RELATÓRIO TÉCNICO

Uma Revisão Estruturada sobre as Vulnerabilidades de Segurança em Ambientes IoT

Janeiro, 2023

Uma Revisão Estruturada sobre as Vulnerabilidades de Segurança em Ambientes IoT

1. Introdução

1.1. Contexto

O atributo de segurança é um dos principais fatores de impacto tanto em sistemas tradicionais quanto em ambientes de sistemas complexos, atrelado ao grau de atenção e cuidado com que os dados devem ser manuseados.

Em ambientes IoT, o atributo de segurança passa a exigir um cuidado redobrado com os seus sistemas de software e dispositivos, por se tratar de dados coletados e compartilhados por diferentes dispositivos e capturando os mais variados tipos de informação, exigindo um certo nível de privacidade. Entretanto, sabemos da fragilidade e dos perigos que espreitam pela rede, gerando muitas ameaças e destacando certas vulnerabilidades que esses sistemas contêm.

No entanto, conhecer as vulnerabilidades que permeiam esses cenários, garante que ameaças possam ser antecipadas e estratégias de mitigação possam ser traçadas para minimizar os riscos de invasão ou roubo de dados. Por este motivo, em uma tentativa de preencher essa lacuna crítica em ambientes IoT e em resposta às preocupações sobre as vulnerabilidades que permeiam as camadas de sistemas IoT, nosso principal objetivo é identificar e elencar as vulnerabilidades conhecidas em ambientes IoT, permitindo dessa forma ter uma base de informações sobre vulnerabilidade apontadas por estudos na área.

Para isso, essa Revisão Estruturada foi planejada e executada de forma a destacar com base em análises detalhadas as vulnerabilidades de segurança existentes em ambientes IoT. Ressaltamos que os resultados obtidos são parciais, já que há procedimentos de investigação (Snowballing) em andamento, que permitirá uma maior precisão nos resultados alcançados.

2. Definições

As definições referentes aos conceitos básicos de vulnerabilidade de segurança vêm da (ISO/IEC 27000 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Visão geral e vocabulário). Onde vulnerabilidade é definida como:

- *“Fraqueza de um ativo ou controle, que pode ser explorada por uma ou mais ameaças.”*
- *“Weakness of an asset or control, that can be exploited by one or more threats.”*

3. Questões de Pesquisa

3.1. Objetivo

O objetivo da pesquisa deste estudo é identificar vulnerabilidades de segurança em sistemas de software e dispositivos IoT.

3.2. Questões

3.2.1. Problema

Aparentemente, não há disponibilidade de solução unificada que forneça os quesitos de segurança que necessitam ser tratados no desenvolvimento de sistemas de software IoT. Sendo assim, conhecer os principais pontos de vulnerabilidade em sistemas deste tipo pode ajudar a mitigar grande parte dos principais e mais comuns riscos associados a esses sistemas de software.

3.2.2. Questão Principal

Quais vulnerabilidades afetam e podem ser identificadas em sistemas de software IoT?

4. Estratégia de Busca

Os dados extraídos e analisados neste estudo serão identificados por meio da biblioteca digital SCOPUS, por integrar uma grande quantidade de outras bibliotecas no seu acervo de dados. Snowballing será usado para complementar as buscas.

4.1. Idioma e Expressão de Busca

O idioma escolhido para a busca e seleção dos trabalhos foi o Inglês.

A busca foi restringida usando-se palavras-chave específicas para encontrar as publicações de interesse. A expressão de busca foi definida seguindo o princípio PICOC (Petticrew & Roberts, 2006)[1] na forma como os sinônimos são separados pelo conector lógico "*OR*" e os termos que compõem a string são separados por "*AND*", utilizando dos parâmetros "*Population*", "*Intervention*", "*Comparison*", "*Outcome*", e "*Context*".

[1] Petticrew, Mark and Helen Roberts. Systematic Reviews in the Social Sciences: A Practical Guide. Oxford, UK: Blackwell Publishing Ltd, 2006, doi:10.1002/9780470754887.

