JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IOT BASED ATTENDENCE SYSTEM USING BLOCKCHAIN

V Mahesh, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana.

Dr. A.Satya Narayana, Professor, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana.

Dr. Dinesh Kumar Rangarajan, Professor & HoD, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana.

Dr. JBV Subrahmanyam, Professor & Principal, Siddhartha Institute of Technology & Sciences, Telangana.

Abstract - Traditionally, student's attendances are taken manually by using attendance sheet given by the faculty members in class, which is a time-consuming event. Moreover, it is very difficult to verify one by one student in a large classroom environment with distributed branches whether the authenticated students are actually responding or not. Using conventional method of calling out names takes approximately 5-10 minutes for marking attendance of entire class. It becomes complicated when strength is more. With the increase in technology, attendance monitoring is designed with android or web-based applications. However, the intention of this design is to provide a Blockchain based app that can be downloaded and used by the organization with no third-party control to meddle with the data. On a blockchain based system, no administrator permission is allowed to editing or deleting data. Someone who inserts an information record on the blockchain will not be able to deny that he is doing the activity. There is an update option to modify attendance when it's needed. However, the modifications are recorded and tracked, just in case it's a fraudulent activity. Attendance is captured using IOT automatically and is entered into the blockchain which makes the data tamper-proof, secure and robust. The privacy of it's users is preserved because the user ids are generated by trusted third party. This data is available for government for Scholarship and other related decision making.

Keywords: IoT, Arduino, NodeMCU, Blockchain, Ethereum, Decentralized Applications, DApp, web3, Smart Contract, IPFS, Infura, Remix.

1. INTRODUCTION

General objective:

• In this thesis project, the innovation consists of develop an IoT smart tool to generate a daily attendance report, avoid data modification, keeping this data history immutable, auditable, and available

for specific people.

Specific objectives:

• Study of biometric access technology.

• Study of blockchain and peer-to-peer technologies.

• Design and build a prototype biometric attendance system

• Design and build an Edge Node, between the device and cloud computing.

• Design and implementation of Smart Contract in Ethereum

• Design a web service for managing blockchain wallet and managing the access to peer-to-peer and blockchain systems.

This project used quantitative experimental methods to collect and analyze the data stored. Each time any employee enters or exits to office or factory, they must "sign the assistance", that is, the system validates the data using ID biometric authentication. [3]. If the data is valid, then it will be stored their clock-in and clock-out time. At the end of every day, a single report can be generated that contains all the employees' working hours. With the use of a Decentralized Applications (DApps) the daily report can be stored inside distributed nodes Inter Planetary File System (IPFS) [4]. The DApps applications interacts directly with blockchain [5] with full replication on every peer in an "untrusted peer-to-peer network". Blockchain transactions are sent to and processed by “random” nodes via Proof of Work and obtained a "hash" with a unique value.

Finally, is obtained a fully trustworthy system that we can trust will not be manipulated. There is no more 'middleman' or centralized authority that holds and controls the information. Every node on the network holds a copy of the ledger, which allows for confirmations, for validity, and for a truly trustless system

IOT and Biometrics

IOT is best served by a set of secure data points; it relies on the integrity of the data sent and received. Those data points share vital information and make important connections that establish relationships and recommendations. Those recommendations often contain sensitive user data–this is where the security of biometrics becomes most important and a key player in strong security for connected devices and retained data. Biometrics provide a secure way to transfer data as well as identify data ports and devices and ensure that they remain secure and their data intact. Biometrics are an optimal security measure, and their continued development will be a key component to creating difficult to breach security protocols. Since the characteristics identified by biometric scanners do not change and are unique to each individual, they make a very secure means of communicating data and creating identifiers for sharing secured data.

Fig 1.1: IOT Fingerprint Module

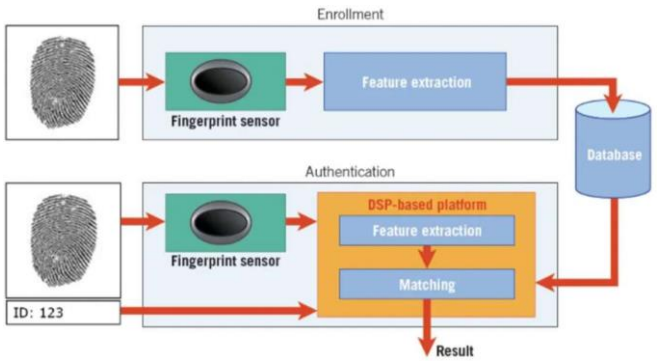

Fig 1.2: Block Diagram of fingerprint processing

1.2 Blockchain Technology

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).

Blocks contain the hash of the previous block, forming a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

The blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.

2. LITERATURE SURVEY

Title: Recording of Student Attendance with Blockchain Technology

Abstract: This research uses qualitative methods using several techniques, such as FGD with experts and literature reviews. The simulation results are carried out directly by comparing the existing system's attendance logs with multichain results. This research produces a product that can be used to implement and become solutions in recording student attendance.

