VI Simpósio de Iniciação Científica 2023
Ciência como ferramenta de transformação da sociedade

Estado da arte em técnicas de teste de software para requisitos de segurança em sistemas de Internet das Coisas

Letícia V. Santos[1] (IC), Lina Garcés (PQ)[1]
[1]*Instituto de Matemática e Computação - IMC,*
Universidade Federal de Itajubá, Itajubá, MG, Brasil.
{d2020023211, lina}@unifei.edu.br

Palavras-chave: Internet of Things. Privacidade. Segurança. Testes de Software, Engenharia de Software

Introdução

A Internet das Coisas (IoT) é uma extensão da Internet que permite que objetos do dia a dia se conectem à Internet, facilitando as atividades cotidianas dos usuários (SANTOS et al., 2016). No entanto, como muitas tecnologias que dependem de redes e armazenamento de dados, a IoT enfrenta desafios de segurança significativos (LEITE, 2019). A segurança da informação é considerada o maior obstáculo para a implantação efetiva da IoT, pois não existem sistemas ou dispositivos 100% seguros (MORAES, 2010).

Para abordar esses desafios, os testes de software são amplamente utilizados para garantir a integridade dos dados, segurança, *performance*, aconformidade e usabilidade dos dispositivos e sistemas de IoT. Muitas pesquisas estão atualmente focadas na proposição de soluções de teste de segurança para a IoT, e é essencial realizar uma avaliação crítica desses estudos para identificar oportunidades de aprimoramento nesta área.

Metodologia

Este trabalho visa sintetizar o conhecimento do estado da arte de teste de segurança para Internet das Coisas. O objetivo é fornecer uma visão completa dos tipos, técnicas e métodos de testes de software na engenharia de software, utilizados para identificar erros e falhas de segurança e privacidade em sistemas de IoT. Para isso, foram executadas as seguintes etapas:

I - Contextualização: A pesquisa começou com a aquisição de conhecimento, incluindo a leitura da Lei Geral de Proteção de Dados (LGPD) e a avaliação do ciclo de manipulação de dados. Em seguida, a necessidade de examinar vulnerabilidades em dispositivos de IoT foi reconhecida, destacando quatro categorias de vulnerabilidades. Leituras sobre testes de segurança, tipos, técnicas e métodos foram conduzidas, complementadas por um minicurso. Após a preparação, a revisão da literatura foi planejada seguindo diretrizes específicas.

II - Planejamento e Execução: A revisão sistemática de literatura foi planejada e executada seguindo as diretrizes de KITCHENHAM e CHARTERS (2007). A base de dados SCOPUS foi escolhida para pesquisa, usando as palavras-chave "security," "testing," e "Internet-of-Things," abrangendo os últimos 5 anos.

III - Extração e Análise: Por fim, um formulário foi desenvolvido[1] para a extração de dados dos estudos selecionados. As perguntas contidas no formulário foram estrategicamente elaboradas para o levantamento de dados relevantes para a pesquisa. Os dados foram analisados para responder cinco perguntas de pesquisa (PPq1 - PPq5), como detalhado na seguinte seção.

PPq1 - Quais técnicas de teste de software (p.ex. unitário, integração, e2e, interface, etc.) têm sido propostas para garantir a segurança em sistemas de IoT?

PPq2 - Quais são os métodos (p.ex. white-box, black-box, híbrido) utilizados para testar segurança em IoT?

PPq3 - Qual o estado dos testes automatizados para identificar erros e falhas de segurança em sistemas de IoT?

PPq4 - Qual o estado de aplicação de técnicas de IA/ML para realizar testes de segurança em sistemas de IoT?

PPq5 - Qual o escopo das técnicas de teste de segurança? Elas possibilitam identificar falhas relacionadas aos diversos atributos de segurança, como por exemplo, confidencialidade, integridade, privacidade, disponibilidade, autenticação, autorização, safety, não-repudiação, compliance, accountability?

