Research Topics

1. E-voting system

   This Electronic Voting System has been developed to help eliminate any chance of tampering and improve the reliability and dependability of a voting system. This system consists of two entities: The Admin and The Voter (The User). Once the Voter has logged in to the system using their valid username and password, they can view the upcoming elections and the candidates contesting the election. Users can also view results once the elections have concluded. This system also shows user the elections that they have participated in so far. On the other side of the application, the admin can view the list of candidates contesting, the list of voters, and the list of elections. Since this system maintains the data using blockchain, it is highly dependable and can be easily scanned to check for signs of tampering and malpractice. In this system, the admin is the sole authority to manage elections, candidates and voters. Admin can also view the votes. Admin can also check if any vote is tampered, thus checking and verifying the block. Voter can view Elections and cast their vote, also can view the winner but cannot see the winning ratio or votes etc. The system uses Blockchain technology to create a block of every vote thus protecting its identity.

2.Vendor authentication system

   In this vendor authentication system, there is a card introduced for vendors that is a common card for all companies. Using this card vendors can authenticate themselves as the registered vendors of that company. That is an RFID card which includes all the details of the user and if he/she is registered as a vendor for the company. In order to be more secure this system we would introduce a face detection system as well which authenticates and check whether the user is the same as the RFID-registered user.

3.Vulnerability tracker

   There is government compliance to scan the servers so currently it is scanned by manually those tasks are automated by this system. In this system, the servers' vulnerabilities will be fixed by assigning them to the relevant person in the organization. When it is fixed by the assigned user it will be forwarded to the department that assigned the task. That department will be checked if it fixed by scanning the server then the status will be updated as the vulnerability is fixed if it is still not fixed the status will be not updated. There are some scenarios the assigned user will reject the assigned tasks since it is note related to them. So that tasks must be assigned to a related user again by that assigning department.