PICOC	STRING
Population	*"ambient intelligence" OR "assisted living" OR "multiagent systems" OR "systems of systems" OR "Cyber-Physical Systems" OR "Industry 4" OR "fourth industrial revolution" OR "web of things" OR "contemporary software systems" OR "smart manufacturing" OR digitalization OR digitization OR "digital transformation" OR "smart cit*" OR "smart building" OR "smart health" OR "smart environment" OR "smart grid"; AND*
Intervention	*"security" OR "vulnerability" OR "weakness" OR "Invasion" OR "threat" OR "attack" OR "anomaly" OR "malware" OR "confidentiality" OR "auditability" OR "risk"; AND*
Comparison	*Não Disponível*
Outcome	*"taxonomy" OR "categories" OR "classification" OR "Catalog"; AND*
Context	*"internet of things" OR "Internet of Everything" OR "IoT"*

Para a Scopus, a string de busca utilizada foi:

TITLE-ABS-KEY (("ambient intelligence" OR "assisted living" OR "multiagent systems" OR "systems of systems" OR "Cyber-Physical Systems" OR "Industry 4" OR "fourth industrial revolution" OR "web of things" OR "contemporary software systems" OR "smart manufacturing" OR digitalization OR digitization OR "digital transformation" OR "smart cit*" OR "smart building" OR "smart health" OR "smart environment" OR "smart grid" OR "autonomous system") AND ("security" OR "vulnerability" OR "weakness" OR "Invasion" OR "threat" OR "attack" OR "anomaly" OR "malware" OR "confidentiality" OR "auditability" OR "risk" OR "menace") AND ("taxonomy" OR "categories" OR "classification" OR "Catalog") AND ("internet of things" OR "Internet of Everything" OR "IoT"))

5. Processo de Seleção dos Estudos

Foram realizados os seguintes procedimentos de seleção na execução da string de busca da scopus:

a. Aplicação dos critérios de seleção baseado no título, resumo e palavras-chave dos artigos;

b. Aplicação dos critérios de seleção baseado na leitura completa dos artigos selecionados na etapa anterior.

Depois de finalizar a seleção por meio do motor de busca, usamos o conjunto de artigos incluídos para executar o snowballing backward (um nível) and forward seguindo o seguinte fluxo:

a. Aplicação dos critérios de seleção baseado no Título dos artigos;

b. Aplicação dos critérios de seleção baseado no Resumo dos artigos;

c. Aplicação dos critérios de seleção baseado na Leitura completa dos artigos aceitos.

6. Critérios de Seleção

6.1. Critério de Inclusão

- Apresentar cenários focados em segurança em sistemas de software IoT; e
- Identificar as vulnerabilidades identificadas dentro destes cenários.
- O trabalho deve ser escrito no idioma inglês.

6.2. Critério de Exclusão

- Não estar disponível ou acessível por completo;
- Estudos Duplicados.

7. Processo de Extração

Para cada fonte candidata, o procedimento de extração é realizado utilizando o modelo apresentado na Seção 7.1.

7.1. Modelo de Extração

A) Dados da publicação:	
Título:	indica o título do trabalho
Autor(es):	nome dos autores
Fonte de Publicação:	local de publicação
Ano da Publicação:	ano de publicação
Resumo:	texto contendo uma descrição do resumo
B) Dados derivados do objetivo:	
Vulnerabilidades	Quais as vulnerabilidades em sistemas de software IoT são destacadas no estudo?

8. Relatório da Execução

- Data de Execução Scopus: 2022/08/12

Foram identificados 638 resultados de documentos. Eliminando proceedings e livros, restaram 492 no total.

  - Arquivo Jab ref com resultados da Scopus

- Incluídos para extração de dados (e usado para o Snowballing):
    - Arquivo Jab ref com os trabalhos aceitos

O conjunto final de artigos selecionados:

- Pelo motor de busca (Scopus)

[A1]. Saha. T. et al. (2022), "SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems Based on Machine Learning," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 870-885, doi: 10.1109/TETC.2021.3050733.

[A2]. AbuEmera, E. A., ElZouka H. A. and Saad A. A. (2022), "Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach," 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, pp. 605-612, doi: 10.1109/ICCECE54139.2022.9712770.

[A3]. Auliar, R. B. and Bekaroo G. (2021). "Security in IoT-based Smart Homes: A Taxonomy Study of Detection Methods of Mirai Malware and Countermeasures," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, pp. 1-6, doi: 10.1109/ICECCME52200.2021.9590841.

[A4]. Tomur, E. et al. (2021) "SoK: Investigation of Security and Functional Safety in Industrial IoT," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, pp. 226-233, doi: 10.1109/CSR51186.2021.9527921.

[A5]. Karie N. M. et al. (2021). "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, doi: 10.1109/ACCESS.2021.3109886.

[A6]. Davis B. D., Mason J. C. and Anwar M. (2020). "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10102-10110, doi: 10.1109/JIOT.2020.2983983.

