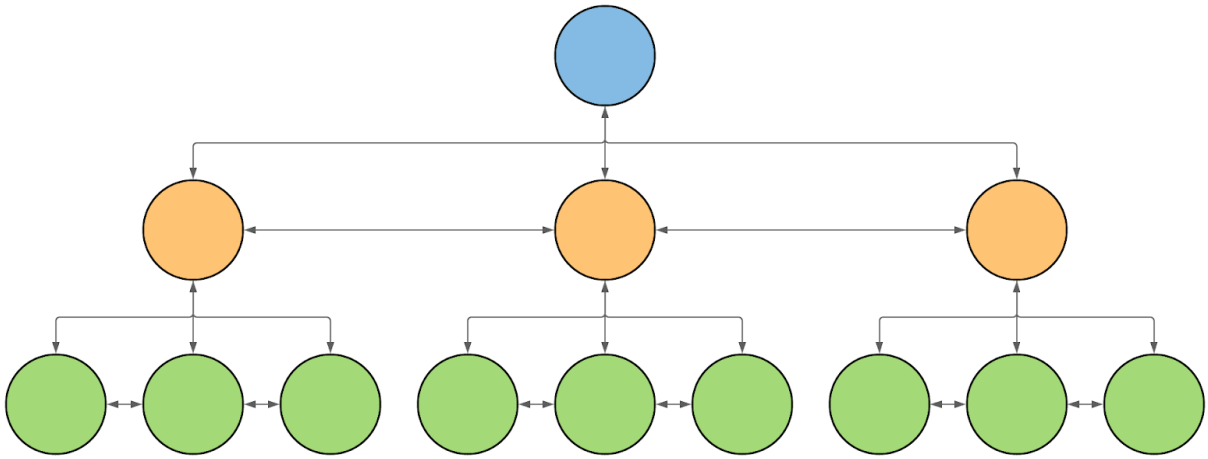
Sistema de votación UCR

Modelo jerárquico

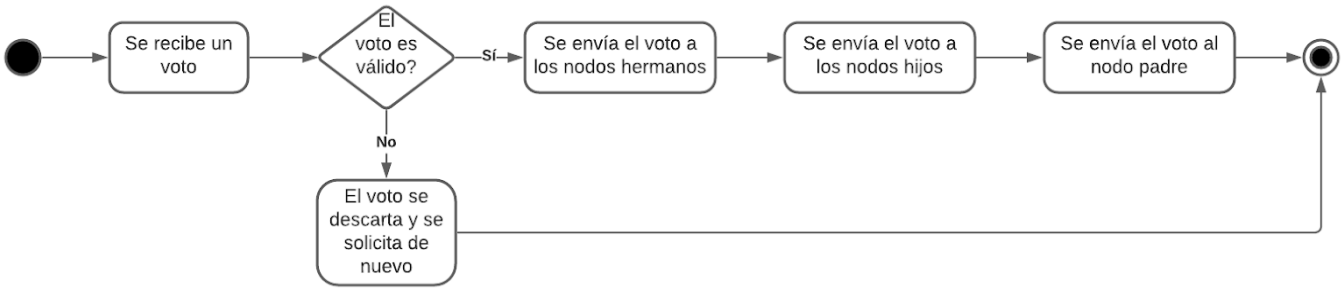
Para solucionar el problema de la votación digital, se propone organizar varias máquinas en un modelo jerarquizado. El nivel inferior de la jerarquía es el que corresponde a las urnas en las que se recolecta el voto del usuario, y el nivel más alto es un servidor o servidores centrales en el Centro de 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), junto con el nombre que recibirá el archivo en el que se almacenará el voto del estudiante. Además, el padrón almacenará una clave diferente para cada estudiante y candidato, para aumentar el nivel de anonimato.

Padrón Electoral

Carné	VotoID	VotoBlanco	VotoInvalido	Candidato1	...	CandidatoN

Diseño lógico de la tabla del padrón electoral. 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.

Padrón Electoral (Ejemplo)

Carné	VotoID	VotoBlanco	VotoInvalido	Candidato1	...	CandidatoN
A12345	556B5870...	5267556B...	24422645...	6A576E5A...	...	77217A25...

Registro y almacenamiento de los votos

Los votos se almacenan como archivos binarios en el almacenamiento físico de las urnas y servidores. Para cada votante se genera un archivo cuyo nombre es el campo *VotoID* asociado al carné del votante. El contenido del archivo es un *hash* del ID del votante y la opción seleccionada para el voto. El contenido inicial del archivo, es decir, cuando el votante no ha votado aún, es un *hash* de la concatenación de todos los valores de la fila del votante en el padrón.

A continuación se muestra un ejemplo de voto para el votante del ejemplo anterior. Suponga que el votante aún no ha votado, entonces el archivo tendría el siguiente contenido:

Una vez el votante haya ejercido su derecho al voto, el archivo podría contener lo siguiente (suma que votó por el candidato 1)

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

- Para los nodos más bajos del modelo se van a utilizar urnas.
- Para los nodos intermedios del modelo se van a utilizar centros de votación.
- Para el nivel más alto del modelo se van a utilizar servidores principales del centro de informática.
- Como mecanismo de autenticación se van a utilizar máquinas verificadoras de algun documento especial o firma digital.
- Para el envío de datos por la red se utilizará encriptación.
- Para el almacenamiento de datos se utilizará un algoritmo de hasheo.
- Para la verificación de la validez de los votos se empleará un algoritmo.
- Para la transmisión de de votos entre nodos se utilizará también un algoritmo.
- 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