2022