Arquitectura Basada en un Modelo para Votación sobre Medios Móviles

Sandra I. Bautista Rosales[1], Chadwick Carreto Arellano[2] y Eduardo Bustos Farías[2]

[1] Instituto Politécnico Nacional, Escuela Superior de Cómputo, Ciudad de México, México
sibauros@hotmail.com
[2] Instituto Politécnico Nacional, Escuela Superior de Cómputo, Ciudad de México, México
{ccarretoa, ebustosf}@ipn.mx

Resumen. El avance de la tecnología ha llegado a impactar incluso en la democracia, que involucra la toma de decisiones no solo a nivel político, sustentando así lo que se ha denominado como voto electrónico. Actualmente existen países que ya han implementado este tipo de elecciones en base a modelos de votación electrónica que se apegan a la legislación de cada uno de ellos y que además hacen uso de dispositivos especializados para la emisión y recepción del sufragio. Sin embargo, aunque ya existe una cantidad considerable de avances tecnológicos para la captación y conteo de votos, aún no se ha considerado un modelo que pueda basarse en el uso de dispositivos móviles, que le brinde a los electores la oportunidad de emitir su voto desde cualquier lugar en el que se encuentren y con la certeza de que los principios del voto y las garantías procedimentales serán respetados.

Abstract. The advancement of technology has come to impact even in democracy, which involves decisions not only at the political level, thereby supporting what has been called e-voting. Currently there are countries that have already implemented such choices based on models of electronic voting adhere to the laws of each of them and also make use of specialized devices for transmission and reception of suffrage. However, although there is a considerable amount of technological advances to capture and count, still has not been considered a model that can be based on the use of mobile devices, that gives voters the opportunity to cast their vote from wherever they are located and with the certainty that the principles of the vote, and due process will be respected.

Palabras clave: Voto electrónico, Seguridad, Dispositivos móviles, Autenticación, Firma digital.

Advances in Computer Science
Research in computing Science 81, 2014 pp. 77-90

I Introducción

Con el avance de las nuevas tecnologías de la información y la comunicación, especialmente el Internet, se ha potencializado el flujo de información a niveles sorprendentes que ha llegado a producir cambios sociales en los países que tienen acceso a este tipo de servicios.

Estos cambios han provocado que la democracia evolucione, los procesos electorales se envuelvan en el flujo de información y la toma de decisiones se facilite; y así todo concurre para considerar la inserción del voto electrónico [2].

Existen países que han ido introduciendo el voto electrónico en sus diferentes procesos electorales de acuerdo con diversos modelos de votación que se apegan al sistema político de cada uno de ellos. Sin embargo, todos estos modelos de votación incluyen dispositivos especializados en la recepción del voto y aún no se ha considerado inclinarse por los dispositivos propios de los usuarios, por ejemplo los dispositivos móviles, para emitir el sufragio.

Por otra parte, el avance continuo de los dispositivos móviles y su capacidad de conectividad con las redes inalámbricas les permite a los usuarios estar comunicados en cualquier momento y desde cualquier lugar (anytime-anywhere); lo que nos lleva a uno de los principales retos que tiene que cumplir toda votación electrónica llevada a cabo por este medio, es decir, proveer seguridad al mandar datos por medio del aire, ya que es uno de los canales de propagación más inseguros para transmitir, por lo que es necesario hacer uso de modelos de seguridad adecuados para cubrir esta necesidad [10]. Esta es la razón por la que el presente trabajo de investigación está enfocado en desarrollar una Arquitectura basada en un Modelo de Votación Electrónica sobre Medios Móviles el cual le permitirá al usuario emitir su voto por medio de un proceso de identificación y autentificación a través de su dispositivo móvil, desde cualquier lugar en el que se encuentre, siempre y cuando cuente con una conexión a Internet.

A continuación en la Sección II se brindará un marco teórico donde se enuncian algunos de los conceptos más importantes para el presente trabajo; en la Sección III se plantea el problema en base a los antecedentes abordados en el marco teórico y se define la problemática a resolver; en la sección IV se describe la Arquitectura propuesta para dar solución a la problemática planteada y finalmente en la sección V se presentan las conclusiones y el trabajo a futuro.