[A7]. Akhunzada A., Islam S. U. and Zeadally S. (2020), "Securing Cyberspace of Future Smart Cities with 5G Technologies," in IEEE Network, vol. 34, no. 4, pp. 336-342, doi: 10.1109/MNET.001.1900559.

[A8]. Sengupta, J., Ruj, S. and Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, art. no. 102481. doi: 10.1016/j.jnca.2019.102481.

[A9]. Roohi A., Adeel M. and Shah M. A. (2019), "DDoS in IoT: A Roadmap Towards Security & Countermeasures," 2019 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, pp. 1-6, doi: 10.23919/IConAC.2019.8895034.

[A10]. Akbar M. A. et al. (2021) "A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors," in IEEE Access, vol. 9, pp. 128841-128861, doi: 10.1109/ACCESS.2021.3104527.

[A11]. Mahapatra, S.N., Singh, B.K. and Kumar, V. (2020). A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges. Arab J Sci Eng 45, 6211–6240. https://doi.org/10.1007/s13369-020-04461-2.

[A12]. Wustrich L., Pahl M. and Liebald S. (2020)."Towards an Extensible IoT Security Taxonomy," 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, pp. 1-6, doi: 10.1109/ISCC50000.2020.9219584.

[A13]. Mrabet, H. et al. (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. Sensors, 20(13), 3625. https://doi.org/10.3390/s20133625.

[A14]. Yang P., Xiong N. and Ren J. (2020). "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, doi: 10.1109/ACCESS.2020.3009876.

[A15]. Yin, X.C. et al. (2019). Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach. Sensors, 19(22), 4952. https://doi.org/10.3390/s19224952.

[A16]. Wazid, M et al. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. Journal of Systems Architecture, 97, pp. 185-196. doi: 10.1016/j.sysarc.2018.12.005.

[A17]. Sicato, J. C. S. et al. (2019). VPNFilter Malware Analysis on Cyber Threat in Smart Home Network. Appl. Sci. 9, 2763. https://doi.org/10.3390/app9132763.

[A18]. Panchal A. C., Khadse V. M. and Mahalle P. N. (2018). "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures". IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630.

[A19]. Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippoupolitis, A., Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home (Open Access). *Computers and Security*, 78, pp. 398-428. doi: 10.1016/j.cose.2018.07.011.

[A20]. Hayashi, Y., Verbauwhede I. and Radasky, W. A. (2018). "Introduction to EM information security for IoT devices". IEEE International Symposium on Electromagnetic Compatibility and IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), Suntec City, Singapore, pp. 735-738, doi: 10.1109/ISEMC.2018.8393878.

[A21]. Alqassem, I. and Svetinovic, D. (2014). "A taxonomy of security and privacy requirements for the Internet of Things (IoT)". IEEE International Conference on Industrial Engineering and Engineering Management, Selangor, Malaysia, pp. 1244-1248, doi: 10.1109/IEEM.2014.7058837.

[A22]. Reda, H.T., Anwar, A., Mahmood, A. (2022). Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts (Open Access). Renewable and Sustainable Energy Reviews, 163, art. no. 112423. doi: 10.1016/j.rser.2022.112423.

[A23]. Shah, Y. and Sengupta, S. (2020). "A survey on Classification of Cyber-attacks on IoT and IIoT devices," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, pp. 0406-0413, doi: 10.1109/UEMCON51285.2020.9298138.

[A24]. Zhao, W., Yang, S. and Luo X. (2020). "On Threat Analysis of IoT-Based Systems: A Survey," 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, pp. 205-212, doi: 10.1109/SmartIoT49966.2020.00038.

[A25]. Kamaldeep, Dutta, M. and Granjal, J. (2020). "Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms," in IEEE Access, vol. 8, pp. 127272-127312, doi: 10.1109/ACCESS.2020.3005643.

[A26]. Sookhak, M., Tang H. and Yu F. R. (2018). "Security and Privacy of Smart Cities: Issues and Challenge," 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, pp. 1350-1357, doi: 10.1109/HPCC/SmartCity/DSS.2018.00224.

[A27]. Prakash S. and Jaiswal S. (2018). "Security Challenges in IoT enabled Smart Grid: Taxonomy of Novel Techniques and Algorithm," 3rd International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, pp. 577-582, doi: 10.1109/ICICT43934.2018.9034345.

[A28]. Sfar, A. R., Chtourou Z. and Challal Y. (2017). "A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges". International Conference on Smart, Monitored and Controlled Cities (SM2C), Sfax, Tunisia, pp. 101-105, doi: 10.1109/SM2C.2017.8071828.