Resultados

Ao executar a string de busca na base Scopus, foram obtidos 419 estudos. Na fase inicial de seleção, após analisar o título, abstract e palavras-chave e aplicar os critérios de inclusão e exclusão, 119 estudos foram

[1]Formulário:https://docs.google.com/forms/d/e/1FAIpQLSclIqu7au2kaVSs6nbwxoZW-LSX5mG-3wANSV8Dv34pkavblw/viewform?usp=share_link

pré-selecionados e, após uma leitura detalhada, 26 foram selecionados para extração de dados. Durante esse processo, duas pesquisadoras avaliaram cada estudo para garantir a consistência do conjunto final de estudos primários com o propósito da revisão. A lista completa dos estudos primários selecionados está disponível em SANTOS e GARCÉS (2023).
A análise dos estudos permitiu obter os seguintes resultados.

PPq1 - Técnicas de Teste de Segurança para Sistemas de IoT

Como notado na Figura 1, os testes de integração estavam presentes em 23 dos 26 artigos, se destacando entre as outras técnicas.

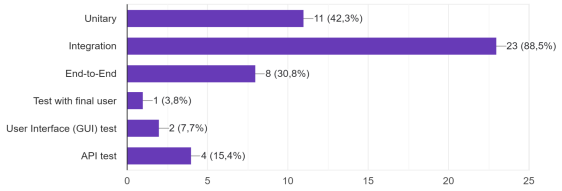

Figura 1 – Técnicas de testes usadas ou propostas nos estudos primários

PPq2 - Métodos para Testar Segurança em Sistemas de IoT

Foram encontrados 10 estudos que realizaram ambas as abordagens, 8 que abordaram a técnica black box e 8 que utilizaram white box. Com isso, nota-se uma igualdade de abrangência entre os métodos, ambos totalizando 69,9% (18/26) dos 26 estudos.

PPq3 - Uso de Ferramentas de Automação para Testes de Segurança em Sistemas de IoT

A maioria dos estudos, i.e., 69,2% (18/26), abordaram automação de testes. A título de exemplificação, segue uma lista com algumas das automações identificadas:

LI, Y. et al. (2020) desenvolveram o IoT-APIScanner, um framework para assegurar o permissionamento correto de recursos da API na nuvem.

AL-HADHRAMI, Y., HUSSAIN, F. K. (2020) propõem um framework, IoT-DDoS, que atua em tempo real para coleta e criação de conjuntos de dados em IoT, explorando geração de tráfego de ataques, método de enfileiramento e extração de recursos, gerando conjuntos de dados para avaliação de sistemas de detecção de intrusão.

SALZILLO, G., RAK, M., MORETTA, F. (2020) modelaram de um framework, SuT4, com o fito de automatizar os procedimentos de teste de penetração para identificar ameaças e possíveis falhas de segurança nos sistemas de Internet das Coisas. Realizaram um estudo de caso com o Open Energy Monitor, abordando o uso do protocolo MQTT e destacando o planejamento de testes de penetração, com a adoção de um banco de dados de inteligência de ameaças cibernéticas oferecido pela MITRE.

PPq4 - Aplicação de Técnicas de IA/ML para Testes de Segurança em Sistemas de IoT

Somente 34,6% (9/26) dos estudos propõem técnicas de IA/ML para testar segurança em sistemas de IoT. Alguns exemplos das utilizações de Inteligência Artificial e Machine Learning, bem como a Deep Learning, que foram encontradas são:

KURNIAWAN, A., KYAS, M. (2019) utilizaram Deep Learning (*Autoencoder)*, que foi usada para para ofuscar os dados do sensor de partes não autorizadas.

SOUZA, V. C. O. *et al*. (2021) utilizaram Machine Learning - *Naive Bayes*, *Support Vector Machine (SVM)*, *Gradient Boosting Tree (GBT)* e *Random Forest(RF)* - na detecção SQL Injection.

GABER, T., EL-GHAMRY, A., HASSANIEN, A. E. (2022) usaram Machine Learning (*Support Vector Machine(SVM)* e *Random Forest Decision Tree(RFDT)*) para detectar ataques de injeção em aplicações IoT.

PPq5 - Escopo dos Testes de Segurança para IoT

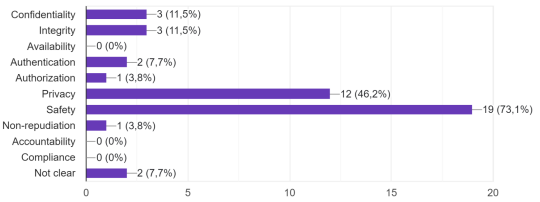

Figura 2– Atributo de segurança que é foco dos testes nos estudos primários

Observa-se, na Figura 2, que, entre os estudos selecionados, alguns requisitos não foram explorados, tais como Disponibilidade, Responsabilização e Conformidade. Além disso, outros requisitos receberam menos ênfase, a saber: Autorização (3,8%), Não-Repúdio (3,8%), Autenticação (7,7%), Confidencialidade (11,5%) e Integridade (11,5%). Além disso, em 7,7% (2/26) dos casos, não foi possível identificar quais requisitos foram explorados. Por fim, os requisitos mais abordados foram Privacidade (46,2%) e Safety (73,1%).