II Marco Teórico

Siendo el voto la expresión pública o secreta de una preferencia ante una o más opciones [1], se puede decir que el voto electrónico (VE) tiene el mismo objetivo, con la excepción de que se emplean mecanismos electrónicos para realizarlo por lo que se pueden identificar dos aspectos del mismo [2]:

a) VE en *sentido amplio*: es todo mecanismo de elección en el que se utilicen los medios electrónicos o cualquier tecnología en las distintas etapas del proceso electoral, principalmente el acto efectivo de votar.
b) VE en *sentido estricto*: es el acto preciso en el que el emitente del voto deposita o expresa su voluntad a través de medios electrónicos (urnas electrónicas) o cualquier otra tecnología de recepción de sufragio.

Teniendo en cuenta esta clasificación, el presente trabajo considerará el voto electrónico en el sentido amplio, lo que lleva a definir algunos conceptos básicos para este aspecto.

Existen diversos sistemas de voto electrónico que actualmente ya son utilizados en diferentes países, principalmente los occidentales; de manera general se identifican tres tipos de sistemas principales y un cuarto [2] que va en proceso de adoptarse por ser más reciente. Los sistemas antes mencionados son:

1) Mediante tarjeta perforada. El elector recibe una tarjeta, en la cual debe perforar su opción por medio de un aparato. Este sistema es un tanto problemático, pues la precisión de la perforación depende del usuario y podrían no contarse adecuadamente la perforación de cada tarjeta. Este es un sistema obsoleto, pero aún lo continúan empleando.
2) Mediante un aparato lector. El votante realiza marcas con un bolígrafo en una papeleta, para que después éstas puedan ser introducidas en un aparato lector y se cuente el voto. El votante no entra en contacto directo con la tecnología, pero sí su papeleta.
3) Mediante aparatos de grabación directa. Usan aparatos similares a un cajero automático, el elector establece su preferencia por medio de una pantalla táctil o un teclado. Puede que el mismo aparato registre el voto o que el voto se grabe en un soporte externo. Tras emitir su voto, el votante utiliza su tarjeta a modo de una papeleta tradicional, introduciéndola en una urna, que a su vez será un aparato lector de tarjetas magnéticas, y que realizará el recuento.
4) Voto electrónico remoto. Es el que provee que el votante no deba desplazarse hasta el colegio electoral y pueda emitir su voto a través de la red (puede ser interna o desde cualquier plataforma conectada a Internet).

El modelo sobre el cual se basa la Arquitectura propuesta corresponde a éste último tipo de sistema..

En general la ***seguridad***, se refiere al cumplimiento de los servicios de seguridad que se listan a continuación [3]:

- **Confidencialidad**. Garantiza que la información privada pueda ser accedida únicamente por las entidades autorizadas.

- **Integridad de los datos**. Se refiere a la protección de los datos de tal manera que no puedan ser modificados, destruidos o extraviados de una manera maliciosa o accidental.
- **Autenticación**. Es un servicio relacionado con la identificación de identidades o de datos. La autenticación de una entidad es la confirmación de su identidad, es decir, una comprobación de que es quien dice ser. La autenticación de datos se refiere a la validez de los datos, lo que implica la integridad de los mismos.

- **No rechazo**. Asegura que el remitente de cierta información no pueda rechazar/negar su transmisión o contenido y que el receptor no pueda negar su recepción o contenido.

La ***firma digital*** es un esquema matemático que garantiza la privacidad de la conversación, la integridad de los datos, la autenticidad del mensaje/emisor digital y el no repudio del remitente [4]. También se puede decir que es un método criptográfico que asocia una identidad, ya sea de una persona en particular o de un equipo a un mensaje enviado a través de transmisión por la red.

La ***firma a ciegas*** es una clase de firma digital producida para mensajes que se mantienen ocultos para el signatario y por lo tanto una tercera entidad solicita la firma [5]. Este concepto fue introducido por Chaum con la finalidad de garantizar anonimato en los sistemas de pago electrónico [6], pero actualmente también se le ha dado uso en los sistemas de votación electrónica. Las firmas a ciegas requieren de dos entidades, el usuario quien solicita la firma y el signatario quien firma el mensaje.

De manera general, un sistema de votación electrónica por Internet debe cubrir con todos los requisitos funcionales del proceso electoral, así como los servicios de seguridad necesarios para protegerse de ataques potenciales provenientes de la red. Algunos de los requisitos esenciales son los siguientes [5]:

- *Autenticación*: sólo los votantes incluidos en el padrón electoral serán autorizados para emitir su voto.

- *Anonimato y no coerción*: nadie debe ser capaz de determinar el valor del voto ni de vincularlo con el votante.
- *Unicidad*: ningún votante debe votar más de una sola vez.
- *Verificación y auditoría*: debe ser posible verificar que al final del proceso electoral, todos los votos fueron contados correctamente.

