Though voting can be done using mobile terminals at any places if the wireless network develops further in thefourthcoming days, the additional requirements for security will be required depending on the wireless circumstances. And the way of authentication must be provided more strongly and there should not be coercive voting or exposure of data in the wireless network. Voting is a key way of democracy reflecting the nation’s intention. Therefore, astudy on security technology applied to the electronic voting system should be progressed continuously in the future.

An internet voting protocol is introduced[6]. The proposed internet voting protocol adopts blind signature toprotect the content of the ballot during casting. It is believed that a secure electronic voting system do not only allow all voters to verify the voting result but also avoid ballot buying, the proposed internet voting protocol is verifiable and discourages ballot buying at the same time.Any unauthorized candidate or party can still try to buy ballots during the election.

However, no voter can prove which ballot was cast by him after the declaration of the election result. In other words, ballot buying may still exist, but the ballot buyer cannot be assured that the voter will mark the ballot as the buyer want. Various security attacks in computer networks such as active and passive attacks are proposed[7]. Once the local area networks get connected to Internet, all the attacks exploit the network security breaches. The network security is very complex, difficult to be designed and – more than all - difficult to be assured.

It is easier to prove that a network can be penetrated, than to prove that it is completely sure. Security system is expensive and introduces unpleasant user limitations. The security systemdoes not grow the network performance, but the threats are real and the risk is too big without a proper security policy Reduce

Various papers has been published for online voting systems. Here are the analyses of some of them.

* “**Vote Verification through Open Standard: A Roadmap**” sought to propose a vote verification technique which would able to verify vote against major possible threats and enables all election participants to verify votes. For this purpose, they need to investigate a combination of both technological and procedural solutions
* “**An Architecture for E-Voting Systems Based on Dependable Web Services**” proposed design for e voting systems based on dependable web services. The results got from the analysis of the evaluation of the proposed design, presented that solution, increase the dependability to a great extent.
* “**Ensuring Voters and Candidates’ Confidentiality in E-voting Systems**” proposed an E-voting procedure which ensures voters and candidate’s confidentiality and accuracy. Many issues still exist, for example, when large number of voters cast their ballots at the same time, will it cause denial of service (DOS) in the Internet? How to design an efficient and secure online voting system?
* The proposed deign in paper “**A Study on the Electronic Voting System using blind Signature for Anonymity**” contains that the voting can be done only at the places where the voting places are installed. Though voting can be done using mobile terminals at any places if the wireless network develops further in the forthcoming days, the additional requirements for security will be required depending on the wireless circumstances
* “**A Verifiable Electronic Voting Scheme Over the Internet**” proposed an internet voting protocol. The proposed internet voting protocol adopts blind signature to protect the content of the ballot during casting. As we believe that a secure electronic voting system do not only allow all voters to verify the voting result but also avoid ballot buying, the proposed internet voting protocol is verifiable and discourages ballot buying at the same time. Any unauthorized candidate or party can still try to buy ballots during the election. However, no voter can prove which ballot was cast by him/her after the declaration of the election result. In other words, ballot buying may still exist, but the ballot buyer cannot be assured that the voter will mark the ballot as the buyer want.
* “**Anatomy and Types of Attacks against Computer Networks**” review the various security attacks in computer networks such as active and passive attacks. Once the local area networks get connected to Internet, all the attacks exploit the network security breaches. The network security is very complex, difficult to be designed and – more than all - difficult to be assured. It is easier to prove that a network can be penetrated, than to prove that it is completely sure.