Discussões

Após analisar os 26 estudos, fica evidente que os requisitos de segurança e privacidade foram os mais testados, já seja individualmente, ambos simultaneamente ou em conjunto com outros requisitos, em 22 dos artigos analisados.

Um outro aspecto notável a ser considerado é a predominância similar dos métodos de teste, i.e., White-box (Caixa Branca), Black-box (Caixa Preta) ou híbrido. Constatamos que 8 artigos optaram pelo uso da técnica Black-Box, identificados como A03, A08, A09, A13, A15, A16, A19 e A20. Por outro lado, 8 estudos adotaram a técnica White-Box, referenciados como A02, A05, A07, A10, A11, A21, A22 e A23. Além disso, observamos que 10 pesquisas analisadas optaram por uma abordagem híbrida, incorporando ambas as técnicas. Esses estudos foram identificados como A01, A04, A06, A12, A14, A17, A18, A24, A25 e A26.

Uma otra observação a destacar é a automatização dos testes, considerada em 18 dos 26 estudos. Além disso, identificou-se propostas de aplicação e utilização de Inteligência Artificial, Machine Learning, bem como Deep Learning em 9 estudos. Com base nessa análise, conseguiu-se representar a relação entre os métodos utilizados (black box, white box ou híbrido), a presença de automação e o uso de IA/ML/DL e os requisitos de segurança aplicados. Apresentamos essas informações na Tabela 1.

ID	*Método*	*Ferramenta*	*IA/ML/DL*	*Req. de Segurança*
A01	Híbrido	Não	Não	Confidencialidade, Integridade e Autenticação
A02	White box	Sim	Não	Não identificado
A03	Black box	Não	Sim	Privacidade
A04	Híbrido	Não	Não	Segurança
A05	White box	Não	Sim	Não identificado
A06	Híbrido	Não	Não	Segurança
A07	White box	Não	Não	Segurança
A08	Black box	Não	Não	Segurança
A09	Black box	Sim	Não	Segurança
A10	White box	Sim	Não	Segurança
A11	White box	Sim	Não	Privacidade e Segurança
A12	Híbrido	Sim	Não	Privacidade
A13	Black box	Sim	Não	Confidencialidade, Integridade, Autenticação, Privacidade, Segurança e Não-repúdio
A14	Híbrido	Sim	Não	Privacidade e Segurança
A15	Black box	Sim	Não	Privacidade e Segurança
A16	Black box	Sim	Não	Segurança
A17	Híbrido	Sim	Não	Segurança
A18	Híbrido	Sim	Não	Confidencialidade, Integridade e Autenticação
A19	Black box	Sim	Não	Privacidade e Segurança
A20	Black box	Não	Sim	Segurança
A21	White box	Sim	Sim	Privacidade e Segurança
A22	White box	Sim	Sim	Privacidade e Segurança
A23	White box	Sim	Sim	Privacidade
A24	Híbrido	Sim	Sim	Segurança
A25	Híbrido	Sim	Sim	Privacidade e Segurança
A26	Híbrido	Sim	Sim	Privacidade e Segurança

Tabela 1 - Resumo das contribuições dos estudos primários contendo os métodos, ferramentas, uso de IA/ML, e requisitos de segurança testados.

Seis dos 9 estudos que aplicam técnicas de IA/ML propõem ferramentas para testar privacidade e segurança em sistemas de IoT seguindo o método White box (A21-A23) ou híbrido (A24 -A26). No relacionado às técnicas black-box elas foram combinadas em ferramentas em cinco estudos, porém nenhuma dessas ferramentas considerou técnicas de IA/ML na sua implementação.