[A29]. Thing V. L. L. and Wu J. (2016). "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences". IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, pp. 164-170, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[A30]. Sookhak, M., Tang, H., He, Y. and Yu, F. R. (2019). "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Secondquarter, doi: 10.1109/COMST.2018.2867288.

[A31]. Patnaik, R., Srujan Raju, K., Sivakrishna, K. (2021). Internet of Things-Based Security Model and Solutions for Educational Systems. In: Kumar, R., Sharma, R., Pattnaik, P.K. (eds) Multimedia Technologies in the Internet of Things Environment. Studies in Big Data, vol 79. Springer, Singapore. https://doi.org/10.1007/978-981-15-7965-3_11.

[A32]. Han, T., Jan, S. R. U., Tan, Z., Usman, M., Jan, M. A., Khan, R., & Xu, Y. (2020). A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers. Concurrency and Computation: Practice and Experience, 32(16), e5300.

[A33]. Sahmi, I., Mazri, T. and Hmina, N. (2019). Study of the Different Security Threats on the Internet of Things and their Applications. In Proceedings of the 2nd International Conference on Networking, Information Systems & Security (NISS19). Association for Computing Machinery, New York, NY, USA, Article 68, 1–6. https://doi.org/10.1145/3320326.3320402.

[A34]. Benzarti, S., Triki, B. and Korbaa, O. (2017). "A survey on attacks in Internet of Things based networks," 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273006.

[A35]. Xu, H., Sgandurra, D., Mayes, K., Li, P., Wang, R. (2017). Analysing the Resilience of the Internet of Things Against Physical and Proximity Attacks. In: Wang, G., Atiquzzaman, M., Yan, Z., Choo, KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science, vol 10658. Springer, Cham. https://doi.org/10.1007/978-3-319-72395-2_27.

[A36]. Gupta, A., and Gupta, S. K. (2022). Flying through the secure fog: A complete study on UAV-Fog in heterogeneous networks. International Journal of Communication Systems, 35(13), e5237.

[A37]. Ali, R.F., Muneer, A., Dominic, P.D.D., Taib, S.M., Ghaleb, E.A.A. (2021). Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review. In: Abdullah, N., Manickam, S., Anbar, M. (eds) Advances in Cyber Security. ACeS 2021. Communications in Computer and Information Science, vol 1487. Springer, Singapore. https://doi.org/10.1007/978-981-16-8059-5_9.

[A38]. Rahimi, H., Zibaeenejad, A., Rajabzadeh, P. and Safavi A. A. (2018). On the Security of the 5G-IoT Architecture. In Proceedings of the international conference on smart cities and internet of things (SCIOT '18). Association for Computing Machinery, New York, NY, USA, Article 10, 1–8. https://doi.org/10.1145/3269961.3269968.

[A39]. Elham Kariri. (2022). IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment, IETE Journal of Research, DOI: 10.1080/03772063.2022.2032848.

8.1 Extração dos Dados

Seguindo o modelo de extração informado na seção anterior, os dados desejados foram identificados e extraídos dos artigos selecionados, a extração dos dados podem ser consultadas no apêndice deste relatório.

9. Relatório da Revisão

Nesta seção serão apresentados a listagem das vulnerabilidade identificadas na revisão executada. Foram identificadas 85 vulnerabilidades, em uma listagem não envolvendo os resultados do snowballing, destacadas na Tabela 1. As vulnerabilidades foram organizadas inicialmente em quatro categorias: *Device*, *Application, Network* e *Peopleware*.

Tabela 1 - Lista de Vulnerabilidades

Artigo	Vulnerabilidade	Categoria
[A8], [A17],[A34]	Access malicious link	Peopleware
[A1], [A6], [A9], [A17], [A25], [A38], [A31]	Buffer overflow	Application
[A19]	Channel interference	Network
[A8], [A19]	Channel voice	Physical
[A29]	Code Modification	Application
[A32]	Communication overhead	Network
[A19], [A23], [A30]	Connected to internet	Network
[A26]	Data and Computation Outsourcing	Application

