Desafios e Soluções em Sistemas de Votação Eletrônica: Um Mapeamento Sistemático

Jéssica I. Pegorini, Natália T. Yada,
Alinne C. C. Souza, Rodrigo T. Pagno, Newton C. Will

Coordenadoria do Curso de Engenharia de Software
Universidade Tecnológica Federal do Paraná (UTFPR)
Caixa Postal 157 – 85.660–000 – Dois Vizinhos – PR – Brasil

{pegorini,yada}@alunos.utfpr.edu.br
{alinnesouza,rodrigopagno,will}@utfpr.edu.br

Abstract. *It is obvious that a fully electronic voting process brings some advantages, such the quick counting of votes and the availability of results, but there are also technological problems to be addressed in order to avoid fraud and failures in the system, ensuring a straightaway process. This paper presents a systematic mapping in electoral security area, which searches for the main information about the protocols used in electronic voting systems, the security measures used and also the vulnerabilities and failures detected in these systems. The results show a convergence of the studies to certain protocols and security measures, besides the main problems to be faced in this area.*

Resumo. *É notório que um processo de votação totalmente eletrônico se traduz em algumas vantagens, como a rápida apuração dos votos e disponibilidade dos resultados, mas também há problemas tecnológicos a serem tratados para evitar fraudes e falhas no sistema, garantindo um processo íntegro. O presente trabalho apresenta um mapeamento sistemático realizado na área da segurança eleitoral, que busca as principais informações sobre os protocolos utilizados em sistemas de votação eletrônica, as medidas de segurança utilizadas e também as vulnerabilidades e falhas detectadas nesses sistemas. Os resultados apontam uma convergência dos estudos a determinados protocolos e medidas de segurança, além dos principais problemas a serem enfrentados nessa área.*

1. Introdução

Tendo em vista que uma eleição é um meio pelo qual a população expressa seu direito à democracia, muitos países vem evoluindo seu processo de votação, adotando sistemas de votação eletrônica, a fim de eliminar fraudes e proteger a privacidade dos eleitores que utilizam esse tipo de votação. Nesse sentido, vários esquemas de votação vem sendo propostos no decorrer dos anos [Zhang et al. 2015].

A votação eletrônica gera maior rapidez e agilidade na apuração dos votos, além de trazer maior acessibilidade para as pessoas que possuem algum tipo de deficiência, pois permite que elas possam exercer seus direitos de maneira independente. Do ponto de vista da segurança, diversos sistemas de votação eletrônica utilizam um processo totalmente auditável e podem eliminar a margem de erro humano. Na teoria, essas são características que asseguram a confiabilidade de um sistema de votação eletrônica [Smartmatic 2018].

No contexto brasileiro, as urnas eletrônicas foram introduzidas no país em 1996, mas só no ano 2000 foi que as eleições se tornaram inteiramente eletrônicas. Embora o sistema de votação do Brasil seja, segundo o Tribunal Superior Eleitoral (TSE), o mais "eficaz e independente sistema de votação do mundo", várias vezes as urnas eletrônicas utilizadas nas eleições brasileiras não passaram pelos testes de auditoria realizados por diversos profissionais da área de tecnologia da informação [Aranha et al. 2018]. Mas vale ressaltar que o Brasil não é o único país a adotar um sistema de votação eletrônica, tampouco o sistema brasileiro é único [Institute for Democracy and Electoral Assistance 2015].

Assim, o presente trabalho tem o intuito de analisar quais são os principais sistemas de votação eletrônica utilizados e propostos ao redor do globo, além das ameaças e contramedidas aplicadas a esses sistemas. Sendo assim, este estudo apresenta um Mapeamento Sistemático realizado na área da segurança eleitoral, que contempla uma breve introdução aos sistemas de votação eletrônica e suas propriedades de segurança na Seção 2, seguido do processo do Mapeamento Sistemático na Seção 3, Análise dos resultados na Seção 4, Discussão na Seção 5 e Conclusões na Seção 6.

2. Fundamentação

Muitas ameaças rondam a segurança de um sistema operacional, podendo colocar em risco os recursos do mesmo. Uma ameaça é um evento que se aproveita de falhas de segurança e explora uma falha específica, podendo resultar em uma vulnerabilidade que causa brechas de segurança do sistema.

Vários países vêm gradativamente substituindo seu tradicional sistema de votação em papel para sistemas eletrônicos, os quais podem ser encontrados em duas categorias diferentes: *Votação eletrônica supervisionada*, que trata-se da votação perante as autoridades eleitorais em locais específicos para realização de eleições, e faz utilização de urnas eletrônicas físicas para a coleta dos votos, e a *Votação Eletrônica Remota*, que é de exclusiva responsabilidade do eleitor, tendo em vista que ela não é supervisionada fisicamente por nenhum tipo de autoridade governamental. Um exemplo desse tipo de votação, é a votação pela Internet [Zissis and Lekkas 2011].

Para que esses novos sistemas de votação sejam seguros, eles devem implementar algumas propriedades de segurança, as quais [Zissis and Lekkas 2011] definem como as mais importantes, e que juntas, podem proteger um sistema de votação eletrônica de diversas ameaças. São elas:

- **Disponibilidade:** O sistema deve ser acessível para uma entidade autorizada poder realizar operações, ou seja, um eleitor autenticado conseguir votar;
- **Confidencialidade:** Apenas as partes autorizadas poderão ter acesso aos dados protegidos, ou seja, o voto do eleitor deve ser privado;
- **Integridade:** Está relacionada à consistência dos dados do sistema, ou seja, o voto de um eleitor deve ser registrado corretamente e não sofrer modificações;
- **Autenticidade:** É a garantia de que os dados são verdadeiros, e que as partes envolvidas são realmente quem elas afirmam ser; e
- **Prestação de contas:** Refere-se à propriedade que garante que as informações se manterão protegidas até o fim do processo de eleição, sem que nenhum atacante consiga modificar essas informações sem ser detectado.