Otros requisitos propuestos por [7] son:

- *Precisión*: Se debe evitar que el voto emitido sea alterado, duplicado o eliminado por cualquier persona. Cada voto legítimo debe ser contabilizado correctamente.

- *Simplicidad*: El proceso de votación debe ser lo más simple posible. En otras palabras, una interfaz de elección electrónica amigable al usuario y que no necesite aprender técnicas complejas y cualquier equipo adicional.

III Planteamiento del Problema

Los avances tecnológicos aunados a las técnicas criptográficas han sido un factor para la paulatina inserción del voto electrónico dentro de los sistemas tradicionales de sufragio. El Internet y diversos dispositivos electrónicos facilitan la captura, recepción y transmisión del voto, ofreciendo así un proceso más cómodo y eficiente para todos los participantes.

No obstante, el nuevo sistema de votación que se deriva del voto electrónico, es decir, el e-voting remoto acarrea también ciertos problemas o riesgos adicionales a los que ya existen en el sistema tradicional. Por ejemplo, la autenticación del usuario, ya que debe de ser identificado para tener los respectivos permisos para votar y a su vez guardar su anonimato al momento de emitir su voto.

Otro problema viene de considerar el Internet como el principal medio de transmisión, pues es necesario implementar los esquemas de seguridad para votaciones electrónicas que ofrezcan seguridad al sistema y confidencialidad a los votantes.

Ya que generalmente el voto es capturado electrónicamente y enviado a una urna electrónica para ser contabilizado al finalizar el periodo de votación, la auditoria se convierte en otro problema, ya que no hay una garantía de que esos votos que van siendo almacenados no sean alterados mientras finaliza la elección.

En la actualidad hay muchos protocolos y esquemas de votación electrónica que van de acuerdo a ciertos modelos de votación. Por ejemplo, "Un esquema verificable del voto electrónico por Internet" [7] proporciona un esbozo de cómo dar seguimiento al proceso de la votación, especificando 4 fases, a saber, fase de registro, autenticación, votación y conteo, además propone cinco entidades participantes: Votantes, Autoridad Certificadora, Centro de autenticación, Centro de supervisión y Centro de conteo, siendo la mayor aportación de este trabajo la verificabilidad.

Otro trabajo titulado "Un Protocolo Seguro de Voto Electrónico para las Elecciones Generales" [8] propone un centro de voto que está compuesto por cuatro pasos con los que navega a través de cinco módulos.

Un tercer protocolo es "Un Mecanismo de Votación Anónima basado en el Protocolo de Intercambio de Claves" [9], éste hace uso de la firma a ciegas y del protocolo de Diffie-Hellman para el intercambio de llaves entre el votante autenticado y el servidor encargado de recibir el mensaje correspondiente al voto. Una de las desventajas de este protocolo es que no permite al votante verificar que su voto haya sido contado correctamente.

En la tabla I podemos observar la comparativa de las diferentes propuestas de modelos y protocolos de votación.

TABLA I.
COMPARATIVA DE POTOCOLOS DE VOTACIÓN ELECTRÓNICA

Protocolos				
Requerimientos	**Protocolo de Liaw [8]**	**Protocolo de Chang-Lee [9]**	**Protocolo de Chun-Ta Li [7]**	**Modelo y Arquitectura propuestos**
Precisión	✓	✓	✓	✓
Simplicidad	X	✓	✓	✓
Apegado a la Ley	✓	✓	✓	✓
Verificabilidad	✓	X	✓	✓
Privacidad	✓	✓	✓	✓
Esquema sobre Internet	✓	✓	✓	✓
Basado en redes inalámbricas	No especifica	No especifica	No especifica	✓
Contemplan dispositivos móviles	X	X	X	✓

IV Arquitectura Propuesta

Con los modelos de votación electrónica que se han propuesto hasta el momento, se puede observar que la mayoría toma en cuenta lugares específicos para que el elector acuda a emitir su voto y/o contemplan dispositivos dedicados a la recepción y conteo del voto. Es verdad que ya existen modelos planteados para un esquema basado en Internet, pero sus descripciones en cuanto al tipo de comunicación que emplearan son muy vagas o casi nulas y dichos modelos se enfocan principalmente en el acto efectivo de votar, dejando de lado las especificaciones y protocolos que se deben de seguir al hacer uso de una red alámbrica o inalámbrica.

