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

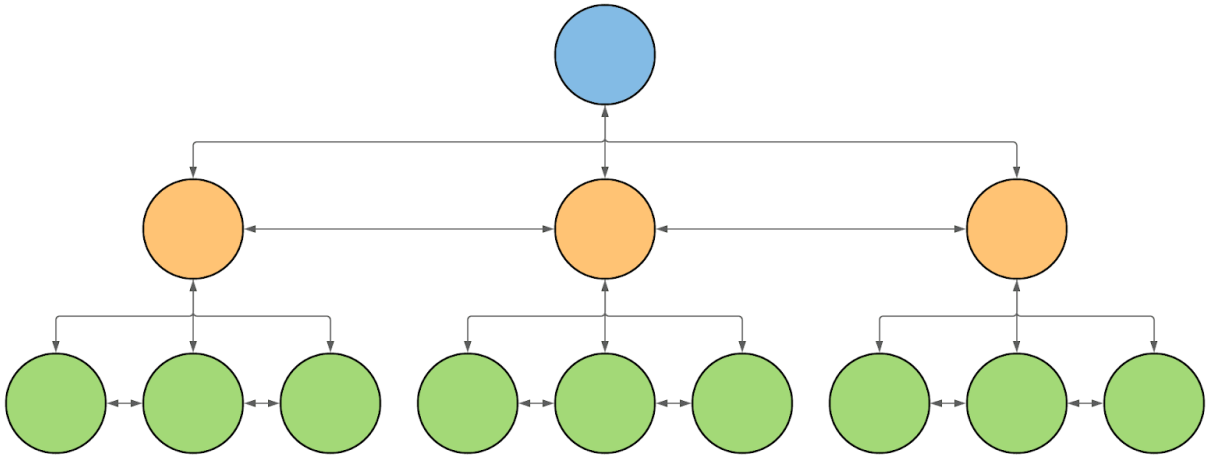
Sebastián González Varela - B93457

Sung Jae Moon - B85176

29 de abril del 202

Modelo jerárquico

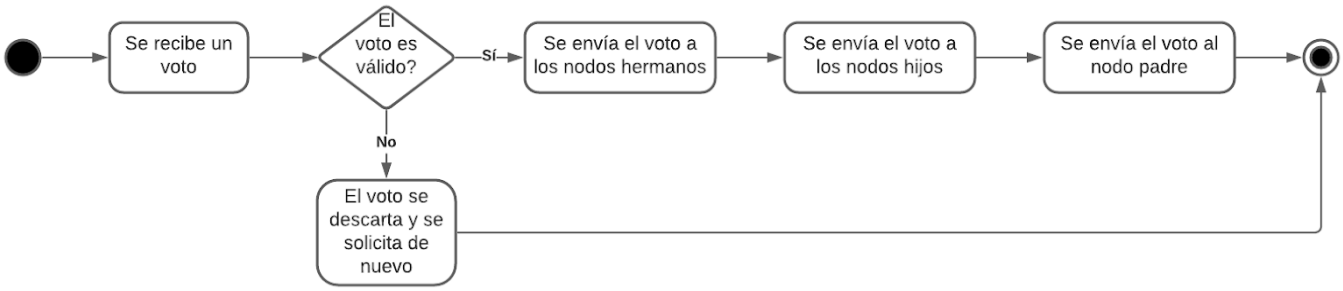
Para solucionar el problema de la votación digital, se propone organizar varias máquinas en un modelo jerarquizado. El nivel inferior de la jerarquía es el que corresponde a las urnas en las que se recolecta el voto del usuario, y el nivel más alto es un servidor o servidores centrales en el Centro de 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

Padrón Electoral

Para proteger el anonimato de los votantes, se considera importante mantener separado el votante del voto. Es por eso que el voto se guarda en un archivo y el padrón electoral en una base de datos. El padrón electoral contiene el nombre del votante, la identificación del votante (número de carné), el centro de votación en el que el estudiante puede votar, el código para acceder a la urna, y si el votante ya ha emitido su voto. La clave del votante es la clave que el usuario debe ingresar en la urna para poder acceder a la papeleta. El votante obtiene la clave de la máquina verificadora.

Padrón Electoral

Nombre	Carne	Centro de Votación	Clave del Votante	Voto emitido

Papeleta Electoral

Cada urna tiene la capacidad de mostrar una papeleta electoral. La papeleta corresponde a una pequeña base de datos que asocia el nombre del candidato con una clave que indica que se votó por dicho candidato.

Papeleta

Nombre del Candidato	Clave de voto

Registro y almacenamiento de los votos

Almacenamiento de los votos

Cuando una persona registrada en el padrón electoral emite su voto, es importante garantizar el anonimato. Es por eso que el voto se almacena en un archivo que tenga un nombre aleatorio e irrepetible. En el archivo del voto se almacena la clave del candidato por el que el votante haya votado.
Para que el nombre del voto sea irrepetible, se considera la opción de agregar como prefijo el ID del centro de votación y el número de urna. El sistema genera una cadena de caracteres alfanuméricos de un largo por definir y los concatena al ID del centro de votación y el número de urna. Por ejemplo, si un usuario vota en el centro de votación FI01, en la urna 06, y el sistema genera la cadena aleatoria “abc123”, el nombre del archivo será FI01_06_abc123.

Ejemplo de registro de un voto

Para este ejemplo, considere el siguiente padrón electoral junto con la papeleta electoral

Padron Electoral

Nombre	Carne	Centro de Votación	Clave del Votante	Voto emitido
Juan	B93457	FI01	AH1738	No

Papeleta Electoral

Nombre del Candidato	Clave de voto
Voto en Blanco	BLANK
Pedro	A1234

Ahora suponga que Juan se presenta al centro de votación FI01 y, tras ingresar su identificación en la máquina verificadora, esta le indica que su clave de votante es AH1738 y que puede proceder a votar en la urna número 06. Con su clave de votante, Juan se dirige a la urna 06, ingresa su clave de votante y decide votar por el candidato Pedro. La urna crea un archivo llamado FI01_06_ABC987 (ABC987 es generado aleatoriamente), y escribe A1234 dentro de ese archivo.

Una vez se haya escrito correctamente el voto en el almacenamiento, se le indica al padrón electoral que Juan ha emitido su voto. El padrón electoral pasaría a tener el siguiente contenido:

Padrón Electoral

Nombre	Carne	Centro de Votación	Clave del Votante	Voto emitido
Juan	B93457	FI01	AH1738	Si

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 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 registrar su voto.
Una vez que se emite el voto,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 y anuncia al candidato ganador.

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