3. Mapeamento Sistemático

Para produzir um conteúdo de qualidade é necessário realizar um levantamento de dados referentes ao campo de pesquisa em que se pretende atuar, e para facilitar o agrupamento desses dados, existem técnicas propostas para auxiliar todo esse processo. A técnica utilizada nesse estudo, é o *Mapeamento Sistemático* (MS), o qual se encontra em conformidade com as diretrizes propostas por [Kitchenham et al. 2010], iniciando com a fase de planejamento, seguindo pela condução e finalizando com a análise de dados.

3.1. Questões de Pesquisa

A primeira fase do MS inclui a formulação de Questões de Pesquisa (QPs) relacionadas ao assunto a ser abordado. As QPs presentes nesse MS foram criadas visando determinar se existem na literatura estudos que registrem quais são os protocolos utilizados em sistemas eleitorais, falhas e vulnerabilidades detectadas, e quais são as medidas de segurança utilizadas por esses sistemas. Para tal, foram criadas as seguintes QPs:

- QP_1: Quais os mecanismos ou protocolos utilizados em sistemas de votação eletrônica?
- QP_2: Quais as medidas de segurança utilizadas em sistemas de votação eletrônica?
- QP_3: Quais as vulnerabilidades e falhas públicas detectadas em sistemas de votação eletrônica?

3.2. Estratégia de Busca

Visando encontrar respostas a essas QPs, foi necessário a montagem de uma *string* de busca, processo esse que combina as palavras chaves e seus sinônimos de cada uma das QPs. Após a criação da *string*, a mesma deve ser calibrada. A calibração consiste em verificar se com a *string* criada os estudos definidos como controle, aqueles estudos principais relacionados com o tema pesquisado, são retornados. Para o contexto desse MS os estudos de [Heiderich et al. 2011], [Zhou et al. 2016], [Pereira and Wallach 2017], [Sebé et al. 2010]. Depois de calibrada a seguinte *string* de busca foi utilizada para a busca por estudos relevantes: *((“security”OR“secure”) AND (“issue”OR “breach”OR “gap”OR “threat”) AND (“e-voting”OR “electronic voting”))*.

As buscas foram conduzidas nas bases: *ACM Digital Library*[1]*, Elsevier (via Science Direct)*[2]*, Engineering Village*[3]*, IEEE Xplore*[4]*, Springer*[5] *e Scopus*[6], de acordo com as diretrizes propostas por [Brereton et al. 2007]. No processo de busca foram considerados apenas os estudos relevantes da última década. Além disso, é importante ressaltar que esse procedimento foi conduzido no período de abril a junho de 2019.

3.3. Critérios de Inclusão e Exclusão

Com base nas QPs descritas na Seção 3.1, foram definidos três Critérios de Inclusão (CI) e oito Critérios de Exclusão (CE), com os quais é possível identificar quais estudos contribuem para as respostas das questões de pesquisa. Os critérios de inclusão concebidos e aplicados são:

[1] *https://dl.acm.org*
[2] *https://www.sciencedirect.com*
[3] *www.engineeringvillage.com*
[4] *www.ieeexplore.com*
[5] *https://link.springer.com*
[6] *www.scopus.com*

- CI_1: estudos primários que apresentam ou propõem uma abordagem, uso ou a aplicação de mecanismos e protocolos utilizados nos sistemas de voto eletrônico;
- CI_2: estudos primários que apresentam ou propõem algum tipo de segurança aplicada a sistemas de votação eletrônica; e
- CI_3: estudos primários que apresentam falhas ou vulnerabilidades detectadas em sistemas de votação eletrônica.

Critérios de exclusão são importantes, pois permitem uma maior precisão na eliminação de estudos considerados não relevantes ao contexto da pesquisa em andamento. Por essa razão, durante a análise dos estudos retornados, todos aqueles que enquadraram-se em ao menos um dos critérios de exclusão abaixo foram descartados. Tais critérios são:

- CE_1: estudos primários que mencionam votação em cédulas de papel, ou sistemas de votação que não são eletrônicos;
- CE_2: estudos primários introdutórios para livros;
- CE_3: estudo primários que não sejam *full paper* ou *short paper* (pôsteres, tutoriais, relatório técnicos, teses e dissertações);
- CE_4: estudos primários que seja uma versão anterior de um estudo mais completo sobre a mesma investigação;
- CE_5: estudos primários que não estejam escritos em inglês ou português;
- CE_6: estudos primários em que a versão completa não é disponível;
- CE_7: estudos primários publicados antes de 2010; e

É importante ressaltar que esses critérios são definidos de acordo com as informações que serão identificadas e sintetizadas relacionadas a área de pesquisa. Por exemplo, no critério CE_5 são considerados somente estudos em inglês e português, pois a primeira é uma língua universal e a segunda é a língua nativa dos autores.

