Vota-i: votação segura pela Internet

Jônatas Moreira de Carvalho[1], **Jorge Lima de Oliveira Filho**[1], **Jauberth Weyll Abijaude**[1], **Álvaro Vinícius de Souza Coêlho**[1]

[1]Departamento de Engenharias e Computação - DEC
Universidade Estadual de Santa Cruz - UESC
Ilhéus, Bahia

jonatas_carvalhow@live.com,{jlofilho,jauberth,degas}@uesc.br

Abstract. *We present* ***Vota-i****, an Internet-based voting system that uses mobile aplication technologies and end-to-end encryption methods to create an environment in which each elector can perform it's will thru the vote, ensuring safety, privacy and being fully audictable.* ***Vota-i*** *has been successfully used in real elections, complying all these requirements.*

Resumo. *Apresentamos o* ***Vota-i****, sistema de votação pela Internet que utiliza tecnologia de aplicações móveis e criptografia de ponta a ponta para prover um ambiente em que cada eleitor possa exercitar sua vontade através do voto, garantindo segurança, sigilo e sendo plenamente auditável. O* ***Vota-i*** *já tem sido utilizado em eleições reais com sucesso, atendendo a todos estes requisitos.*

1. Introdução

Desde a democracia clássica, definida na Grécia antiga, o processo de escolha pelo voto - e as eleições - tem sido um processo essencial e recorrente [DE AQUINO 2009]. Com efeito, o exercício do voto, e particularmente as eleições, são a principal alternativa para, em sociedades democráticas, se decidir disputas que sejam de interesse coletivo. Todavia, como não deixam de representar uma disputa, é natural e esperado que exista pouca confiança de parte a parte. Daí que os sistemas de votação, desde a antiguidade, precisam se mostrar confiáveis e verificáveis. Com a popularização da computação, o processo de votação foi incorporado em ambientes eletrônicos, comumente referidos como *e-voting*, que também precisaram se mostrar confiáveis e verificáveis. Isto representou uma série de desafios, que foram vencidos ao longo do tempo à medida em que as tecnologias avançavam. Contudo o mesmo avanço tecnológico abriu a fronteira mais recente, e hoje já se desenvolve sistemas de votação pela Internet, referidos como *i-voting*.

Na literatura científica, e mesmo na indústria de software, já existem abordagens funcionais e robustas para *i-voting*, dentre os quais destaca-se o sistema **Helios**™, o sistema mais popular atualmente, mas que ainda deixa algumas lacunas a serem preenchidas em critérios de segurança e auditabilidade. Aqui neste trabalho apresentamos o **Vota-i**, que aborda o processo de *i-voting* mas implementa mecanismos alternativos de segurança do voto e auditabilidade do sistema.

2. *E-Voting* e *I-Voting*

Apesar de genericamente se falar em Votação Eletrônica, na verdade o processo de votação eletrônica pode ser dividido em dois. Um, o mais tradicional, já usado há muitas

décadas, é referido como Votação Eletrônica (*e-voting*). É o processo com um dispositivo computacional programado cuja interface permite que o eleitor preencha uma cédula e, assim, o processo de votação seja executado [Gibson et al. 2016]. Mais recentemente, com a popularização da Internet e dos dispositivos móveis como *Laptops*, *Tablets* e *Smartphones*, surge o conceito de *i-voting*, que é a possibilidade de o eleitor utilizar a conexão pela Internet para depositar seu voto [Górny 2021]. Ambas as abordagens representam importante avanço no processo de votação porque aumentam o nível de segurança, já que a implementação de protocolos de segurança e auditoria em sistemas computacionais tornam o voto inviolável nestes sistemas (veja na Seção 3).

O processo de votação pela Internet traz a vantagem da pervasividade, pois o eleitor não precisa comparecer a um local especifico para exercer o voto; basta que esteja com um dispositivo configurado e conectado à Internet. Isto potencialmente aumenta a participação, conforme menciona Ádrian Albala *et al.*: "*a introdução do i-voto, (...), aumentou a participação entre os eleitores com maior propensão a se abster e, em menor grau, entre os eleitores ocasionais*" [Albala et al. 2023]. Por sua vez, é importante ressaltar que o modelo de votação eletrônica tradicional, *e-voting*, impõe ao eleitor a necessidade de comparecer fisicamente ao local de captação do voto, o que evidentemente pode afetar o comparecimento. Contudo, discute-se se isto é compensado pela segurança, já que o eleitor, uma vez presente a uma mesa de votação, está menos sujeito a constrangimento ou coação, e sua presença física permite que efetivamente se verifique sua identidade. O *i-voting*, por sua própria natureza, não garante nem uma coisa nem outra.