[A5]	Data and Information Leakage	Network
[A8]	Data Inconsistency	Application
[A3],[A10],[A23],[A24],[A35]	Default configuration	App+Net
[A1], [A4], [A6], [A7], [A8], [A10], [A11], [A17], [A18], [A19], [A23], [A24], [A25], [A32], [A33], [A34], [A36], [A37], [A38], [A39]	Denial of service	Network
[A8]	Device spoofing	Network
[A7],[A8],[A12],[A19],[A20],[A24],[A25],[A34],[A36]	Device tampering	Physical
[A11],[A19],[A22],[A24],[A33],[A38]	Eavesdropping	Network
[A7],[A8],[A17],[A19],[A20],[A29],[A31],[A33],[A34],[A36],[A38],[A39]	Electromagnetic emanations leaking	Physical
[A11],[A16],[A22],[A30]	Energy restraints	Physical
[A4],[A6],[A7],[A8],[A10],[A11],[A12],[A16],[A17],[A33],[A34],[A38],[A39]	Fake/malicious node	Network
[A10],[A11],[A19],[A26]	Heterogeneous Interaction	App+Net
[A35]	Human manipulation/influence	Peopleware
[A19]	Identifying the product vendor	Peopleware
[A17],[A19]	Implement home networks on internet gateways	Network
[A21],[A26],[A30]	Improper Device Management	Physical
[A10]	Insecure application server	Network
[A5],[A10],[A11],[A26]	Insecure data transfer and storage	App+Net+Phy
[A30],[A31]	Insecure Initialization	Application
[A11],[A31],[A33]	Insecure Interfaces	App+Phy

[A5],[A23],[A31]	Insecure of Software/Firmware	Application
[A1],[A4],[A5],[A12],[A23]	Insecure Update Mechanisms	App+Net+Phy
[A5]	Insufficient IoT Device Testing	Physical
[A33]	IoT device network services	Application
[A5],[A12]	Know physical details	Peopleware
[A12]	Knowledge about the commands	Peopleware
[A9]	Lack data transmission range	Physical
[A5],[A11],[A24],[A33]	Lack of a secure update mechanism	Physical
[A2],[A4]	Lack of access control	App+Phy
[A5]	Lack of Active Device Monitoring	Application
[A1],[A2],[A5],[A10],[A11],[A14],[A18],[A19],[A23],[A25],[A26],[A27],[A29],[A30],[A31],[A36],[A37],[A38],[A39]	Lack of encrypting	App+Net+Phy
[A10]	Lack of firmware updates	Physical
[A7]	Lack of physical hardening	Physical
[A1],[A2],[A3],[A4],[A5],[A8],[A9],[A11],[A13],[A16],[A17],[A18],[A21],[A23],[A25],[A29],[A30],[A33],[A36],[A37]	Lack of proper authentication mechanisms	App+Net+Phy
[A5],[A7]	Lack of Proper Privacy Protection	Net+Phy
[A4],[A16],[A18],[A19],[A20],[A23],[A24],[A29]	Lack of side channel protection	App+Net+Phy
[A5]	Lack of standardization	Application
[A11]	Lack of technical support	Peopleware
[A5],[A19],[A22],[A24],[A25]	Lack secure communication protocols	Network
[A10]	Localization transmission	Physical
[A6],[A9],[A10],[A11],[A12],[A16],[A22],[A25],	Low computing power	Physical

[A28],[A30],[A33],[A37]		
[A9]	Low quality level code	Application
[A33],[A38]	Malicious Code	Application
[A23]	Malware in the network	Network
[A37]	Management of data	Application
[A8]	Manipulating the code execution flow of the device	Physical
[A7]	Manipulation of various control messages and system commands	Physical
[A8]	Memory leakage	Application
[A11]	Network protocol problems	Network
[A2],[A19],[A21],[A24]	Non-repudiation	Application
[A12],[A23]	Obtaining console access	Physical
[A10],[A17],[A19]	Personal and social circumstances	Peopleware
[A18],[A36],[A23],[A24],[A33],[A38]	Phishing	Peopleware
[A6],[A23],[A33],[A38],[A39]	Physical damage	Physical
[A16]	Physically stolen	Physical
[A11],[A12],[A17]	Poor physical security	Physical
[A18]	Remote Code Execution	Application
[A9]	Resource constraints	Physical
[A24]	Resource depletion	Network
[A32]	Single-point dependency	Network
[A8]	Sleep Denial	Physical
[A12],[A17],[A24],[A31],[A33],[A37]	Sleep deprivation	Physical
[A5],[A6],[A7],[A19],[A33],[A39]	Social engineering	Peopleware
[A25]	Software flaws	Peopleware