3.4. Extração dos Dados

Para a extração dos dados foram realizados os seguintes passos: *i)* leitura do título e *abstract* de cada estudo; *ii)* leitura da introdução e conclusão de cada estudo; e *iii)* leitura na íntegra de cada estudo. Para cada passo foram aplicados os critérios de inclusão e exclusão, até chegar a um resultado que contou com 44 estudos considerados relevantes, pois abordavam diretamente assuntos que respondiam às QPs definidas anteriormente. A partir da extração dos dados de cada estudo primário incluído, foi possível organizá-los em três categorias de acordo com os assuntos que cada um deles aborda, sendo elas :

- C_1: **Protocolos:** reúne estudos que abordam algum tipo de protocolo de segurança utilizado em sistemas eleitorais;
- C_2: **Medidas de Segurança:** contém os estudos relacionados a medidas de segurança aplicados ao sistemas de votação eletrônica; e
- C_3: **Falhas e Vulnerabilidades:** consiste na seleção dos estudos que apresentam as vulnerabilidades e falhas detectadas em sistemas eletrônicos de votação.

Diante dessas categorias, foram classificado três objetivos principais abordados diretamente por alguns dos estudos incluídos. Esses objetivos são:

- O_1: **Identificação:** engloba a identificação de vulnerabilidades e falhas detectadas em sistemas de votação, medidas de segurança aplicadas aos protocolos já existentes que são utilizados nesses sistemas, e também propõe alguns novos protocolos que implementam medidas de segurança já existentes;

- O_2: **Melhoria:** estudos que propõem melhorias em protocolos ou medidas de segurança aplicadas a sistemas de votação; e
- O_3: **Mitigação:** estudos que abordam formas de aliviar ou suavizar as vulnerabilidades em sistemas de votação.

Após realizar a leitura integral dos estudos, foi possível fazer uma associação de uma ou mais categorias abordadas em cada um dos estudos, conforme será apresentado na Seção 4.

3.5. Condução do Mapeamento Sistemático

Efetuando as consultas nas bases de dados eletrônicas, primeiramente foram retornados 2117 trabalhos, conforme disposto na Tabela 1.

Tabela 1. Quantidade de estudos retornados por base de dados eletrônica.

Base de Dados	Quantidade
ACM Digital Library	49
Elsevier (via Science Direct)	767
Engineering Village	129
IEEE Xplore	47
Springer	840
Scopus	285
Total	**2117**

A Figura 1 apresenta uma visão geral do processo de condução do MS. A partir da busca 2117 estudos foram retornados, dos quais 164 foram excluídos pois se tratavam de estudos duplicados, indexados em mais de uma base de dados. Dos 1953 restantes, 1490 foram descartados por meio da leitura do título e *abstract*, os quais revelaram que os mesmos não eram relevantes ao tema abordado. Na análise da introdução e conclusão dos 463 estudos restantes, apenas 91 foram incluídos para a leitura na íntegra, onde novamente foram excluídos 47, totalizando 44 estudos relevantes incluídos.

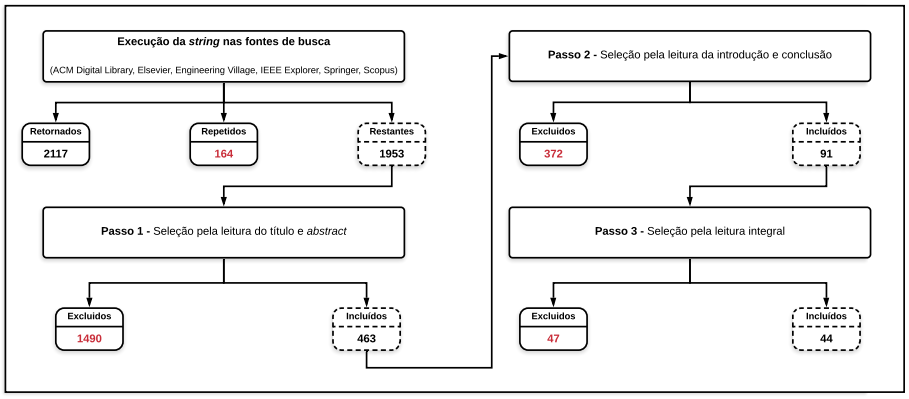

Figura 1. Condução do Mapeamento Sistemático

4. Análise e Síntese dos Resultados

Após a seleção final dos estudos primários, a atividade de extração dos dados foi realizada sobre os 44 estudos incluídos. Nesta etapa foram extraídos os dados principais de cada

estudo, como ano e tipo de publicação, país de origem do autor (considerando o primeiro autor), e classificação dos estudos pelas categorias e objetivos especificadas na Seção 3.4.

Na Figura 2, é apresentado a visão geral dos estudos primários publicados por ano. É possível observar que entre os estudos incluídos, o ano em que concentra-se o maior número de estudos dentre os selecionados, é o ano de 2015, contendo 9 estudos publicados. Já nos anos de 2012 e 2014 não foi selecionado nenhum estudo.

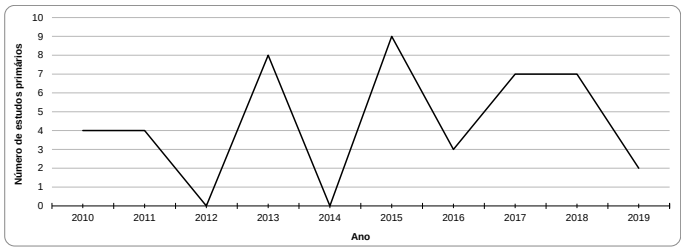

Figura 2. Relação de estudos por ano de publicação

Os estudos também foram analisados em relação ao país de origem do autor principal e tipo de publicação, conforme apresentados nas Figuras 3 e 4. É possível observar que os países com o maior índice de estudos publicados são a Índia e a China, com 6 e 4 estudos respectivamente. Em seguida encontram-se a Coreia do Sul e a Espanha com 3 estudos cada.

