**QUANTUM SECURE BLOCK-CHAIN SYSTEM USING POST-QUANTUM CRYPTOGRAPHY**

|  |  |
| --- | --- |
| **GUIDE** | **STUDENTS NAME** |
| Ms.T.P.Kamatchi | HARSHAL RAM R V (19DC08) |
|  | GOUTHAM BALAJI P S (19DC06) |
|  | KARTHIKEYAN T (19DC11) |

The objective of this project is to create a block-chain system that allows its nodes to perform quantum secure transactions and with quantum secure consensus (proof of work) mechanism. This is made possible by Post Quantum or quantum-resistant cryptography which is cost and time effect method to counter the quantum threats and it is implemented in a classical computer. Mathematical hardness of these cryptographic algorithm makes it secure against quantum attacks by quantum computers running Grover’s and Shor’s algorithms.

There are various types of PQC schemes which are safe against Shor’s and Grover’s algorithms. In this project lattice-based cryptography has been chosen to be implementing in the block-chain system because its most effective against the quantum threats, performs well when implemented in block-chain and its security properties based on worst-case assumptions. The name lattice based cryptography derived from fact that cryptography scheme in this area use the mathematical problems based on lattices. There are trapdoor functions quantum computers cannot crack, however. One such solution is to use a series of lattice operations instead of the traditional multiplication method. A lattice is a multidimensional mathematical group formed from a basis. The basis can be any set of linearly independent vectors whose components are whole integers.

Diagram, letter

Description automatically generated This block-chain system implements lattice-based cryptography in both digital signature and consensus mechanism. This allows a node in the block-chain system to make quantum secure transaction with another node. This is possible by the implementation of lattice based digital signature scheme. To confirm these transactions a lattice-based consensus mechanism is implemented.

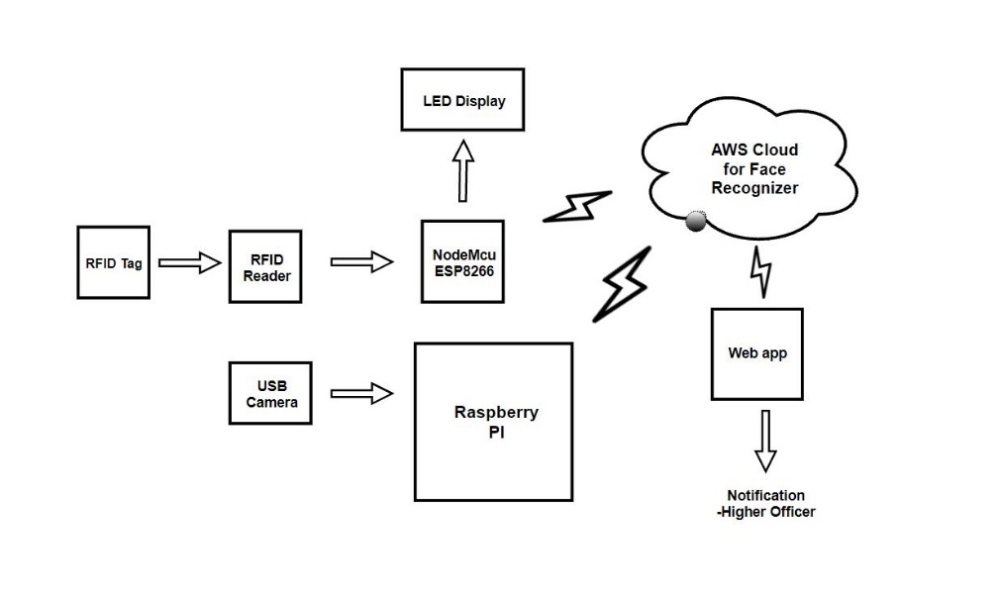
**IOT BASED ATTENDANCE MONITORING SYSTEM**

|  |  |  |
| --- | --- | --- |
| **GUIDE** | **STUDENTS NAME** | |
| Ms.P.ABIRAMI | Bala Ganesh A | (19DC03) |
|  | Nishanth S | (19DC16) |
|  | Vishnu Prasad N | (19DC26) |

In the Fingerprint based existing attendance system, a portable fingerprint device need to be configured with the students fingerprint earlier. Later either during the lecture hours or before, the student needs to record the fingerprint on the configured device to ensure their attendance for the day. The problem with this approach is that during the lecture time it may distract the attention of the students.

Biometrics seem secure on the surface. After all, you’re the only one with your ears, eyes, and fingerprint. But that doesn’t necessarily make it more secure than passwords. A password is inherently private because you are the only one who knows it. Of course hackers can acquire it by brute force attacks or phishing, but generally, people can’t Access it. On the other hand, biometrics are inherently public. Think about it: your ears, eyes, and face are exposed. You reveal your eyes whenever you look at things. With fingerprint recognition you leave fingerprints everywhere you go. With voice recognition, someone is recording your voice. Essentially, there’s easy access to all these identifiers.

Our proposed system uses USB Camera which is connected to the raspberry pi camera slot. Live video stream of students is captured in the class with USB1 camera, Raspberry pi takes those images as input images and sends to the cloud server and we make use of face recognition service to compare the input images with the existing image which is already uploaded in the database. Matched images are detected and attendance is marked with date and time for students present in class in the local data base using MYSQL. Unmatched images are denied. This process is carried out for every period and students are given attendance accordingly. A unique RFID card is given to the faculty, when faculty enters the classroom and swipes the RFID card, the RFID sensor scans and sends the data to the database and displayed on OLED. We also, design a web application for the tracking of their attendance. Admin tracks the attendance of the students and faculty periodically or whenever required by the administration and finds the result. The result is displayed on the monitor screen and stores the validate images in the database. Student attendance will be monitored and if the student is absent for that class then the notification will send to the faculty and parents.

****