Isto posto, o entendimento que trazemos como premissa é que, no limite da tecnologia atual, tipicamente o *e-voting* se presta mais adequado aos processos eleitorais formais das repúblicas democráticas, como é o caso do Brasil. Enquanto o *i-voting* se mostra mais atraente para votação em comunidades controladas, com alto nível de esclarecimento, bem como para consultas populares de maneira geral. Na UESC, sendo uma universidade e, como tal, uma comunidade tipicamente controlada e com bom nível de esclarecimento, realizamos um total de 16 eleições para departamentos e colegiados, todas por mecanismo de *i-voting*. Todas com sucesso.

3. Trabalhos Correlatos

Já se fala e se usa o termo *e-voting* há quase de 40 anos. Apesar de alguns desafios ainda permanecerem em aberto, é necessário reconhecer avanços importantes tanto no contexto de protocolos de segurança quanto na usabilidade dos sistemas. Em comum se tem o uso de diferentes estratégias de criptografia, embora cada solução apresente suas peculiaridades por conta de tecnologias e objetivos [Gibson et al. 2016]. Ao contrário do que muitas vezes se propaga pelas redes sociais [Kelency 2024], na verdade a quantidade de países que aderem à votação eletretônica é cada vez maior. Dados mais recentes apontam a adoção de *e-voting* em recentes eleições gerais ou regionais na Índia, Brasil, Estônia, Filipinas, Argentina, EUA, Bélgica, Canadá, Japão, México, França e Peru, entre outros [Darmawan 2021].

É importante destacar o pioneirismo do Brasil, que desenvolve eleições com a chamada "Urna eletrônica" desde o século passado (1998), e onde boa parte dos padrões protocolares usados no mundo inteiro foram desenvolvidos, tais como uso de criptografias simétrica e assimétrica e verificação *on the fly* das urnas no processo de Votação Paralela

[Vicari 2024].

A evolução "natural" da votação eletrônica caminha para a votação pela Internet. Esta, porém, apresenta alguns desafios adicionais, por conta da conectividade dos dispositivos e de não haver necessidade de o eleitor comparecer fisicamente a um local para exercer o voto [Stockemer and Wigginton 2024]. Em linhas gerais, os principais desafios são.

1. Autenticação. Na votação por Internet o eleitor é autenticado pelo dispositivo em que ele está conectado: tipicamente um *smartphone* ou um computador pessoal. Garantir que a pessoa que está preenchendo o voto seja realmente o eleitor cadastrado é um desafio complexo que segue em aberto. Some a isto a possibilidade de o voto estar sendo executado sob algum tipo de constrangimento ou coação.
2. Duplicidade do voto. Pode ocorrer de o processo de votação não ser completado (falha de conexão, bateria de dispositivos, etc.), e o eleitor que que iniciar o processo de novo. Isto abre caminho para tentativas de inserir votos em duplicidade.
3. *Man in the middle*. Uma pessoa mal intencionada pode utilizar a conexão com o servidor e enviar um voto se passando por um eleitor cadastrado.
4. Inviolabilidade. O voto deve ser produzido pelo eleitor e armazenado de forma que seja impossível se saber quem o proferiu, mas ao mesmo tempo seja possível se verificar a vontade ali manifestada.
5. Segurança. Não pode ser possível se adulterar um voto depois de emitido, tampouco o resultado de uma eleição

Alguns sistemas de votação pela Internet já existem e estão em uso, com bastante sucesso. Destes, o que mais se destaca mundialmente é o **Helios Voting** [Adida 2008]. O Helios tem sido usado com muito sucesso em diversos contextos eleitorais, e é o sistema que definiu uma série de protocolos utilizados por todos os demais. Implementa técnicas avançadas de criptografia e, a rigor, permite que o seu código seja auditado. Entretanto, nenhum destes processos é simples de ser executado. Para que o código seja auditado, é necessário se proceder à instalação local do sistema, já que não é possível auditar o Helios no seu próprio domínio. Isto desencoraja o procedimento de auditoria e enfraquece a confiança no processo eleitoral. Além disso, o Helios prevê que a cédula seja preenchida numa aplicação web, e dali enviada para o servidor. Isto cria uma fragilidade, pois muitos navegadores são de código aberto - adulteráveis portanto - e não é razoável supor que todos os navegadores de todos os eleitores sejam auditáveis [Heiderich et al. 2012].