Levando em consideração que estudos científicos são publicados e divulgados em diferentes tipos de eventos, 39% dos 44 incluídos foram publicados em periódicos, o que representa um total de 17 estudos. Os outros 27 que representam 61%, foram publicados em conferências. Destaca-se que 10 desses estudos foram publicados em eventos realizados no país de origem do autor principal, o que representa 37% dos 27 estudos. Foi possível observar ainda, que 2 estudos foram publicados em eventos que ocorreram no pais de origem de pelo menos um dos autores, correspondendo à 7,4% dos estudos.

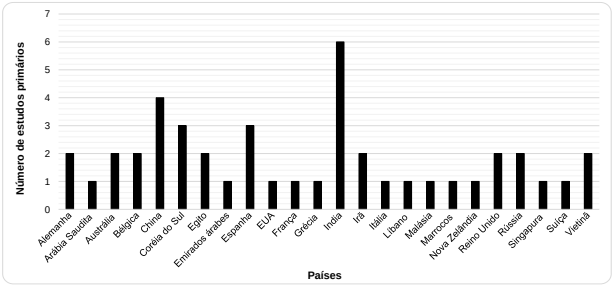

Figura 3. Relação de estudos por país de origem do primeiro autor

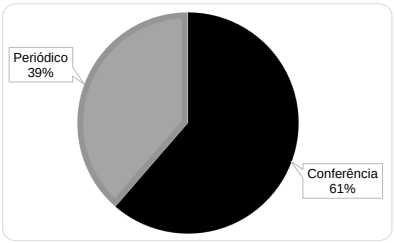

Figura 4. Relação de estudos por tipo de publicação

De acordo com as categorias citadas na Subseção 3.4, na Figura 5 são apresentados o número de estudos que se enquadram em cada uma das categorias e as suas respectivas interseções. Dentre os 44 estudos incluídos, nenhum deles está relacionado somente à C_1, diferente de C_2 e C_3 que apresentaram 10 e 2 estudos, respectivamente. Notou-se que nas interseções entre C_1 e C_2, C_2 e C_3 e C_1 e C_3, foram encontrados respectivamente, 16, 9 e 0 estudos. Já na interseção das três categorias, foram encontrados 6 estudos.

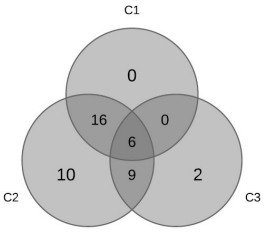

Figura 5. Interseção de estudos por categorias

Como discutido anteriormente, alguns estudos puderam ser classificados em mais de uma categoria, uma vez que os autores relacionavam a existência de um protocolo específico para uma medida de segurança implementada em um sistema de votação, ou algum tipo de vulnerabilidade ou falha de algum protocolo ou medida de segurança proposta.

Na Figura 6 é ilustrado o mapeamento dos estudos relacionando os objetivos com as categorias. Os estudos foram organizados da seguinte forma: no eixo x estão os três objetivos identificados na Seção 3.3, e no eixo y estão as categorias. Os valores que aparecem nas interseções entre os eixos x e y representam o número de estudos que citam o(s) objetivo(s) que foram relacionados a uma determinada categoria. O tamanho de cada circunferência (*bubble*) é representado pelo número de estudos classificados em ambos os pares de categorias.

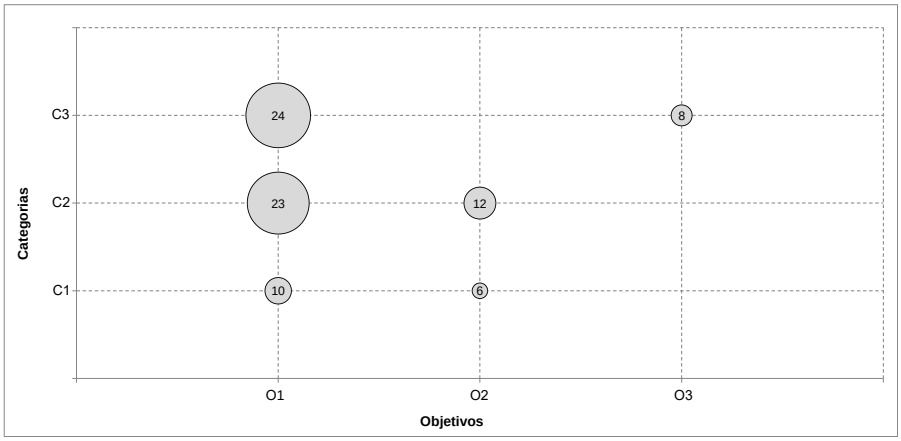

Figura 6. Classificação de estudos por categorias e objetivos

Dentre os 44 estudos incluídos, apenas 10 abordaram a proposta (O_1) de um novo protocolo (C_1), e 6 propuseram melhorias (O_2) em protocolos (C_1) já existentes. Em segundo plano observa-se que 23 estudos identificaram (O_1) o funcionamento de algum tipo de medida de segurança (C_2) existente, enquanto que em 12 desses estudos foram propostas melhorias (O_2) para medidas de segurança (C_2) existentes. Nas falhas e vulnerabilidades (C_3) identificadas (O_1), foram encontrados um total de 24 estudos, com somente 8 apresentando a mitigação (O_3) dessa categoria (C_3). A classificação e categorização integral de todos os estudos analisados pode ser conferida na Tabela 2.

