Implementation of Identity Based Encryption in e-Voting System

Siti Rahayu Selamat, RobiahYusof and Kong Pei Rou
Faculty of Information Technology and Communication,
Universiti Teknikal Malaysia Melaka,
Ayer Keroh, Melaka, MALAYSIA
sitirahayu@utem.edu.my, robiah@utem.edu.my

Abstract

This paper explains about the design and implementation of Identity Based Encryption (IBE) in web-based Voting application. IBE is a completely new approach to the problem of encryption which was found on the traditional Public Key Infrastructure. It can be used on any arbitrary string as a public key, enabling data to be protected without the need for certificates and reduction of infrastructure cost due to certificates database maintenance. Protection implemented in this application is a key server that controls the mapping of identities to decryption keys where the key is only one-time pad implementation. By using the IBE technique, authentication and security can be preserved in the web-based Voting application where it provides integrity, authenticity, anonymity and confidentiality in this application.

***Keywords*—Identity Based Encryption (IBE), Public Key Infrastructure (PKI), Public Key Cryptography (PKC), Public Key Generator (PKG), Identity Public Key Cryptography (ID-PKC), web-based Voting application.**

1. Introduction

In modern democratic society, voting is one of the important duties of a citizen. The term voting does not only suggest the public governmental election but it also includes all election under commercial organizations, student councils, board elections, and etc. People was always being discourage to participate because of the aspect of time consuming for presenting themselves to the polling station. Therefore, e-voting which mainly consisted of web-based voting and electronic machine voting is beginning to be widely deployed. However, the controversial issues of deploying the e-voting in a public governmental election has gather much debate from different parties mainly regarding the security and confidential issues of the application. Gartner Inc. has noted that almost 75 percent of attacks are tunneling through web applications [9]. Web application security is a significant privacy and risk compliance concern that remains largely unaddressed.

1.1 Problem Statement

Security is the main issues to be considered when developing an application of web-based voting. Voter integrity, authentication, anonymity and confidentiality were those among the security aspects that will be included in this implementation.

1) Integrity (Completeness)

Completeness can be defined as all votes must be counted correctly and accurately [4]. In a web-based voting application, a voter could not see the flow of the vote they cast, unlike the traditional paper-vote scheme where the vote is put in a locked vote-box. In order to provide the voter confidence towards their vote in terms of few issues such as uncounted vote and vote being tampered, the integrity issue should be implemented during the process of the transmission to the vote server.

2) Authentication (Eligibility)

The web-based application needs to authenticate the voter before the vote is being cast to provide the eligibility service where it refers to only a legal individual should be allowed to vote or participate in the voting process [4]. Based on the current authentication used in web-based voting application, it only depends on the login id and login password. Hence it will expose the system to unauthorized voter to participate in the voting process.

3) Anonymity (Unreusability)

Anonymity or Unreusability is defined as only once voting process per voter is allowed [4]. Hence implementation of unique identity as the authentication

method should be integrated in the system to prevent repeated voter registration.

4) Confidentiality (Privacy)

Confidentiality or Privacy in a voting process can be explained as votes and vote's content secrecy [4]. In web-based voting application, only authorized voter can access the protected voting information.

2. Overview of PKC, IBE and web-based voting application

2.1 Public Key Cryptography (PKC)

Cryptography is the study of "mathematical" systems involving two kinds of security problems: privacy and authentication [3]. To overcome the problems found in the symmetric cryptography, the idea of Public Key Cryptography was first introduced by [3]. In 1978 and 1979, Rivest, Adelman and Shamir published their seminar papers on public key cryptography which explained a practical method of the implementation of Public Key Cryptography, this could be found in [6]. This system differs from the traditional ciphers, it make use of two keys in the process of encryption and decryption. That would be a public key, and a private key.

Based on [3] and [6] on the concept of Public Key Infrastructure, if Alice wishes to encrypt and send a message to Bob, Alice would have to obtain Bob's Public Key and encrypt the message with Bob's Public Key. Thus, the message can only be read by Bob. This is because the decryption on the message can only be done with Bob's Private Key which only Bob knows and no one else. However, this approach has a major weakness. How can Alice be assured that the Public Key she has obtained is indeed Bob's Public Key? To solve this problem, the public key certificate is used. A certificate is issued by a trusted third party called the Certification Authority (CA). With the solution with CA, Bob can present his or her public key to the authority in a secure manner and obtain a certificate. Bob can then publish the certificate. Alice which needs to obtain Bob's public key can obtain the certificate and verify that whether the public key is valid and indeed belongs to Bob. By this, Alice can be assured that the message that she is sending to Bob can only be decrypted and read by Bob and no one else.