Na abordagem do Vota-i desenvolvemos um sistema que pode ser plenamente auditado e que prescinde do navegador para que o eleitor preencha a cédula.

4. O processo eleitoral na UESC

Como na maior parte das universidades públicas brasileiras, a UESC também realiza eleições para a composição das coordenações de seus colegiados de curso, bem como direção de departamento e, naturalmente, para o cargo de reitor. Trata-se de uma comunidade relativamente pequena, contando com aproximadamente 816 professores, 380 servidores e técnicos e 8977 estudantes (dados de 2024), podendo ser classificada como uma comunidade de pessoas com nível educacional considerado alto.

O regimento prevê que os processos eleitorais na UESC sejam conduzidos com voto secreto e facultativo, sendo que em alguns casos se exige quórum mínimo para a

validação do processo eleitoral. Além disso, a UESC disponibiliza para todas as pessoas de sua comunidade um sistema de e-mail corporativo, tornando-se portanto viável para a implementação de sistemas de votação pela Internet, conforme discutido na seção 2.

5. O sistema Vota-i

O Vota-i é um sistema de votação que implementa criptografia de ponta a ponta, garantindo que a cédula preenchida seja criptografada dentro de um processo local no dispositivo do eleitor, antes de ser enviada pela Internet. O sistema foi concebido com três componentes, sendo dois aplicativos para *smartphone* Android™ e um servidor de dados[1].

O **servidor** de dados na versão atual está hospedado no Google Firebase™. Ali se alojam os dados das eleições, bem como o cadastro dos eleitores, além dos processos de autenticação de usuário, envio e recebimento de cédulas para eleitores que desejam votar.

O App **Vota-i Gestão** permite a administração das eleições. Com ele é possível se criar uma eleição com todos os seus parâmetros (veja na Seção 4), inclusive comandar a geração das chaves de criptografia. Também é possível cadastrar eleitores individualmente ou a partir de um arquivo *.csv*. Além disso, os comandos de iniciar e encerrar eleições estão disponíveis, bem como a execução do procedimento de apuração dos resultados, que é descrito na Seção 5.2. Por questões de segurança, nesta versão do sistema o aplicativo de gestão só pode ser instalado diretamente a partir do pacote de instalação.

Finalmente, o aplicativo **Vota-i**, onde o eleitor efetivamente preenche a cédula e manifesta sua vontade. Esta aplicativo faz o processo de autenticação do eleitor juto ao servidor e, em seguida, permite que a votação seja executada de maneira segura, como descrito na Seção 5.1.1. Este aplicativo votação está disponível na plataforma Google Play™.

5.1. Processo de eleição com o Vota-i

Para se executar uma eleição no sistema Vota-i, é necessário a composição do **Colégio Eleitoral**, que é o conjunto de pessoas que estarão aptas a votar. Estas pessoas receberão uma senha gerada aleatoriamente que lhes dará direito de acessar o sistema Vota-i para exercer o voto.

É também necessário que se registre a própria eleição, utilizando o aplicativo de gestão. Nesta etapa, define-se o que constará na cédula eleitoral - as opções que o eleitor vai ter para escolher - e se procede à geração automática de duas chaves de criptografia: uma pública, que será enviada a cada eleitor no momento de votar, e outra, privada, que permanecerá sempre dentro do dispositivo onde foi produzida, e será utilizada para proceder à apuração.

Após iniciado o processo eleitoral, os eleitores procedem normalmente à votação, utilizando o aplicativo **Vota-i** até que, em algum momento, por decisão dos organizadores, a eleição é encerrada. A partir deste momento é possível proceder-se à apuração, com geração de relatório listando o total de votos obtidos, a lista de eleitores que compareceu, bem como a lista dos ausentes. Todas estas funcionalidades estão implementadas no aplicativo de gestão.