Tabela 2. Tabela geral da classificação dos estudos incluídos

Estudos primários	Q1: Protocolo	Q2: Medidas de Segurança	Q3:		E-voting
			Falhas	Vulnerabilidades	
[Jin et al. 2019]	Protocolo de Autenticação negável Heterogênia - HDA	Autenticação Verificação em Lote	-	-	Votação Eletrônica Remota
[Gurubasavanna et al. 2018]	-	Autenticação Biométrica Captura de Face	-	-	Votação Eletrônica Supervisionada
[Bistarelli et al. 2019]	-	Bitcoin	-	-	Votação Eletrônica Remota
		Multchain	-	-	
[Nassar et al. 2018]	Protocolo de Contagem de Votos	Criptografia Homomórfica de Paillier	Negação de Serviço	- Servidor de Contagem de votos não confiável - Intromissão da Rede	Votação Eletrônica Remota
[Babenko and Pisarev 2018]	Protocolo Descrito na Linguagem CAS+	- Autenticação das partes, - Sigilo de Dados - Proteção contra ataques de repetição	-	-	Votação Eletrônica Supervisionada
[Saqib et al. 2018]	Protocolo baseado em Assinatura Cega	Biometria	-	-	Votação Eletrônica Remota
[Yu et al. 2018]	-	- Blockchaim - Criptografia Homomórfica	-	-	Votação Eletrônica Remota
[Zhu et al. 2018]	-	- Blockchaim - Assinatura Cega - Assinatura de Anel	-	-	Votação Eletrônica Remota
[Lakshmi and Kalpana 2018]	-	- Identificação Exclusiva - (AADHAR) - Biometria	-	-	Votação Eletrônica Supervisionada
[Haines and Boyen 2016]	- Criptografia Híbrida - Recriptografia	Produção de recibo com assinatura falsa	-	-	Votação Eletrônica Remota
[Pereira and Wallach 2017]	-	Verificação Ponta-a-ponta	Modificação do Hash dos Votos	Ataque de choque em máquinas trapaceiras	Votação Eletrônica Supervisionada
[Hsiao et al. 2017]	-	- Criptografia de Curva Elíptica - Criptografia Assimétrica - Função Hash - Assinatura de Anel	-	-	Votação Eletrônica Remota
[AboSamra et al. 2017]	Protocolo Baseado no conceito do Prêt-à-Voter	- Criptografia de chave Simétrica - Criptografia de Chave pública	-	-	Votação Eletrônica Supervisionada
[Kate and Katti 2016]	-	- Algoritmo de criptografia AES - Criptografia Visual	-	-	Votação Eletrônica Remota
[Kumar et al. 2017]	Protocolo ID-BS	- Assinatura cega de Bodyreva - Assinatura baseada em identidade de Chon-Cheon	-	-	Votação Eletrônica Remota
[Shakiba et al. 2017]	Protocolo ESIV	- JavaCard3 - Criptografia de Chave Pública	-	-	Votação Eletrônica Remota
[Kiayias et al. 2017]	TPKE	- Esquema de Compartilhamento Secreto Verificável	Quebra da Privacidade do Eleitor	Suscetível ao ataque MITM	Votação Eletrônica Remota
[Babenko et al. 2017]	-	- Criptografia Simétrica - Gost - Função Hash	Qualquer pessoa pode votar	- Vulnerabilidade Humana Influenciar legalmente o resultado das eleições - Identificação do Usuário	Votação Eletrônica Supervisionada
[Zhou et al. 2016]	MVP	DRMM	-	-	Votação Eletrônica Supervisionada
[Chang et al. 2015]	Apollo	- Criptografia de chave Assimétrica Criptografia de chave Simétrica		Perda de privacidade do Eleitor	Votação Eletrônica Remota
[Will et al. 2015]	-	- Criptografia Homomórfica - Agentes móveis	-	Agentes móveisnão é tão robusto quanto as exigências do Governo	Votação Eletrônica Remota
[Dossogne and Lafitte 2015]	Protocolo de Auto-Cálculo	- Criptografia de Chave pública homomórfica - Criptografia de Paillier - Criptografia ElGamal	-	-	Votação Eletrônica Remota
[Zhang et al. 2015]	Kerberos	- Criptografia de Chave Simétrica - Assinatura Cega	Negação de Serviço	-	Votação Eletrônica Remoto
[Tornos et al. 2015]	Protocolo de Votação Portátil	- Assinatura de Anel -Criptografia de Chave Pública PKB	-	-	Votação Eletrônica Remota
[Kiayias et al. 2015]	TPKE	- Criptografia de chaves Publicas -Benaloh challenge	-	Suscetível ao ataque MITM	Votação Eletrônica Remoto
[Mohammadpourfard et al. 2015]	FOO	- Criptografia RSA - JavaCard3	-	-	Votação Eletrônica Remota
[Rura et al. 2015]	-	- Criptografia Visual - Sistema Criptográfico de Decriptação - Esteganografia	- Ataque Dos - Ataque de Abstenção Forçada	Incoercibilidade	Votação Eletrônica Remota
[Kartit et al. 2015]	-	- Criptografia ElGamal - Criptografia Homomórfica RSA	-	-	Votação Eletrônica Remota
[Huarte et al. 2013]	Protocolo do Canal Anônimo	- Assinatura Cega - SmartCards - Inspeção NVP - Proteção a prova de Voto	-	-	Votação Eletrônica Remota
[Srinivasan et al. 2013]	TPKE	TCE - Criptografia controlada por Token	Ataque de Enchimento de cédulas	-	Votação Eletrônica Remota
[Kim et al. 2013]	-	- Assinatura Cega - Criptografia Independente - Compartilhamento Secreto	-	-	Votação Eletrônica Supervisionada
[Hussien and Aboelnaga 2013]	-	- Assinatura Cega baseada em RSA - Criptografia Homomórfica	-	-	Votação Eletrônica Remota
[Khelifi et al. 2013]	-	- Assinatura cega - Assinatura de Anel - Comprometimento de Bits	Falhas humanas	-	Votação Eletrônica Remota
[Nguyen and Dang 2013b]	Protocolo livre de Colusão	-Assinatura Cega - Criptossistema de Chave Simétrica	-	-	Votação Eletrônica Remota
[Nguyen and Dang 2013a]	Protocolo de Votação pela Internet	-Assinatura Cega - Cédulas Dinâmicas - Criptossistema de Chave Simétrica	-	-	Votação Eletrônica Remota
[Heiderich et al. 2011]	-	-	Invasor interfere em um processo de votação sem deixar rastros Extração de dados via CSS	- Controle remoto de localização - Não utiliza cabeçalho HTTP	Votação Eletrônica Remota
[Olembo et al. 2011]	-	Autenticação baseada em Segredo Token de Autenticação	-	Softwares mal-intencionados	Votação Eletrônica Remota
[Cortier and Smyth 2013]	-	Remoção de Cédulas Duplicadas	Helios permite que o voto do eleitor seja revelado	-	Votação Eletrônica Remota
[Lavanya 2011]	-	-	- Ataque de roubo de votos - DOS	-	Votação Eletrônica Supervisionada
[Peng 2011]	-	Criptografia de Rede Mista	Ataque de Relação em rede mista	-	Votação Eletrônica Remota
[Lee et al. 2010]	-	- Autenticação - Encriptação - Auditoria	-	- Mal funcionamento - Alteração no Registro de votação - Votação não autorizada -Alteração da dados do sistema	Votação Eletrônica Supervisionada
[Yoon et al. 2010]	Protocolo de autenticação Confiável	Criptografia ElGamal	-	-	Votação Eletrônica Remota
[Sebé et al. 2010]	-	Criptografia de ElGamal	-	-	Votação Eletrônica Remota
[Spycher and Haenni 2010]	Protocolo de Sistema Híbrido	- Criptografia ElGamal - Criptografia Limiar	-	-	Votação Eletrônica Remota

