UNIVERSIDAD DE COSTA RICA

FACULTAD DE INGENIERÍA

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN E INFORMÁTICA

PI Redes - Sistemas Operativos

CI-0123

Grupo Tronaditas

Profesores:

Luis J. Quesada

Luis Gustavo Esquivel

Ricardo Gang

Proyecto-Etapa 1

Elaborado por:

Daniel Artavia Cordero - B70771

Oscar Navarro Céspedes - B95549

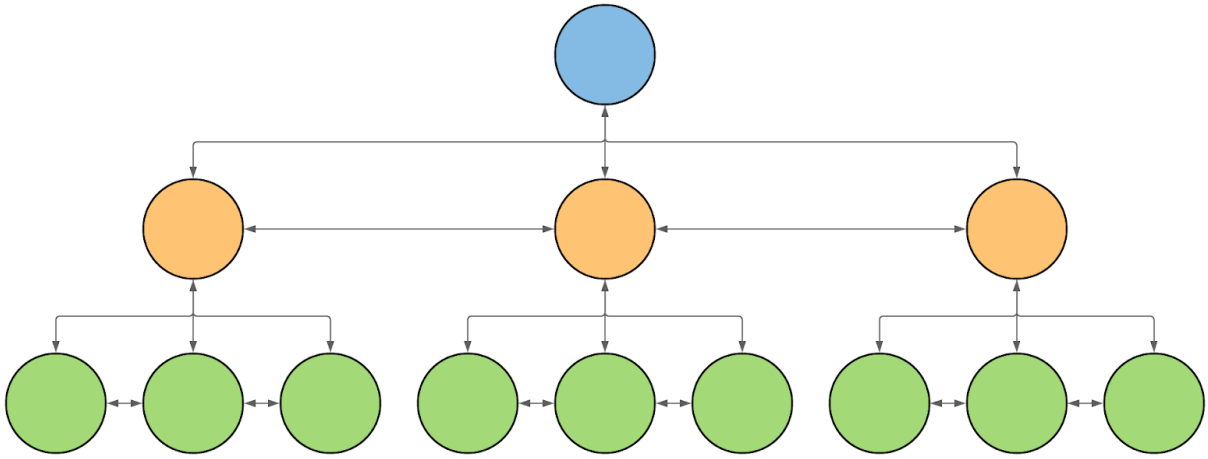
Sebastián González Varela - B93457

Sung Jae Moon - B85176

29 de abril del 202

Modelo jerárquico

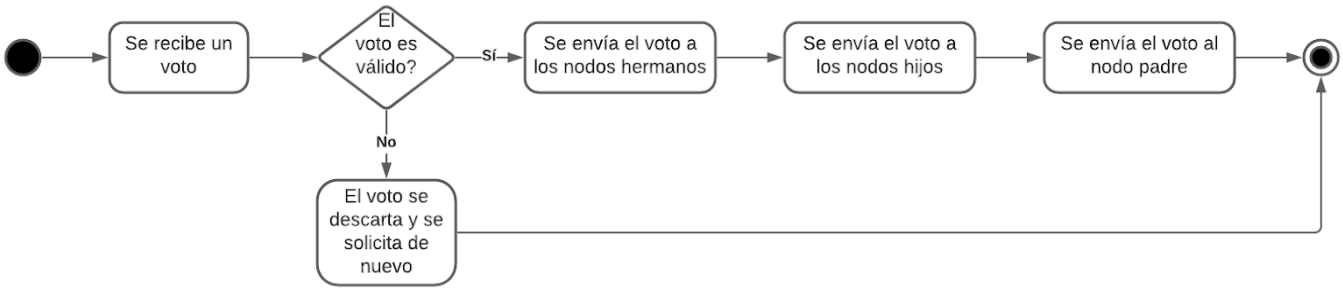
Para solucionar el problema de la votación digital, se propone organizar varias máquinas en un modelo jerarquizado. El nivel inferior de la jerarquía es el que corresponde a las urnas en las que se recolecta el voto del usuario, y el nivel más alto es un servidor o servidores centrales en el Centro de Informática. Los nodos intermedios dependen de cómo se quiera separar el padrón electoral; por ejemplo, se podría dividir por facultades y luego por escuelas, en cuyo caso existirían dos niveles intermedios. La cantidad de niveles intermedios es irrelevante para la implementación ya que todos funcionan de igual manera. La cantidad de niveles intermedios es importante únicamente para la distribución de la carga y fines estadísticos o administrativos.



Ejemplo de modelo jerárquico con 3 niveles. Azul es el nivel superior y verde el nivel inferior. Todos los nodos que sean hijos de un mismo nodo padre estarán conectados entre sí, y con el nodo padre.