[1]Não houve orçamento para o aplicativo ser disponibilizado na versão iOS.

5.1.1. Detalhes Importantes

Para melhor entendimento da maneira como o sistema Vota-i cumpre requisitos discutidos na Seção 3, alguns aspectos do sistema precisam ser melhor apresentados.

Inicialmente, é importante ressaltar que o sistema utiliza um par de chaves de criptografia assimétrica geradas a partir do algoritmo **RSA** [Milanov 2009]. Além disso, a chave privada, que é a única maneira de se apurar o resultado das eleições, **jamais deixa o dispositivo onde é gerada**.

O eleitor que manifesta desejo de votar precisa estar cadastrado no colégio eleitoral, e é autenticado por uma senha que foi enviada para seu e-mail corporativo. Neste momento o servidor verifica se o eleitor efetivamente ainda não depositou seu voto, e então concede ou nega autorização conforme o caso.

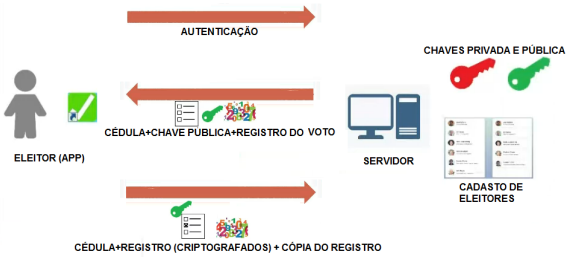

Figura 1. O processo de Votação

Conforme ilustrado na Figura 1, após se identificar, o eleitor recebe no seu aplicativo (de forma transparente para ele) a cédula eleitoral, a chave pública de criptografia e o *identificador de voto*, um número gerado aleatoriamente para identificar o voto, sem associá-lo ao eleitor. Após preencher a cédula e solicitar o envio do voto, esta é criptografada junto com o identificador do voto num único pacote. Este pacote é enviado, junto com outra cópia do identificador do voto, para o servidor. Note que tudo isso ocorre dentro do processo do aplicativo que está executando no dispositivo do eleitor. Tudo isto é feito para atender a critérios de segurança, conforme mostrado nas Seções 5.3, 5.3.1 e 5.3.2.

Ao receber o voto criptografado mais o identificador, o servidor verifica se aquele identificador foi efetivamente gerado, além de checar mais uma vez se o eleitor ainda não votou. Se tudo estiver correto, o voto é armazenado no servidor, que agora registra o comparecimento do eleitor.

5.2. A apuração

Após o encerramento da votação, procede-se à apuração dos resultados. Esta apuração deve ser procedida utilizando-se o aplicativo de gestão, e usando-se o dispositivo em que foi criada a eleição, pois apenas ali está disponível a chave privada necessária para executar este processo.

Conforme ilustrado na Figura 2, o processo de apuração ocorre com o envio, por parte do servidor, de todos os votos criptografados, mais os registros de identificação dos mesmos. Cada um dos votos é descriptografado, e o identificador é verificado como válido (foi gerado pelo servidor naquela eleição). Procede-se, assim, à contabilização de cada um dos votos.

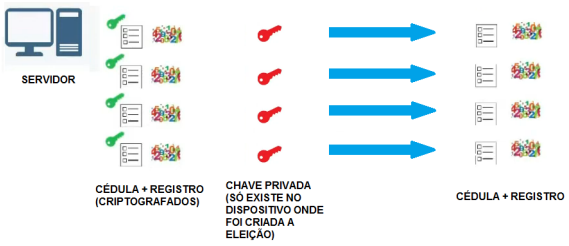

Figura 2. O processo de Apuração

A eleição está terminada, e a partir de agora cada um dos votos pode ser conferido a qualquer momento usando-se a chave pública. Todavia, é impossível associar qualquer voto ao eleitor que o emitiu.

5.3. Aspectos da Segurança no Vota-i

A explanação sobre o processo de eleição com o uso do sistema Vota-i permite que se explore as estratégias pelas quais o sistema, além de proceder à autenticação do eleitor, cumpre os demais requisitos de segurança.