En cuanto a la seguridad, la mayor parte de los protocolos propuestos usan relativamente mecanismos sencillos de autenticación, por ejemplo, tarjetas inteligentes y/o una comprobación de que el votante se ha registrado previamente en una base de datos, por lo cual es necesario hacer uso de distintos mecanismos de autenticación para poder brindar confiabilidad en el sistema de votación.

Por otra parte, los modelos de votación electrónica ya propuestos solamente mencionan que las diferentes entidades gubernamentales deben participar y vigilar que el proceso de la votación se realice correctamente, pero dichos modelos no contienen un apartado dedicado a la parte legislativa que es aplicada en cada una de las naciones democráticas.

La importancia de llevar la votación electrónica a un esquema móvil es de vital importancia, ya que brindaría a los votantes un modelo de votación mucho más conveniente para ellos, haciendo uso de las bondades que brindan sus propios dispositivos móviles, es decir, permitirles emitir su voto desde cualquier lugar en dónde se encuentren (y esté disponible una red inalámbrica), sin necesidad de trasladarse a un lugar donde se encuentre algún dispositivos especializado en recibir o contabilizar el voto.

El modelo propuesto es una alternativa que se podría ir adoptando en las diversos países democráticos, ya que además de brindarle beneficios a los votantes al romper con las barreras geográficas, también es conveniente para las entidades encargadas de gestionar todo el proceso de la votación, pues evitaría gastos innecesarios en material (papel, bolígrafos e incluso dispositivos especializados que pueden llegar a ser muy costosos) y la mayor parte de los esfuerzos se podrían enfocar en garantizar la seguridad del sistema y del votante.

El Modelo de Votación Electrónica Móvil propuesto, consta de cuatro capas como se observa en la Fig. 1

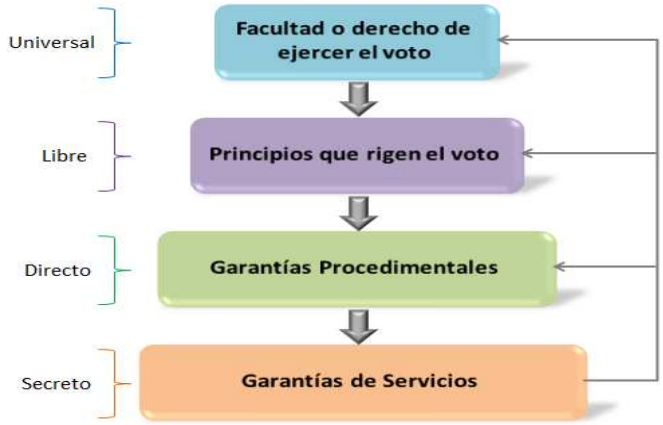

Fig. 1. Modelo propuesto de Votación Electrónica Móvil (Fuente propia)

Cada capa está enfocada a diversos aspectos y fases dentro del proceso de votación, a continuación se describe cada una:

A. ***Facultad o derecho de ejercer el voto***: Se refiere primeramente al proceso de registrar a los votantes que cumplen con los requisitos básicos para poder votar, de esa manera se les otorgará un nombre de usuario y contraseña para después hacer uso de ellos en el proceso de identificación del votante.
B. ***Principios que rigen el voto***: En esta capa se especifican el proceso de autenticación del votante, la cual se realizará por medio de la Firma Electrónica y la implementación del algoritmo de encriptación RSA para autenticarse a través de su dispositivo móvil, además de especificar los principios del voto, como son el sufragio universal, libre, igual y secreto, por mencionar algunos.

C. ***Garantías Procedimentales***: Esta capa involucra la emisión de documentos, certificados, por ejemplo el certificado de autenticación de usuario; también se especifican los aspectos legislativos que regirán el proceso de la votación y se definen las reglas de acuerdo con la legislación del país o de la entidad organizadora de la votación.

D. ***Garantías de Servicios:*** En esta capa se especifican las garantías con las que debe cumplir cada procedimiento especificado dentro de la votación, por ejemplo la transparencia, la verificación de la autenticación, verificación del voto emitido por medio de un certificado digital, la integridad de la información, comunicación segura en el envío de datos a través de la implementación del algoritmo AES, entre otros.