According to [5], the maintenance and storage which is needed for the database of certificates and the associated keys has become a difficulty in the traditional PKI. Because of the nature of traditional PKI of using certificates to verify keys, traditional PKI will be inferior in the application of a distributed system where the management of key revocation mechanism is difficult. One of the ways for the traditional PKI to overcome this hurdles is to use a short-lived certificate, and a short-lived certificates will introduce a high maintenance cost for the key and certificate updates in the traditional PKI. However, by using the Identity Based Encryption the problem in which was introduced in traditional PKI would be solved because the certificate is eliminated.

Based on [5], another drawback of the traditional PKI would be the key pair setup on both the sender and receiver that needs to be done before any communication using the key pair could be continued. In traditional PKI, the public key is generated at the same time with the private key. This would mean that in order for A to send an encrypted message to B, B would have to first setup its public key and private key in the system. This drawback is solved by using Identity Based Encryption as the public key for Identity Based Encryption could be generated at a different time with the private key and by anyone who wish to encrypt a message. As a solution to all the problems of certificate in traditional PKI, hence the idea of Identity Based Encryption is presented.

2.2 Identitiy Based Encryption (IBE)

Identity Based Encryption (IBE) is an encryption scheme where the public key is based on an arbitrary string. IBE has remained a scheme which does not have a practical method to implement it since [8] has introduced it. Until recently in a paper, [2] describe an IBE system using the Weil Pairing that solved many of the inefficiencies of previous systems. The system was called "Stanford IBE system". This cryptosystem has chosen cipher text security in the random oracle model assuming an elliptic curve variant of the computational Diffie-Hellman problem. Additionally, the performance of this system is comparable to the performance of ElGamal encryption. Therefore, the Boneh solution is the first practical IBE scheme which involve Setup - this function generates global system parameters and generates a master-key; Extract - this call uses the master-key to generate a private key that corresponds to an arbitrary public key string ID; Encrypt - takes a message and encrypts it using the public key ID; Decrypt - decrypts a message using the corresponding private key.

Identity-Based Encryption is advantageous in key management comparing to the certificate based PKI. In traditional asymmetric mechanisms, the key pair is generated from random information unrelated to the method identifying that key pair within the system [5]. The public key generation in Identity Based Encryption can also be invoked at the different time

with the private key in the system where the public key in traditional PKI could only be generated at the same time when private key is generated.

In Identity Based Encryption, a sender can send a secure message to a receiver just using the receiver's identity information, even before the receiver obtains his private key from the Private Key Generator (PKG). This is very unlikely in the traditional PKI where user must establish their key pair before a sender can send an encrypted message to the receiver. By using the information such as receiver position in an organization, the validity date, and etc, IBE is flexible in the providing the application in public key revocation and delegation of encryption key. IBE accomplishes expiration by specifying a valid time segment during which a public key is valid. For example, When Alice send a mail to Bob, Alice would use the public key consisting of the public identifier and a valid time, such as key: bob@hotmail.com || current-year. In doing so Bob can use his private key during the current year only. Once a year Bob needs to obtain a new private key from the PKG. Hence, we get the effect of annual private key expiration. Note that unlike the existing PKI, Alice does not need to obtain a new certificate from Bob every time Bob refreshes his certificate.

In "Stanford IBE System", [2] describes that IBE achieve the delegation of decryption key by implementing Threshold Key Issuing. This is done by not placing the Master Keys in a single location but rather distributing it to different entities. [1] has concluded that by using Identity Based Encryption, the complexity and cost of managing and establishing the public keys and certificates is significantly reduced. As in conclusion, although research interest in Identity Public Key Cryptography (ID-PKC) is very strong at the moment, it is a relatively new technology in comparison to PKI.

2.3 Web-based Voting application

Web-based Voting is the act of casting a vote using a system that employs internet based protocols [7]. Internet voting has been referred to as the ultimate challenge in network security and data encryption. Web-based voting is inevitability a convenient means for a voter to cast their vote, but the existing web-based application has often fail to provide the needed anonymity and verification which is vital in a voting application. The environment that internet voting operates within create unique security concerns. Vote integrity and confidentiality can be protected while votes are transmitted over the Internet through the use of digital signature and encryption technology [10]. The security requirement of a web-based voting is defined as in [4] are completeness, soundness, privacy, unreusability, eligibility, fairness, and verifiability.

3. Design

The e-Voting system is divided into eight modules which focus on the privacy and authentication as the security requirements of the voting process using Identity Based Encryption. The modules are Voter Registration Module, Voter login Module, Voting Module, Infrared SMS Module, Encryption/Decryption Module, Vote Server Module, PKG Server Module and Vote Tabulation Module.