5. Discussão

Levando em consideração os estudos retornados pelo MS, pode-se observar que existem diversos protocolos utilizados em sistemas de votação eletrônica, onde cada qual possui um objetivo diferente com a finalidade de garantir que o sistema implemente as principais propriedades de segurança. Porém, alguns protocolos acabam sofrendo com algum tipo de falha, ocasionando uma vulnerabilidade no sistema. Um exemplo disso, é o protocolo de contagem de votos de [Nassar et al. 2018], que através de um ataque de negação de serviço, ou ataque DoS, faz com que seu servidor de contagem de votos não seja confiável. Outro exemplo é o protocolo TPKE, pois é suscetível ao ataque MITM, o que pode causar a perda de privacidade do eleitor, [Kiayias et al. 2017, Kiayias et al. 2015].

Uma medida de segurança aplicadas ao TPKE, é a baseada em criptografia de chaves públicas, como mostra o estudo de [Kiayias et al. 2015]. Entretanto, diferentes outros tipos de protocolos, como o baseado no conceito do *Pret-à-voter* [AboSamra et al. 2017], protocolo ESIV [Shakiba et al. 2017], e protocolo de auto-cálculo [Dossogne and Lafitte 2015] também utilizam esse tipo de medida de segurança, onde a criptografia de ElGamal também é utilizada no protocolo de Auto-cálculo. Os protocolos de autenticação confiável [Yoon et al. 2010], e protocolo de sistema híbrido [Spycher and Haenni 2010] também utilizam essa criptografia em seu sistema de segurança.

A assinatura cega é uma das medidas de segurança mais utilizadas pelos autores em diferentes sistemas e tipos de protocolos, [Zhu et al. 2018, Kumar et al. 2017, Zhang et al. 2015, Huarte et al. 2013, Kim et al. 2013, Khelifi et al. 2013, Nguyen and Dang 2013b, Nguyen and Dang 2013a], onde combinada com outras medidas de segurança podem garantir o anonimato do eleitor e a segurança do sistema. Nesse sentido, ela é utilizada para evitar uma das ameaças mais comuns desse tipo de sistema, o ataque de negação de serviço, [Nassar et al. 2018, Zhang et al. 2015, Rura et al. 2015, Lavanya 2011]. Além da assinatura cega, a criptografia homomórfica de Paillier [Nassar et al. 2018], criptografia de chave simétrica [Zhang et al. 2015], criptografia visual, decriptação e esteganografia [Yu et al. 2018] também são técnicas de segurança utilizadas para evitar esse tipo de ataque.

Entre os sistemas de votação, o que mais teve destaque negativo foi o Hélios, que se trata de um sistema de votação pela Internet. Estudos como os de [Kiayias et al. 2017] e [Srinivasan et al. 2013] mostram que esse sistema é suscetível ao ataque MITM e ataque de enchimento de cédulas, podendo sofrer também de uma vulnerabilidade que pode revelar o voto do eleitor [Kiayias et al. 2017, Cortier and Smyth 2013]. Além disso o estudo de [Heiderich et al. 2011] mostra que esse sistema não implementa o cabeçalho HTTP. As medidas de segurança aplicadas a esse sistema, se tratam de esquemas de compartilhamento secreto verificável, criptografia controlada por *token* e remoção de cédulas replicadas.