Cada capa tratará de cubrir una de las cuatro características esenciales del voto tradicional que también se deben aplicar al Voto Electrónico sobre medios móviles, como se enlistan a continuación:

- ***Universal***, porque el derecho al voto es inherente a todos los ciudadanos, sin más restricción que cumplir las condiciones que establece la entidad que organiza.
- ***Libre***, porque el ciudadano vota por la opción de su preferencia de manera consciente e informada, sin que persona alguna ejerza presión o lo condicione de alguna manera.
- ***Secreto***, porque el ciudadano emite su voto privado, y ninguna persona puede requerirle información sobre el sentido del mismo.
- ***Directo***, porque el ciudadano acude a votar personalmente.

Para verificar la funcionalidad del Modelo de Votación Electrónica, se ha diseñado una Arquitectura para poder montar un caso de estudio que consiste en una Urna Electrónica Móvil que será implementada sobre dicha Arquitectura que se muestra en la Fig. 2, donde también se aprecia en qué parte de la Arquitectura se implantará cada capa del Modelo propuesto.

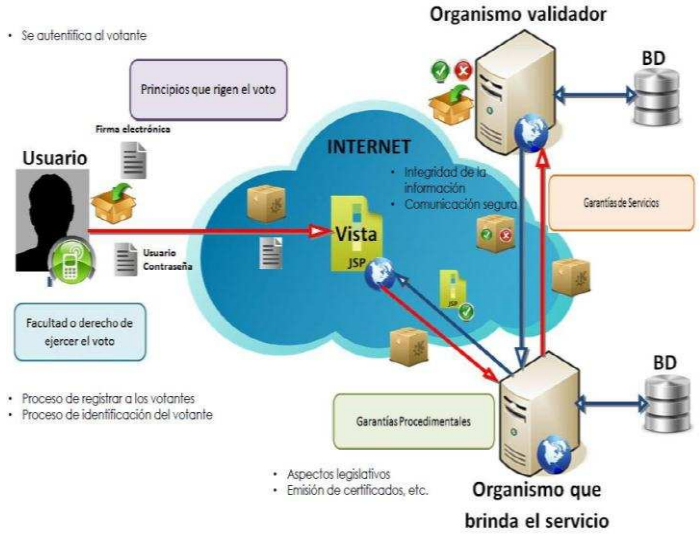

Fig. 2. Descripción de cada capa del Modelo en la Arquitectura propuesta. (Fuente propia)

El flujo de datos que seguirá la Arquitectura será como se describe a continuación y se aprecia gráficamente en la Figura anterior

- El usuario ingresa a la interfaz de la aplicación, si aún no está registrado no podrá acceder a ningún servicio y tendrá que proceder a registrarse.

- Para el registro, el usuario tendrá que mandar un paquete de datos a una vista a través de la red, es decir, debe seleccionar la opción de registrarse, llenar los datos que se le pidan y enviar ese paquete de datos a través de Internet.
- Estos datos serán redireccionados a un servidor, que es el organismo que brinda el servicio con la aplicación de voto electrónico móvil.
- El organismo que brinda la aplicación de voto envía el paquete de datos a otro servidor, que le pertenece al organismo validador de registro, en este caso un administrador se hará cargo de verificar que los registros se realicen de manera correcta.
- El organismo validador del registro revisará los datos del paquete y regresará una respuesta de éxito o fallo en el Registro.
- Dependiendo de la respuesta del organismo validador, será la acción que emita el organismo que brinda la aplicación de votación electrónica móvil y por ende las vistas que se le desplieguen al usuario.

V Caso de Estudio

Las tecnologías que se utilizaron para desarrollar el Caso de Estudio se dividen en tres módulos y se describen a continuación:

1. **Aplicación Móvil**
    a. Sistema Operativo Móvil: Android
    b. Lenguajes de Programación: SDK 4.0 Ice-Creame Sandwich API level 15 debido a las herramientas de seguridad, criptografía y canales seguros de comunicación que se han incluido a partir de esta versión.
    c. Sistema Gestor de Base de Datos: SQLite ya que es el sistema gestor de base de datos que ocupa android y brinda la facilidad de conectarse con MySQL.
2. **Aplicación Web**
    a. Lenguajes de programación
        i. Java SE7U25 JDK: Se eligió este lenguaje debido a la portabilidad que brinda la máquina virtual en diversos sistemas operativos.
        ii. JSF 2.0: (Java Server Faces) Este framework simplifica el desarrollo de interfaces web y permite el uso del modelo vista controlador.

iii. Primefaces 4.0: Es un complemento de código abierto para JSF que ayuda a mejorar la interacción del usuario con la página web.

