Abstract

Voting is most important phenomenon in democratic world. E-Voting systems are security critical systems based on the analysis of potential vulnerabilities, threats, attacks and other security risks. This thesis aids the formal modeling of security protocols and model checking of E-Voting systems using process algebraic approach CSP and a model checker PAT. We are using NSPK protocol where man-in-the-middle-attack was found, which ensures the authentication property of an E-Voting systems. Authentication refers that no intruder will destroy or replace the vote after an eligible voter casts it. This work will check the authentication of vote (vote does not changed or destroyed).