Como ameaças à validade deste mapeamento, vale destacar a criação e adaptação da *string* de busca. Como as palavras e expressões que a compõem são derivadas das QPs, a correta construção desta é vital para a efetividade da pesquisa. Para mitigar esta ameaça, a *string* de busca foi criada e calibrada para verificar se os estudos definidos como controle, na Seção 3.2, retornaram com a *string* de busca executada. Além disso, foi solicitado a um especialista que avaliasse a *string* para validá-la e melhorar sua efetividade.

Por fim, a última ameça está relacionada ao processo de seleção de estudos. Para minimizar essa ameaça, com o objetivo de assegurar um processo de seleção imparcial e evitar vieses foi desenvolvido um protocolo de pesquisa sobre as orientações estabelecidas por [Kitchenham et al. 2010]. Esse protocolo contêm as questões de pesquisa, estratégia de busca, critérios de inclusão e exclusão, bem como a forma como os dados serão extraídos.

6. Conclusões

Neste estudo foram apresentados e discutidos os resultados de um mapeamento sistemático conduzido com o objetivo de identificar os principais protocolos de votação eletrônica utilizados, as vulnerabilidades e falhas em que esses sistemas são expostos, além das medidas de segurança mais utilizadas por esses sistemas.

É importante destacar que um mapeamento sistemático é suscetível a falhas, especialmente quando a identificação dos estudos primários é feita somente por buscas automatizadas em bases de dados indexados. Em geral, o mapeamento contribuiu para um melhor entendimento do atual estado da arte dos sistemas eleitorais para a identificação de limitações, protocolos e medidas de segurança usados, além das vulnerabilidades que esses sistemas sofrem.

Os resultados mostraram um grande número de estudos que discutem sobre as falhas encontradas em protocolos utilizados por diferentes sistemas eleitorais em todo o mundo, e também as várias medidas de segurança que podem ser implementadas por esses tipos de sistemas, para garantir que as ameaças à segurança dos mesmos seja amenizada.

Como trabalhos futuros, para melhorar a cobertura do processo de seleção dos estudos e, consequentemente minimizar a ameaça quanto aos estudos não incluídos, pretende-se complementar os resultados obtidos neste MS por meio da busca manual em anais de congressos e periódicos na área, que não são indexados nas bases de dados eletrônicas, e por meio da análise das referências de cada estudo incluído.

Referências

AboSamra, K. M., AbdelHafez, A. A., Assassa, G. M., and Mursi, M. F. (2017). A practical, secure, and auditable e-voting system. *Journal of Information Security and Applications*.

Aranha, D. F., Nunes, T., and Cardoso, C. (2018). Execução de código arbitrário na urna eletrônica brasileira. (July):1–36.

Babenko, L. and Pisarev, I. (2018). Cryptographic protocol security verification of the electronic voting system based on blinded intermediaries. In *Proc. of the 3rd IITI*. Springer.

Babenko, L., Pisarev, I., and Makarevich, O. (2017). A model of a secure electronic voting system based on blind intermediaries using russian cryptographic algorithms. In *Proc. of the 10th SINCONF*. ACM.

Bistarelli, S., Mercanti, I., Santancini, P., and Santini, F. (2019). End-to-end voting with non-permissioned and permissioned ledgers. *Journal of Grid Computing*.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., and Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Systems and Software*, 80:571–583.

Chang, D., Chauhan, A. K., Kang, J., et al. (2015). Apollo: End-to-end verifiable voting protocol using mixnet and hidden tweaks. In *Proc. of the 18th ICISC*. Springer.

Cortier, V. and Smyth, B. (2013). Attacking and fixing helios: An analysis of ballot secrecy. *Journal of Computer Security*.

Dossogne, J. and Lafitte, F. (2015). Blinded additively homomorphic encryption schemes for self-tallying voting. *Journal of Information Security and Applications*.

Gurubasavanna, M., Shariff, S. U., Mamatha, R., and Sathisha, N. (2018). Multimode authentication based electronic voting kiosk using raspberry pi. In *Proc. of the 2nd International Conference on I-SMAC*. IEEE.

Haines, T. and Boyen, X. (2016). Truly multi-authority 'prêt-à-voter'. In *Proc. of the E-Vote-ID*. Springer.

Heiderich, M., Frosch, T., Niemietz, M., and Schwenk, J. (2011). The bug that made me president a browser-and web-security case study on helios voting. In *Proc. of the 3rd Vote-ID*. Springer.

Hsiao, T.-C., Wu, Z.-Y., Liu, C.-H., and Chung, Y.-F. (2017). Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme. *Advances in Mechanical Engineering*.

Huarte, M., Goirizelaia, I., Unzilla, J. J., Matías, J., and Igarza, J. J. (2013). A new fully auditable proposal for an internet voting system with secure individual verification and complaining capabilities. In *Proc. of the 10th SECRYPT*. IEEE.

Hussien, H. and Aboelnaga, H. (2013). Design of a secured e-voting system. In *Proc. of the ICCAT*. IEEE.

Institute for Democracy and Electoral Assistance (2015). Use of e-voting around the world. `https://www.idea.int/news-media/media/use-e-voting-around-world`. Acessado em: 08/07/2019.

Jin, C., Chen, G., Yu, C., Zhao, J., Jin, Y., and Shan, J. (2019). Heterogeneous deniable authentication and its application to e-voting systems. *Journal of Information Security and Applications*.

Kartit, Z., El Marraki, M., Azougaghe, A., and Belkasmi, M. (2015). Towards a secure electronic voting in cloud computing environment using homomorphic encryption algorithm. *International Journal of Applied Engineering Research*.

