Abstract

Reham M. Mahmoud Kouta

Proposed Secured Remote E-Voting Model Based on Blind Signature

We proposed a secured e-voting system model by using blind signature. Our proposed model achieved all security requirements which are: (authentication, privacy, integrity, non repetition). Our proposed model depends on these main entities that are involved within the voting processes (voters registration, voting, counting, audit), these entities are: certificate authority, ministry of interior, voter, high committee of elections(investigator), counter) The voter can vote from any remote where with secured data transfer (ballot) by using the blind signature to blinded ballot and then sign it, when it sent to the high committee of elections (investigator) for checking the voter eligibility there is encrypting random value r that attached with the blind ballot, using for removing blind the ballot which is encrypted by counter's public key. The high committee of elections checks the signature of voter and checks that if he eligible voter not. Then remove the voter's digital signature and put his digital signature and then sends to counter party. The counter party checks the signature of high committee of election and extracts the random value r by decrypting with his private key and removing blind the ballot and counts the vote