A primeira escolha estratégica é a implementação do voto a partir de um aplicativo (o *Vota-i*), ao invés de utilizar um navegador web. Esta escolha permite que a cédula preenchida pelo eleitor só exista dentro do espaço de processo do aplicativo, saindo dali apenas após completado o processo de criptografia. Como este é um espaço de memória de acesso exclusivo do processo **Vota-i**, e como o aplicativo é controlado (e auditado, veja na seção 5.4), é difícil alguma ação externa consiga violar a integridade ou o sigilo do voto. Além disso, utilizamos o algoritmo RSA com chaves de 1024 bits para criptografar cada cédula preenchida, tornando impossível, na prática, que o voto seja violado. A chave privada, que pode descriptografar os votos, permanece o tempo inteiro armazenado no dispositivo onde está instalado o aplicativo **Vota-i gestão**.

Do lado do servidor, um número gerado aleatoriamente para identificação dos votos permite que o sistema seja imune a ataques *man in the middle* (descrito na Seção 5.5), bem como aumenta a segurança da criptografia.

Há ainda a se considerar que os códigos fontes do aplicativo de votação, do aplicativo de gestão e os dados do servidor são de verificação pública e, após sua compilação, o o código $MD5$ [Gupta et al. 2014] é disponibilizado para todos os interessados e pode ser verificado a qualquer momento. Isto impede que qualquer parte do sistema seja modificada, o que comprometeria a integridade da eleição. Os resultados destas estratégias são discutidos a seguir.

5.3.1. Inviolabilidade do voto

Com o uso de uma chave pública de criptografia, mais o fato de que a cédula preenchida é enviada pelo aplicativo apenas depois de criptografada, qualquer tentativa de alteração de um voto é impossível, pois isto só pode ser feito com acesso à chave privada.

5.3.2. Sigilo do voto

O voto só é enviado depois de criptografado, e não guarda nenhuma relação com o eleitor. Todavia, um mesmo voto, ao ser criptografado, poderia gerar um mesmo resultado que outro. Por exemplo, numa emocionante eleição sobre o melhor achocolatado, dois eleitores diferentes que votassem **Nescau**™ teriam sequencias de dados iguais após a criptografia, já que esta se procedeu sobre cédulas idênticas. Isto gera uma potencial falha na proteção do sigilo do voto, pois a interceptação do voto de um eleitor e a comparação com outro voto cujo conteúdo é conhecido permitiria saber qual foi a escolha do eleitor, caso haja coincidência.

No Vota-i este expediente não funciona, porque a cédula é criptografada **junto com o identificador do voto**, gerando um dado único para cada cédula, ainda que dois eleitores tenham feito a mesma escolha.

5.4. Auditoria

O sistema Vota-i permite auditoria plena da integridade de todos os seus componentes e, além disso, inspirado no processo eleitoral brasileiro, permite que se proceda a eleições paralelas para aferir a honestidade de todo o sistema. As estratégias para garantir estas propriedades são descritas a seguir.

5.4.1. Integridade dos programas

Após a verificação independente do código fonte, e após este ser submetido ao procedimento de votação paralela (veja abaixo), todos os componentes (aplicativos, e servidor) são compilados e o código $MD5$ de cada um deles é disponibilizado publicamente. A partir de então, qualquer tentativa de se alterar os aplicativos ou o servidor se torna inexequível, pois a checagem do respectivo $MD5$ denunciaria isto.

5.4.2. Votação paralela

Inspirado no sistema eleitoral brasileiro, a ideia da votação paralela é submeter o sistema Vota-i a várias votações de demonstração, com a presença e participação de quaisquer interessados.

Para que seja procedida esta votação paralela, cria-se uma eleição e cadastra-se eleitores para ela. Quem desejar participar recebe uma quantidade de eleitores para conduzir no processo de votação. Cada interessado, então, manifesta publicamente os votos que lhe couberam, e preenche, também em público, a cédula correspondente no aplicativo **Vota-i**. Neste momento ele pode executar um voto válido, mas pode também tentar qualquer subterfúgio: anular o voto, votar em branco, tentar votar duas vezes, iniciar a votação em mais de um dispositivo, etc.

Ao final do procedimento o sistema apresenta os resultados, que são previamente conhecidos por todos os participantes, e atesta sua integridade.