Pros: Collect and store data automatically, Possible to update and maintain attendance records

Cons: Increased equipment expense.

Title: An IOT Based Private Blockchain Framework for Attendance Management

Abstract: The proposed private blockchain framework is implemented in python using Flask as web application framework. The data of students after scanning the QR code is added to the mark attendance block. The registration, subject creation and QR code generation blocks are generated with 0.017 seconds approximately.

Pros: Shows accurate timings, Simple to operate.

Con: System is ineffective if there is no power supply.

Title: STUDENT ATTENDANCE SYSTEM USING BLOCKCHAIN TECHNOLOGY

Abstract: Attendance is very important to every student. To make sure the student's attendance is secure from other third parties, student's attendance system using blockchain technology will be implemented. First one is, to prevent time consuming process for student's attendance. Second one is, to develop a system for student's attendance using blockchain technology. The last one is, to provided better security to this system.

Pros: Possible to update and maintain attendance records, Simple to operate.

Cons: Difficult to maintain and repair, Increased equipment expense.

3. SYSTEM ANALYSIS:

3.1 Objectives

Generally, in many institutions attendance is monitored and marked using conventional systems like android or other similar web applications. Few conventional databases do not have features like checking whether any information has experienced unauthorized

changes or not. In this system when the data is entered into the blockchain, no one is allowed to edit or delete the data. This makes the application transparent and different from other web-based attendance systems as IOT is used to capture the attendance through biometric of the students in the class. Students' poor attendance rate is one of the most challenging problems tackled by the college management today. With the help of this application student's attendance rate can be improved which is also helpful for government to take precise decisions regarding scholarship like schemes for students with transparent data. Using blockchain and some encryption techniques, this application is made secure from any manipulations.

3.2 Methodology

The fingerprint module will collect the fingerprint data from the multiple users and sends it over the internet to the website. The Enrolment of fingerprints is done on the Server and verification is done on the client with the transmission of fingerprint templates over the network. The website is coded in HTML, CSS; JSP has a MySQL database and records of attendance stored in Blockchain. By logging into the website, the student can view all their attendance records. The timestamp of students' attendance is encrypted and stored in the blockchain.

5.1 Architecture Diagram

Web applications are by nature distributed applications, meaning that they are programs that run on more than one computer and communicate through network or server. Specifically, web applications are accessed with a web browser and are popular because of the ease of using the browser as a user client. For the enterprise, software on potentially thousands of client computers is a key reason for their popularity. Web applications are used for web mail, online retail sales, discussion boards, weblogs, online banking, and more. One web application can be accessed and used by millions of people.

Like desktop applications, web applications are made up of many parts and often contain mini programs and some of which have user interfaces. In addition, web applications frequently require an additional markup or scripting language, such as HTML, CSS, or JavaScript programming language.

