**Authentication before Casting Vote using Biometrics**

**Abstract:**

It has always been arduous task for the election commission to conduct free and fair polls in our country, the largest democracy in the world. Crores of rupees have been spent on this to make sure that the elections are riot free. But, now-a-days it has become common for some forces to indulge in rigging which may eventually lead to a result contrary to the actual verdict given by the people. Also, the voters have to show their identity card or voter ID card whenever they go to the polling booth to cast their vote. This is a time consuming process as the person verifying the voters has to check the voter ID card or the identity card with the list he has, confirm it as an authorized card and then allow the voters to poll their votes.

This paper aims to present a new way of verifying people, who are eligible to vote, employing biometrics in order to avoid rigging and to enhance the accuracy and speed of the process. The voters don’t need to carry their ID as their details are already stored in the database in the form of fingerprints.

Biometrics is now one of the most popular, reliable and promising identification technologies. It is extensively deployed in education, healthcare, banking and finance and many more applications. The reasons underlying the popularity of biometrics are obvious: reliability, security, efficiency, and high user acceptance. Unlike other identification techniques, biometrics deals with human identity tightly bound to a specific person. The basic point of these machines is also to examine the fingerprints data of an individual and compare it to a database of other fingerprints. Another important reason fingerprint scanners are used is that, they provide a quick, easy, efficient, and secure measure through which an individual with the proper access privileges can authenticate. First, the print is usually searched for in a database of fingerprints, once it is found it then looks at the print to see what access privileges are associated with the prints and compares them to the access they are trying to gain. As a result, the use of automated fingerprints identification systems that record, store, search, match and identify fingerprints is rapidly expanding. These automated fingerprint identification systems can be integrated with a microcontroller and other peripherals to form an embedded system which is comprehensive electronic authentication machine with fingerprint identification system.

As a pre-poll procedure, a database consisting of the fingerprints of all the eligible voters in a constituency is created. During elections, the voter at the polling booth has to enter his fingerprints. The fingerprint reader will read the details from the tag. This data will then be passed to the controlling unit for the verification. The controller will read the data from the reader and will compare this data with the already existing data. If the data matches with the already stored information, the person is allowed to cast his vote. If the data does not match or in case of repetition a message is displayed on the screen and the person will not be allowed to cast his vote. Also the police station nearby to the election poll booth is informed about the identity of the imposter.