5.5. Possíveis ataques

Assim como qualquer sistema de *i-voting*, o Vota-i parte do pressuposto de que cada eleitor é responsável pela segurança de sua própria senha de acesso. Esta senha, porém, não é de livre escolha do eleitor, porque isto abriria a possibilidade de ataques por meio de engenharia social. Desta maneira, a senha de cada eleitor é gerada aleatoriamente pelo sistema Vota-i, e enviada diretamente ao e-mail institucional do eleitor.

5.5.1. Tentativa de violar o voto

Para se violar e alterar um voto depois de criptografado, seria necessário quebrar a criptografia RSA de 1024 bits. No melhor de nosso conhecimento, esta tarefa ainda é impossível na prática[2].

Uma alternativa seria acessar a cédula eleitoral preenchida pelo eleitor **antes** do processo de criptografia. Mas observe que isto obrigaria que o atacante tenha acesso à memória interna do dispositivo (*smartphone* ou similar) e, além disso, conseguir acessar a área protegida do processo do App **Vota-i**. Importante ressaltar que não se trata de destruir os dados, ou o processo do App, mas de acessar a área interna do processo para modificar os dados da cédula eleitoral. E isto teria que ser feito durante o tempo em que o eleitor preenche a cédula. Porque após o seu envio a oportunidade se perde. Isto também torna impossível, na prática, a quebra do sigilo do voto.

5.5.2. Ataque *Man in the Middle* [Bhushan et al. 2017]

O ataque *man in the middle* é a ideia de algum agente mal intencionado se interpor entre o envio e o recebimento de uma mensagem (dado). Num sistema de *i-voting* isto é potencialmente explorável pois a conexão com o servidor pode ser feita por algum aplicativo pirata.

O atacante, porém, não possui os dados de autenticação do eleitor, já que apenas com a senha enviada ao e-mail corporativo isto seria possível. Resta, porém, ao atacante, a possibilidade de criar uma cédula falsa e criptografar com a chave pública, para em seguira a enviar ao servidor, "roubando" assim o voto de algum eleitor.

Ocorre que este expediente não funciona no Vota-i porque cada voto precisa ser enviado junto com um identificador, que é gerado aleatoriamente no servidor, e que é recebido apenas pelo aplicativo que fez a autenticação. Os votos que forem recebidos com identificador inválido são descartados pelo servidor.

6. Resultados

O sistema foi utilizado em 16 eleições no período da Pandemia, envolvendo um total de 988 eleitores[3]. Não se verificou nenhum problema de violação ou exposição de voto. Nenhum ataque com sucesso foi confirmado. A única situação indesejada foi a ausência de quórum mínimo numa das eleições, coisa que o sistema poderia alertar antes de se encerrar a votação. Mas apesar disso, o sistema permite o monitoramento da presença

[2]Se fosse o caso, bastaria gerar chaves maiores

[3]Um colegiado incluiu todos os estudantes do curso no respectivo colégio eleitoral

dos eleitores durante o processo de votação, de forma que o quórum podia ser verificado a qualquer momento. Além do uso em processos eleitorais reais, desenvolvemos experimentos para estressar o sistema e verificar se as estratégias adotadas cumpriam os objetivos.

6.1. Experimentos

Para estes experimentos, colocou-se *smartphones* com o aplicativo **Vota-i** instalado numa rede local, e seus respectivos endereços IPs ficaram públicos. Utilizou-se também PCs com programas "sniffers" para tentativas de quebra de sigilo e violação do voto. Os ataques podiam usar qualquer estratégia, mas, apesar de conseguirem copiar cédulas inteiras na rede, a criptografia não permitiu que o voto fosse violado ou exposto. Além disso, os ataques *man in the middle* tampouco surtiram efeito.

7. Fragilidades observadas

Uma das fragilidades que foram observadas é que alguns eleitores apresentaram resistência à ideia de baixar e instalar o aplicativo de votação em seus dispositivos. A alternativa, que seria instalar um emulador Android™ no Windows™ também sofreu resistência, pois este expediente demanda muito tempo e consome muitos recursos da máquina hospedeira. Além disso, não foi possível encontrar um emulador estável para o ambiente Linux. Finalmente, usuários iOS (Apple ™) não puderam ter sua versão do aplicativo de votação porque o custo do desenvolvimento e da disponibilização na loja de aplicativos não coube no orçamento do projeto.