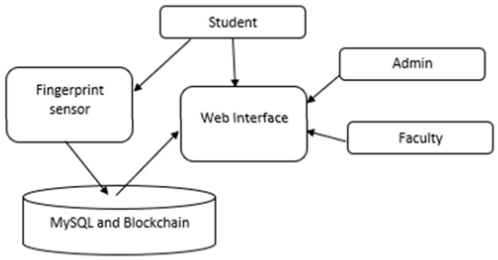

Fig 3.1: Architecture Diagram

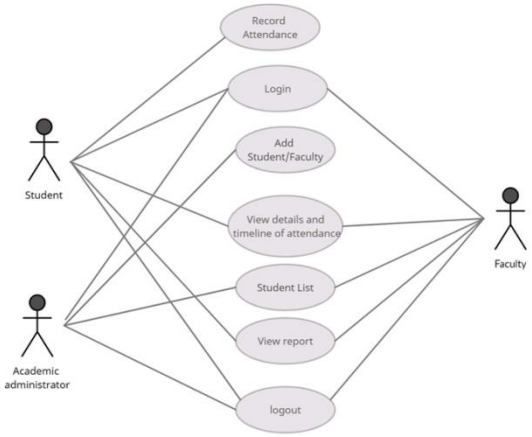

Fig 3.3.1: Use Case Diagram

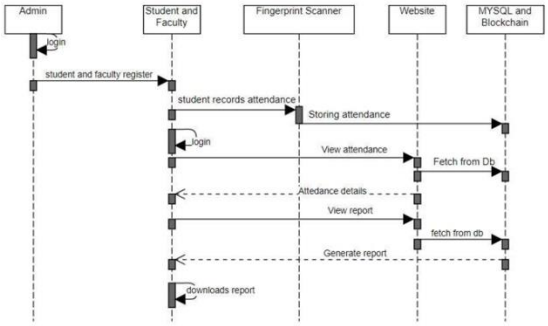

Fig 3.3.2: Sequence Diagram

4. OUTPUT RESULTS:

Test Case Id	Test Scenario	Expected Result	Actual result	Pass/Fail
TC01	Check whether application is working fine after copying url	Index Page should be displayed	As Expected	Pass
TC02	Check whether navbar is working fine	Respective login pages open	As Expected	Pass
TC03	Check whether login is done	Navigated to respective Home pages	As Expected	Pass
TC04	Check whether registration of student is done	Data stored in database	As Expected	Pass
TC05	Check whether registration of faculty is done	Data stored in database	As Expected	Pass
TC06	Check whether attendance is stored in blockchain	Data stored in Blockchain and displayed	As Expected	Pass
TC07	Check whether student can view their attendance	Logged in Student's time records is displayed	As Expected	Pass
TC08	Check whether student can view report	Logged in Student's report is displayed	As Expected	Pass
TC09	Check whether student is able to download report	Print dialog box with report is opened	As Expected	Pass
TC10	Check whether admin can view student list	All registered students details is displayed	As Expected	Pass
TC11	Check whether admin can view all students attendance	All registered students time records are displayed	As Expected	Pass
TC12	Check whether faculty can view student report	Only the given student roll number report is displayed	As Expected	Pass
TC13	Check whether faculty is able to download student report	Print dialog box with report is opened	As Expected	Pass
TC14	Check whether faculty can view all students attendance	All registered students time records are displayed	As Expected	Pass
TC15	Check whether logout is working	Session ends and navigated to Index page	As Expected	Pass

Fig 4.1: Test cases

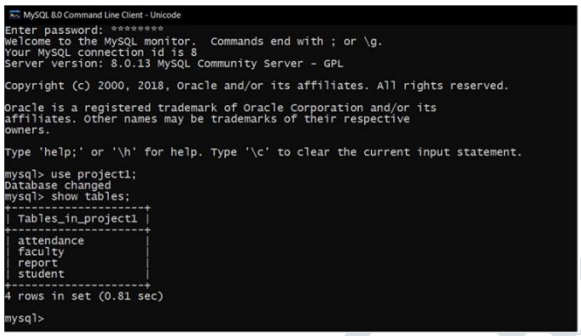

Fig 4.2: Tables in the project

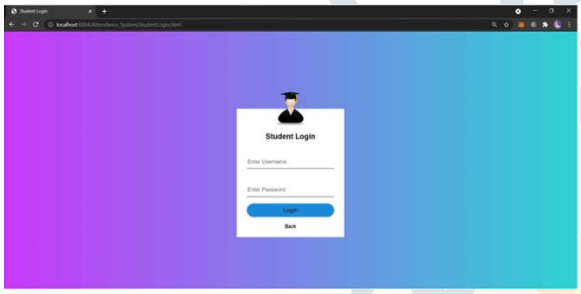

Fig 4.3: Test case showing navbar functionalities working

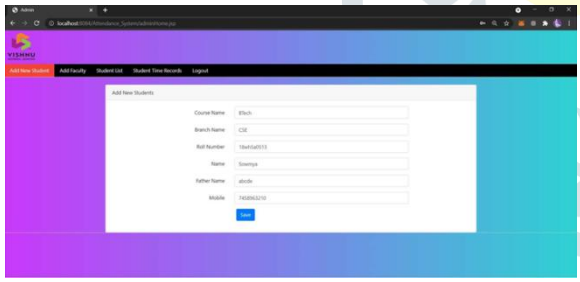

Fig 4.4: Test case showing login is done and navigated to home page

5. CONCLUSION

5.1 Conclusion:

This application helps to automize the attendance system and makes easy to manage all the data. Encryption, decryption and blockchain makes the application very secure. The application has a very user-friendly UI and is made keeping UI and UX into consideration.

The future enhancement of this application is

- To use Ethereum to make the application up to data with the technologies
- To generate automatic weekly and monthly reports

5.2 Future Scope

5.2.1 Hardware

- There is a possibility of forging fingerprints by using glue or latex. This can be avoided by developing a fingerprint reader with improved spoof-print detection. This reader is to be built using RaspiReader. Inside the RaspiReader's 3D-printed housing, LEDs shine light through an acrylic prism, on top of which the user rests their finger. The prism refracts the light so that the two Camera Modules can take images from different angles. The Pi receives these images via a Multi Camera Adapter Module feeding into the CSI port. Collecting two images means the researchers' spoof detection algorithm has more information to work with. (Link for this is mentioned in the references.)

5.2.2 Software

- Certain php scripts can be written to provide more functionality to the users.
- A functionality can be added to provide faculty with a functionality to select a student from a given set of registered students for the course he is offering and then have a look at the to date attendance record.
- Functionality can be added to send a mail to a student if his attendance is below a certain acceptable level. This mail would be informing him about the consequences of having a low attendance.

REFERENCES

[1] W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," Business horizons, vol. 52, no. 4, pp. 357–365, 2009.

[2] A. M. Kaplan and M. Haenlein, "Users of the world, unite! the challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59–68, 2010.

[3] J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue," 2015.

[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.

[5] S. K. N, S. K, and D. K, "On privacy and security in social media a comprehensive study," Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211

[6] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.

[7] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.

[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.