Conclusões

Os estudos iniciais desempenharam um papel crucial na pesquisa, fornecendo conhecimento sobre a Lei Geral de Proteção de Dados (LGPD), o ciclo de vida

dos dados e os princípios da Internet das Coisas (IoT). Essa base teórica foi fundamental para a compreensão das leis que regem o tratamento de dados e para explorar técnicas de teste visando a segurança de dados em redes de dispositivos interconectados. Além disso, a compreensão dos testes de software se revelou essencial para garantir a qualidade da IoT e a conformidade com a legislação de privacidade.

A análise dos periódicos selecionados revelou que os estudos na área da IoT e seus testes estão explorando áreas importantes e necessárias. A pesquisa nesse campo é crucial, pois a IoT está se tornando cada vez mais presente em diversos aspectos da vida cotidiana, como doméstica, educacional, saúde e industrial. Portanto, os pesquisadores devem continuar a aprofundar seu conhecimento neste domínio em constante crescimento.

Este estudo demonstra a importância de tomar decisões informadas no desenvolvimento da pesquisa, utilizando dados obtidos na análise de artigos publicados. Em última análise, destaca-se a relevância da investigação relacionada à segurança e privacidade na Internet das Coisas.

Agradecimentos

À Universidade Federal de Itajubá (UNIFEI) pelo apoio, espaço e suporte fornecidos para a condução das pesquisas. Ao CNPq pela dedicação e pelo incentivo à pesquisa, o que possibilitou o desenvolvimento desta pesquisa.

Referências

AL-HADHRAMI, Y; HUSSAIN, F. K. **Real time dataset generation framework for intrusion detection systems in IoT**. Future Generation Computer Systems, v. 108, p. 414-423, jul. 2020.

GABER, T., EL-GHAMRY, A., HASSANIEN, A. E.. **Injection attack detection using machine learning for smart IoT applications**. Physical Communication: 2022. Disponível em:10.1016/j.phycom.2022.101685. Acesso em: 31 ago. 2023.

KITCHENHAM, B., CHARTERS, S. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report, 2007.

KURNIAWAN, A., KYAS, M. **A privacy-preserving sensor aggregation model based deep learning in large scale internet of things applications**. IEEE 17th World Symposium on Applied Machine Intelligence and Informatics, p. 391-396: 2019. Disponível em:10.1109/SAMI.2019.8782758 Retrieved from www.scopus.com. Acesso em: 31 ago. 2023.

LEITE, L. R. C. **Internet das Coisas (IoT): vulnerabilidades de segurança e desafios**. Orientado por: Rogério Nunes de Freitas. Trabalho de conclusão de curso - Faculdade de Tecnologia de Americana, Americana, 2019. Disponível em: http://ric.cps.sp.gov.br/handle/123456789/3978. Acesso em: 30 ago. 2023.

LI, Y.. (2020). **IoT-APIScanner: Detecting API Unauthorized Access Vulnerabilities of IoT Platform**. 29th International Conference on Computer Communications and Networks (ICCCN): 2020.

MORAES, A. F. **Segurança em Redes: Fundamento**s. São Paulo, 2010.

SALZILLO, G., RAK, M., MORETTA, F. **Threat Modeling based Penetration Testing: The Open Energy Monitor Case study**. 13th International Conference on Security of Information and Networks, 2020. Disponível em: https://dl-acm-org.ez38.periodicos.capes.gov.br/doi/10.1145/3433174.3433181. Acesso em: 31 ago 2023.

SANTOS, B. P. *et al.* **Internet das Coisas: da Teoria à Prática**. Capítulo 1. Livro de Minicursos do XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRCSD). Salvador, BA, Brasil. 2016

SANTOS, L. e GARCÉS, L. **Relatório: Estado da arte em técnicas de teste de software para requisitos de segurança em sistemas de Internet das Coisas.** Biblioteca Manuá UNIFEI. (2023)

SOUZA, V. C. O. et al. **Análise de diferentes técnicas de pré-processamento em algoritmos de Aprendizado de Máquina na detecção de SQL Injection**. Seminário Integrado de Software e Hardware (SEMISH), 48. , 2021, Evento Online. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 257-264. Disponível em: https://doi.org/10.5753/semish.2021.15830. Acesso em: 31 ago. 2023.

VIVIANI, F. P. **Categorização de vulnerabilidades de segurança em sistemas de IoT**. Orientador: Lina Maria Garcés Rodriguez. Trabalho de Conclusão de Curso - Universidade Federal de Itajubá, Itajubá, 2022.