8. Conclusões e Trabalhos Futuros

Apesar de ter sido utilizado em eleições reais, o **Vota-i** é uma prova de conceito, pois mostra uma alternativa concreta de *i-voting* que implementa soluções que aprofundam a segurança e a auditabilidade do sistema como um todo. Teve muita importância durante a pandemia, onde a votação presencial era simplesmente impraticável. Todavia, com a volta à normalidade, e às reuniões presenciais, implicações regimentais da UESC atualmente impedem sua adoção. Mas há a perspectiva de que estas questões sejam superadas em breve.

Uma das questões que não puderam ser endereçadas neste projeto foi o desenvolvimento de versões *iOS* dos aplicativos de gestão e de votação. Então este é um projeto futuro que obviamente se posa para ser enfrentado. Além disso, atendendo ao incômodo de usuários que preferem não instalar aplicativos em seus dispositivos, surge o desenvolvimento de um *front end* web para captação de voto, embora isto represente uma potencial brecha de segurança - coisa que deverá ser deixada bem clara para o usuário que fizer esta opção.

Outro projeto possível é evoluir o *Vota-i* para um protocolo geral de *i-voting*, definindo um padrão ao qual outros sistemas poderão aderir, e assim alcançar os mesmos níveis de segurança e auditabilidade. Adicionalmente, o desenvolvimento do piloto de uma API permitirá que diferentes aplicativos e sistemas baseados em web possam ser integrados ao processo.

Finalmente, um desafio que já está sendo enfrentado é a implementação de um servidor descentralizado, para que os sistemas de votação possam prescindir de uma autoridade controladora das eleições e dos dados. Conforme estudos recentes apontam, a

implementação dos servidores de votação através da tecnologia *blockchain* retira, da autoridade eleitoral, a prerrogativa de armazenar dados, sendo, portanto, uma alternativa promissora que merce ser explorada também

Referências

Adida, B. (2008). Helios: Web-based open-audit voting. In *USENIX security symposium*, volume 17, pages 335–348.

Albala, A., Borges, A., and Rennó, L. (2023). Voto eletrônico remoto (i-voto) e a pandemia de covid-19: uma proposta de política pública. *Revista de Sociologia e Política*, 31:e014.

Bhushan, B., Sahoo, G., and Rai, A. K. (2017). Man-in-the-middle attack in wireless and computer networking—a review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*, pages 1–6. IEEE.

Darmawan, I. (2021). E-voting adoption in many countries: A literature review. *Asian Journal of Comparative Politics*, 6(4):482–504.

DE AQUINO, R. (2009). *HISTORIA DAS SOCIEDADES: DAS COMUNIDADES PRIMITIVAS AS SOCIEDADES MEDIEVAIS*. AO LIVRO TECNICO.

Gibson, J. P., Krimmer, R., Teague, V., and Pomares, J. (2016). A review of e-voting: the past, present and future. *Annals of Telecommunications*, 71:279–286.

Górny, M. (2021). I-voting–opportunities and threats. conditions for the effective implementation of internet voting on the example of switzerland and estonia. *Przeglad Politologiczny*, (1):133–146.

Gupta, S., Goyal, N., and Aggarwal, K. (2014). A review of comparative study of md5 and ssh security algorithm. *International Journal of Computer Applications*, 104(14).

Heiderich, M., Frosch, T., Niemietz, M., and Schwenk, J. (2012). The bug that made me president a browser-and web-security case study on helios voting. In *E-Voting and Identity: Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers 3*, pages 89–103. Springer.

Kelency, C. (2024). *From the Questioning of the Voting Machines to the Delegitimization of Institutions: The Populist Attacks on Electoral Institutions in Brazil*. PhD thesis, University of Guelph.

Milanov, E. (2009). The rsa algorithm. *RSA laboratories*, pages 1–11.

Stockemer, D. and Wigginton, M. (2024). The (complex) effect of internet voting on turnout: Theoretical and methodological considerations. *Policy & Internet*.

Vicari, I. (2024). A urna eletrônica brasileira: entre controvérsias e desinformação.