3.1 Voter registration module

e-Voting System requires the voter to register in order to participate in the election to obtain their authorization. Principles use in the e-Voting System is "one-certificate, one vote". Identity Based Encryption (IBE) is implemented where the usage of certificate is eliminated and replaced by the user's unique identity. This system generate the combination of National Identification Number and email address as the user's unique identity.

3.2 Voter Login Module

Eligible voter will have their registered Login ID and password to log into the system successfully.

3.3 Voting Module

This is the main part of this system where the voter cast their vote. In this module, voter will be able to make their selection and submit the vote to the server by using IBE encryption to secure the transmission.

3.4 Infrared SMS Module

This module is responsible to send confirmation SMS to voter once the vote is confirmed and saved in database. SMS will be sent via infrared using an infrared-enabled mobile phone.

3.5 Encryption/Decryption Module

This module is responsible for all the cryptography function. Vote will be encrypted and decrypted using the function in this module.

3.6 Vote Server Module

The Vote server module is used to keep track of all votes' transaction. If vote transaction exists, this module will call the decryption module to decrypt the vote and save the vote to the database.

3.7 PKG Server Module

This module is responsible for generating key pairs and accommodate key request in the e-Voting System.

3.8 Vote Tabulation Module

The function of this module is to count the encrypted vote which was sent to the vote server. The tabulation must be accurate to ensure completeness in the system. Vote must be counted only once. The encrypted vote which was kept in the vote server can only be decrypted by using the private key of the vote server and will be stored in the database server.

4. Implementation

The implementation of e-Voting system includes IIS version 5.1, Microsoft Access 2003, Java Virtual Machine, and Java Development Kit running on Windows XP. It can be illustrated in Figure 1.

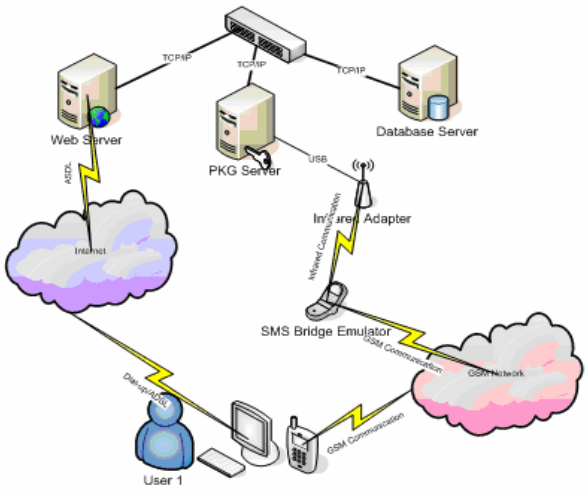

Figure 1 e-Voting System environment

4.1 Server configuration

e-Voting System is a web-based application which is developed using the ASP (Active Server Page) language for the web component. Thus, in order to be able to start writing and viewing ASP web page, the web server is required to be running. Microsoft IIS (Internet Information Service) version 5.1 is installed to the workstation to turn it into a web server. Infrared Adapter must be connected to the server for the confirmation of voting process by sending SMS to the voter.