3. Servicio Web

a. Lenguajes de programación: Java para poder programar el algoritmo de cifrado AES y RSA ya que es el lenguaje provee de algunas librerías para la implementación de estos algoritmos.
b. Sistema Gestor de Base de Datos: MySQL Server porque debido a la compatibilidad que existe entre Java Server Faces y los conectores brindados por Java se facilita la conexión entre estas dos herramientas.

Restricciones del Sistema

- El sistema estará enfocado a smartphones con el sistema operativo android con una versión igual o superior a la 4.0.
- El sistema debe contar con una conexión a internet mediante datos móviles para poder llevar a cabo la votación.
- El sistema deberá de contar con un dispositivo de almacenamiento externo que contenga la información cifrada del usuario.

El sistema requerirá de la validación inicial de usuarios por parte del órgano organizador o regulador del evento.

Cabe aclarar que la inserción del voto electrónico a través de dispositivos móviles debe ser una transición paulatina, usando primeramente este tipo de votación como un apoyo a la votación tradicional mientras se sigue trabajando en todos los elementos que tienen que converger para que la votación sobre medios móviles se pueda implementar en su totalidad.

VI Conclusiones y trabajo a futuro

En el presente trabajo se describió la propuesta y avance de una Arquitectura basada en Modelo de Votación Electrónica sobre Dispositivos Móviles. Como se pudo observar, el Modelo se basa en cuatro capas para cubrir los diferentes aspectos que se deben de considerar en el Voto Electrónico y la Arquitectura nos brinda la conectividad entre cada uno de los componentes. Pretende como aportación el poder

garantizar no solamente la identificación y autenticación del votante, sino también pretende lograr la protección de la identidad del usuario, así como la seguridad de los votos emitidos. Por otro lado, con la implementación del Modelo en la Arquitectura se brindará transparencia a lo largo de todo el proceso y no solamente al finalizar la votación.

Actualmente se está trabajando en pruebas de seguridad del mecanismo de Autenticación de usuarios de la Urna Electrónica Móvil (caso de estudio) y pruebas al canal por donde fluyen los datos, el cual es una parte de un Modelo de Seguridad en Redes Móviles que la firma electrónica del usuario para su funcionamiento [12] y en la aplicación para el usuario en el sistema operativo Android.

Agradecimientos

Los autores del presente trabajo agradecen a ESCOM, CIC, ESIME, COFAA y a la SIP por las facilidades proporcionadas para el desarrollo del presente trabajo.

Referencias

1. Real Academia Española, Diccionario de la lengua española, 22ª ed. 2010, http://lema.rae.es/drae/
2. Téllez Valdés, Julio. El voto electrónico, México, Tribunal Electoral del Poder Judicial de la Federación (2010) http://www.te.gob.mx/documentacion/publicaciones/Temas_selectos/14_voto.pdf
3. F. Rodríguez-Hernríquez, N.A. Saquip, A. Díaz Pérez, C. K. Koc. Cryptographic Algorithms on Reconfigurable Hardware (Signals and Comminication Technology). Springer Verlag, New York, Inc. (2006)
4. Kaur, R. Digital Signature. Guru Nanak Dev University, India. International Conference on Computing Sciences (2012)
5. M. de L. López García. Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales. Centro de Investigación y Estudios Avanzados del Instituto Politécnico Nacional. México (2011)
6. D. Chaum, R. L. Rivest and A. Sherman. Crypto 82 in Advances in Cryptology 1981 to 1997, Vol. 1440 of Lecure Notes in Computer Science, p. 13-19. Springer Berlin (1999)
7. Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai. A verifiableElectronic Voting Scheme over the Internet. Sixth International Conference on Information Technology: New Generations, Las Vegas Nevada (2009)
8. H. T. Liaw. A secure electronic voting protocol for general elections. Computers & Security (2004)
9. C.C. Chang and J. S. Lee. An anonymous voting mechanism based on the key exchange protocol. Computers & Security (2006)
10. Mudhakar Srivatsa. Who is Listening? Security in Wireless Networks. IEEE-International Conference on Signal processing, Communications and Networking, Madras Institute of Technology, Anna University Chennai, India, pp. 167-172 (2008)

11. Gentles, Donovan and Sankaranarayanan. Biometric Secured Mobile Voting. Kingston, Jamaica (2011)
12. Hernández O. Luis E. Modelo de Seguridad para Redes Aplicado a Dispositivos Móviles. Escuela Superior de Cómputo, Instituto Politécnico Nacional (2013)
13. L. Bass, P. Clements, R. Kazman, Software Architecture in Practice, 2nd Edition, Addison Wesley (2003)