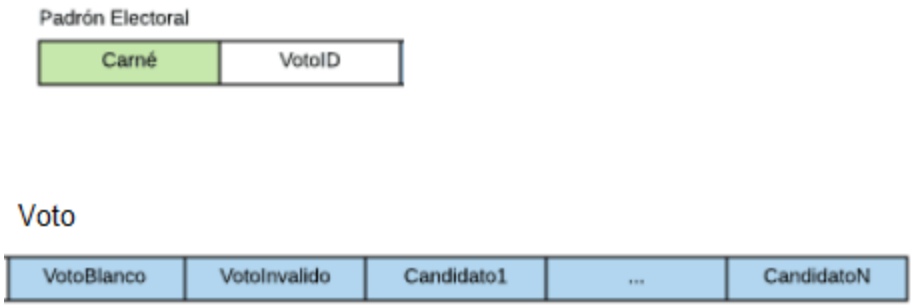
Transmisión de los votos

Para asegurar la integridad de los votos, cada vez que se recibe un voto en una urna, una copia del voto es enviada a cada nodo en la red. Para que un nodo acepte una modificación a un voto es indispensable que una gran mayoría o la totalidad de los demás nodos tengan ese mismo dato. La transmisión de las copias de un voto es primeramente horizontal y posteriormente vertical; es decir, que la urna receptora envía la copia a las demás urnas del centro de votación y luego al servidor de la escuela o facultad, el cual enviará el voto a las otras escuelas o facultades y de ahí será enviada a las urnas de esa otra escuela o facultad. Lo que se busca es tener la mayor cantidad de copias posibles y así poder descartar cualquier copia que se haya intentado modificar, ya sea por terceros o por errores físicos en los dispositivos de almacenamiento o transmisión.



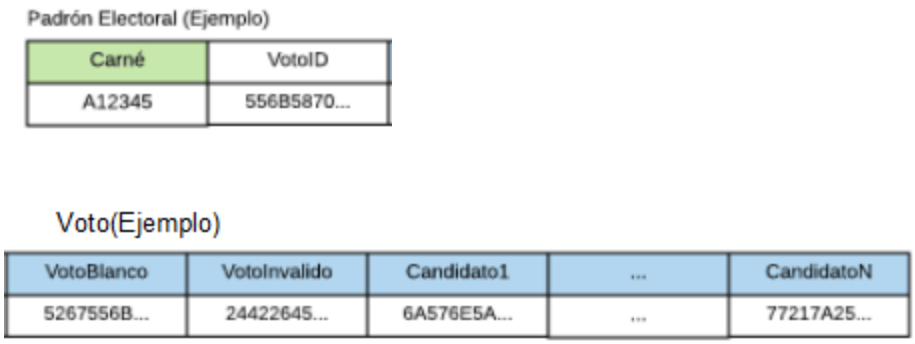
Almacenamiento de los votantes y los candidatos

Para proteger el anonimato de los votantes, se considera importante mantener separado el votante del voto. Es por eso que el voto se puede guardar en un archivo y el padrón electoral en una base de datos. El padrón electoral contiene una lista con la identificación de los estudiantes (número de carné) y el código único generado para cada estudiante en la máquina verificadora.



Diseño lógico de la tabla del padrón electoral y la tabla del voto. En verde, la clave primaria; en celeste, columnas para las claves para los votos.

Las claves para los votos son claves de 1024 bits. *VotoID* debe ser único y generado aleatoriamente; podría usarse una clave de 128 o 256 bits como nombre de archivo, para respetar el largo máximo de nombre de archivo del sistema de archivos. A continuación se muestra un ejemplo de cómo se vería una fila del padrón electoral.



Registro y almacenamiento de los votos

Cuando un usuario emite su voto se crea un archivo con un nombre generado al azar que contiene la información correspondiente del voto, sin ninguna información que lo vincule al usuario que emitió el voto (así se mantiene el voto secreto) .
En el momento que se emite un voto el padrón recibe la información que indica que la persona ya votó, con esto se diferencia entre los estados de voto emitido y voto no emitido de un usuario.
Se envía el archivo con el voto por la red, dado que en cualquier situación en el que algún componente falle se tenga ese respaldo para mitigar contingencias, también se tiene esto para la verificación de los votos, cuando el tiempo límite para las votaciones concluya el sistema cuenta los votos emitidos hasta el momento y anuncia al candidato ganador.

Los votos se almacenan como archivos binarios en el almacenamiento físico de las urnas y servidores, los votos son encriptados para su envío y almacenamiento.

Proceso de recepción de votos

Para registrar el voto de un votante, se deben cumplir ciertos requisitos:

- Que el votante esté inscrito en el padrón
- Que el votante esté inscrito en el centro de votación
- Que el documento de identificación corresponda a la persona que se presenta al centro de votación

Para la validación de los requisitos anteriores, lo recomendable sería que seres humanos capacitados verifiquen la validez del documento de identificación y lo comparen contra una lista de los votantes autorizados en el centro de votación. Sin embargo, para aumentar el nivel de virtualidad del proceso, se podría considerar que el padrón, o parte de este, esté almacenado en una máquina en recepción; el propósito de esta máquina sería escanear el documento de identificación y generar un código que permitiría al votante iniciar sesión en la urna y así acceder a su archivo para registrar su voto.

Lista de Tareas

Se especifica en mayor detalle en la lista de issues de git.

Padrón electoral

- Generador del padrón electoral
- Almacenamiento de votantes y candidatos
- Almacenamiento de votos

Voto

- Recepción de votos
- Contador de votos

Seguridad/validación

- Algoritmos de encriptación y hashing
- Validador de identidad de los votantes/usuario
- Algoritmo de validación de votos

Redes/comunicación

- Comunicación del servidor entre componentes
- Algoritmo de transmisión de votos

Lista de componentes

- Urnas.
- Centros de votación.
- Servidores principales del centro de informática.
- Máquinas verificadoras de algún documento especial o firma digital.
- Encriptación.
- Algoritmo de hasheo.
- Algoritmo de validez de voto
- Algoritmo de transmision de votos
- Padron electoral

Lista de Funcionalidades

- Verificación de identidad en la máquina verificadora o de recepción del centro de votos
- Verificación de que el votante no haya emitido su voto anteriormente
- Verificación de las personas en el Padrón
- Recepción de voto
- Hasheo del voto
- Transmisión del voto
- Conteo de votos
- Emision del Voto
- Interfaz Grafica de Usuario