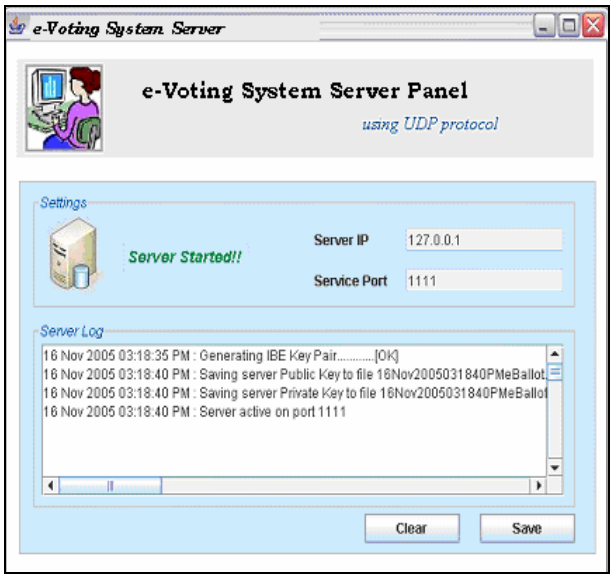

Figure 2 e-Voting System Server Panel

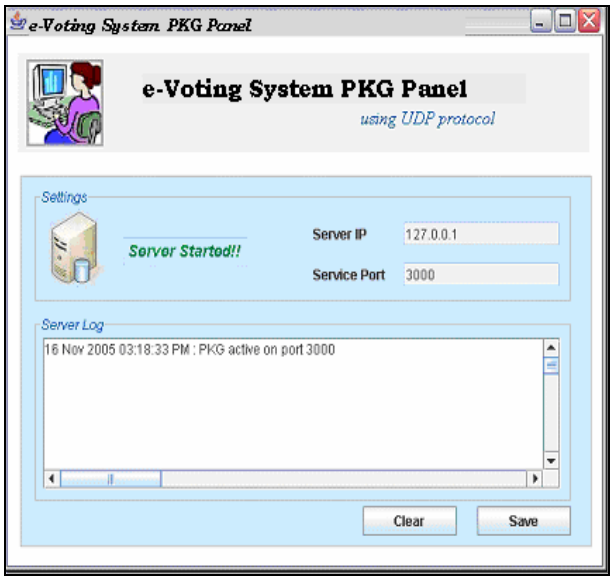

Figure 3 e-Voting System PKG Panel

4.2 Platform configuration

Scripting language using Java is used to develop e-Voting System in the client –server aspect. The core module in E-Voting which is the Identity Based Encryption and Decryption module is coded in java using the technique of Applet and java GUI to embed the module into the webpage.

The whole process of the e-Voting System can be illustrated as shown in Figure 5 below.

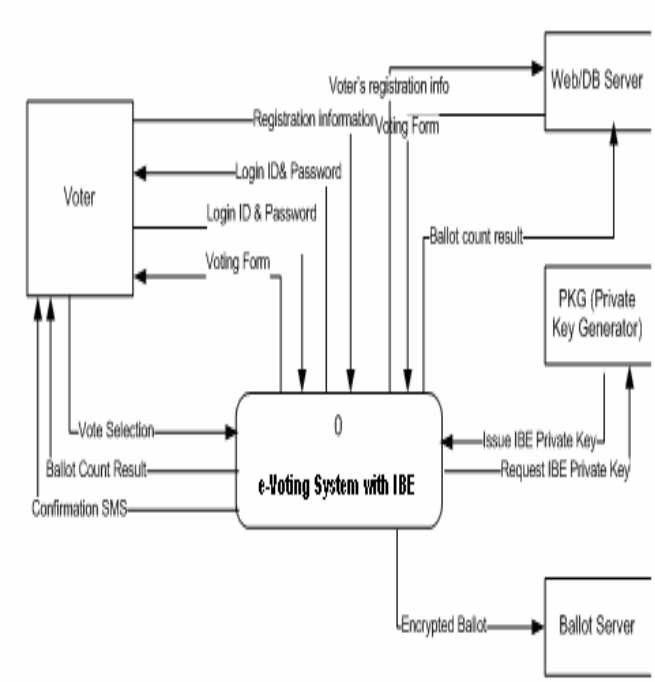

Figure 5 DFD of e-Voting System

5. Conclusion and future works

The implementation of IBE concept based on the Elliptic Curve Cryptography in e-Voting System has provides integrity, authenticity, anonymity and confidentiality in web-based voting application. It is a new approach to the problem of encryption which was found on the traditional Public Key Infrastructure. . It use any arbitrary string as a public key, enabling data to be protected without the need for certificates and reduction of infrastructure cost due to certificates database maintenance. Protection implemented in this system is a key server that controls the mapping of identities to decryption keys. From this result, by eliminating the need for certificates, IBE removes the hurdles of PKI: certificate lookup, lifecycle management, Certificate Revocation Lists, and cross-certification issues. IBE's simplicity enables it to be used in ways PKI could not where IBE can be used to build security systems that are more dynamic, lightweight and scalable.

References

[1] Joonsang Baek et al, "A Survey of Identity Based Encryption", School of Network Computing, Monash University

[2] Boneh and Franklin (2001), "Identity Based Encryption from the Weil Pairing"

[3] W. Diffie and M. Hellman (1976), "New Directions in Cryptography"

[4] Fujioka et al (1992), "A Practical Voting Scheme for Large Scale Election", AsiaCrypt92

[5] Paterson and Price, "A Comparison between Traditional Public Key Infrastructures and Identity-Based Cryptography", Information Security Group, Mathematics Department, University of London

[6] R.L Rivest et al. (1978), "A Method of obtaining Digital Signatures and Public Key Cryptosystems"

[7] Ed Rodriguez (13 Dec 2001), "Security Requirements for Internet Voting System", ACSAC01

[8] A Shamir (1984), "Identity Based Cryptosystem and Signature Schemes"

[9] "Airline Web Sites Seen As Riddled With Security Holes," Computer World, February 4, 2002. (http://www.computerworld.com/securitytopics/security/story/0,10801,67973,00.html)

[10] California Internet Voting Taskforce (2000) "A Report on the Feasibility of Internet Voting "