Kate, N. and Katti, J. (2016). Security of remote voting system based on visual cryptography and sha. In *Proc. of the ICCUBEA*. IEEE.

Khelifi, A., Grisi, Y., Soufi, D., Mohanad, D., and Shastry, P. (2013). M-vote: a reliable and highly secure mobile voting system. In *Proc. of the PICICT*. IEEE.

Kiayias, A., Zacharias, T., and Zhang, B. (2015). On the necessity of auditing for election privacy in e-voting systems. In *Proc. of the e-Democracy*. Springer.

Kiayias, A., Zacharias, T., and Zhang, B. (2017). Auditing for privacy in threshold pke e-voting. *Information & Computer Security*.

Kim, C. S., Jung, C. D., Ha, S. Y., and Park, C. H. (2013). A study on the ubiquitous e-voting system for the implementation of e-government. *International Journal of Security & Its Applications*.

Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., and Linkman, S. (2010). Systematic literature reviews in software engineering–a tertiary study. *Information and Software Technology*.

Kumar, M., Katti, C. P., and Saxena, P. C. (2017). A secure anonymous e-voting system using identity-based blind signature scheme. In *Proc. of the ICISSP*. Springer.

Lakshmi, C. J. and Kalpana, S. (2018). Secured and transparent voting system using biometrics. In *Proc. of the 2nd ICISC*. IEEE.

Lavanya, S. (2011). Trusted secure electronic voting machine. In *Proc. of the ICONSET*. IEEE.

Lee, K., Lee, Y., Won, D., and Kim, S. (2010). Protection profile for secure e-voting systems. In *Proc. of the 6th ISPEC*. Springer.

Mohammadpourfard, M., Doostari, M. A., Ghaznavi Ghoushchi, M. B., and Shakiba, N. (2015). A new secure internet voting protocol using java card 3 technology and java information flow concept. *Security and Communication Networks*.

Nassar, M., Malluhi, Q., and Khan, T. (2018). A scheme for three-way secure and verifiable e-voting. In *Proc. of the 15th AICCSA*. IEEE.

Nguyen, T. A. T. and Dang, T. K. (2013a). Enhanced security in internet voting protocol using blind signature and dynamic ballots. *Electronic Commerce Research*.

Nguyen, T. A. T. and Dang, T. K. (2013b). A practical solution against corrupted parties and coercers in electronic voting protocol over the network. In *Proc. of the ICT-EurAsia*. Springer.

Olembo, M. M., Schmidt, P., and Volkamer, M. (2011). Introducing verifiability in the polyas remote electronic voting system. In *Proc. of the 6th ARES*. IEEE.

Peng, K. (2011). A general and efficient countermeasure to relation attacks in mix-based e-voting. *International Journal of Information Security*.

Pereira, O. and Wallach, D. S. (2017). Clash attacks and the star-vote system. In *Proc. of the E-Vote-ID*. Springer.

Rura, L., Issac, B., and Haldar, M. (2015). Vulnerability studies of e2e voting systems. In *Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering*. Springer.

Saqib, M. N., Kiani, J., Shahzad, B., Anjum, A., Ahmad, N., et al. (2018). Anonymous and formally verified dual signature based online e-voting protocol. *Cluster Computing*.

Sebé, F., Miret, J. M., Pujolàs, J., and Puiggalí, J. (2010). Simple and efficient hash-based verifiable mixing for remote electronic voting. *Computer Communications*.

Shakiba, N. M., Doostari, M.-A., and Mohammadpourfard, M. (2017). Esiv: an end-to-end secure internet voting system. *Electronic Commerce Research*.

Smartmatic (2018). Benefícios do voto eletrônico. `http://www.smartmatic.com/pt/votacao/voto-eletronico/`. Acessado em: 14/10/2018.

Spycher, O. and Haenni, R. (2010). A novel protocol to allow revocation of votes a hybrid voting system. In *Proc. of the ISSA*. IEEE.

Srinivasan, S., Culnane, C., Heather, J., Schneider, S., and Xia, Z. (2013). Countering ballot stuffing and incorporating eligibility verifiability in helios. In *Proc. of the NSS*. Springer.

Tornos, J. L., Salazar, J. L., and Piles, J. J. (2015). Optimizing ring signature keys for e-voting. In *Proc. of the IWCMC*. IEEE.

Will, M. A., Nicholson, B., Tiehuis, M., and Ko, R. K. (2015). Secure voting in the cloud using homomorphic encryption and mobile agents. In *Proc. of the ICCCRI*. IEEE.

Yoon, E.-J., Yoo, K.-Y., Yeo, S.-S., and Lee, C. (2010). Robust deniable authentication protocol. *Wireless Personal Communications*.

Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., and Au, M. H. (2018). Platform-independent secure blockchain-based voting system. In *Proc. of the ISC*. Springer.

Zhang, H., You, Q., and Zhang, J. (2015). A lightweight electronic voting scheme based on blind signature and kerberos mechanism. In *Proc. of the 5th ICEIEC*. IEEE.

Zhou, Y., Zhou, Y., Chen, S., and Wu, S. S. (2016). Mvp: an efficient anonymous e-voting protocol. In *Proc. of the GLOBECOM*. IEEE.

Zhu, Y., Zeng, Z., and Lv, C. (2018). Anonymous voting scheme for boardroom with blockchain. *International Journal of Performability Engineering*.

Zissis, D. and Lekkas, D. (2011). Securing e-government and e-voting with an open cloud computing architecture. *Government Information Quarterly*.