[A18]	Spoofing id	Physical
[A8]	Spoofing signal	Network
[A6],[A17],[A18],[A32],[A33]	SQL injections	Application
[A24]	Systems low-cost	Application
[A11],[A38]	Tag Cloning	Physical
[A6],[A7],[A8],[A24],[A29],[A32],[A33],[A38]	Unauthorized access	App+Net
[A5]	Unsecured network communications	Network
[A5]	Untrusted device acquisition	Peopleware
[A3],[A7],[A15],[A23]	Unused ports enabled	Network
[A5]	Vendor security posture	Peopleware
[A5],[A9],[A10],[A11],[A13],[A14],[A21],[A25],[A27],[A28],[A30],[A38],[A39]	Weak control access	App+Phy
[A4]	Weak credential management	Application
[A3],[A4],[A5],[A8],[A18],[A23],[A37]	Weak, guessable or default passwords	App+Net+Phy
[A19]	WiFi de-authentication	Network

10. Conclusão

Diante da expansão significativa pela qual os dispositivos IoT tem passado nos ultimos anos, é visível seu potencial de engajamento nos mais variados setores, o que requer uma atenção especial para como comporta e manipula seus dados, já que para tecnologias IoT a variedade de dados sensíveis é realmente grande.

Por esse motivo, a segurança nos ambientes IoT passa a ser um componente crucial para o funcionamento adequado desse tipo de tecnologia. E dentre os principais vetores associados à segurança, destacamos as Vulnerabilidades como campo de estudo com impacto significativo na retenção de danos associados à ameaças ou ataques que possam interferir diretamente no desempenho das tecnologias IoT.

Esse relatório busca apresentar um conjunto de vulnerabilidades identificadas no contexto da IoT, classificadas inicialmente entre quatro categorias ligadas às principais camadas da IoT (Física, Aplicação e Rede), com o acrescimo do *Peopleware,* onde são associadas as vulnerabilidades ligadas diremente ao agente humano. Foram catalogadas com as buscas 85 vulnerabilidades, dentre os estudos identificados apenas pela maquina de busca.

Este é um relatório parcial, o mesmo ainda está em andamento com a realização do *Snowballing*, a fim de complementar os resultados obtidos e tornar o trabalho ainda mais sólido.

APÊNDICE A – EXTRAÇÃO DE DADOS

A) Dados da publicação:	
Título:	SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems Based on Machine Learning
Autor(es):	Saha, T. and Aaraj, N. and Ajjarapu, N. and Jha, N.K.
Fonte de Publicação:	IEEE Transactions on Emerging Topics in Computing
Ano da Publicação:	2022
Resumo:	Cyber-physical systems (CPS) and Internet-of-Things (IoT) devices are increasingly being deployed across multiple functionalities, ranging from healthcare devices and wearables to critical infrastructures, e.g., nuclear power plants, autonomous vehicles, smart cities, and smart homes. These devices are inherently not secure across their comprehensive software, hardware, and network stacks, thus presenting a large attack surface that can be exploited by hackers. In this article, we present an innovative technique for detecting unknown system vulnerabilities, managing these vulnerabilities, and improving incident response when such vulnerabilities are exploited. The novelty of this approach lies in extracting intelligence from known real-world CPS/IoT attacks, representing them in the form of regular expressions, and employing machine learning (ML) techniques on this ensemble of regular expressions to generate new attack vectors and security vulnerabilities. Our results show that 10 new attack vectors and 122 new vulnerability exploits can be successfully generated that have the potential to exploit a CPS or an IoT ecosystem. The ML methodology achieves an accuracy of 97.4 percent and enables us to predict these attacks efficiently with an 87.2 percent reduction in the search space. We demonstrate the application of our method to the hacking of the in-vehicle network of a connected car. To defend against the known attacks and possible novel exploits, we discuss a defense-in-depth mechanism for various classes of attacks and the classification of data targeted by such attacks. This defense mechanism optimizes the cost of security measures based on the sensitivity of the protected resource, thus incentivizing its adoption in real-world CPS/IoT by cybersecurity practitioners
B) Dados derivados do objetivo:	
Vulnerabilidades	“Due to the absence of sender and receiver addresses in the data frames, every ECU can freely publish and receive messages from the bus. While this enables

	easier addition of new ECUs to the network, it poses a grave security threat to the system." "This allows a malicious node on the CAN bus to receive all the data frames through sniffing. The absence of encryption makes it easier to analyze the collected frames." "Using the details of the data frames, the adversary can broadcast malicious frames on the bus by spoofing a particular node. Absence of authentication schemes compromises the integrity of messages on the CAN bus" "Denial of Service (DoS): The CAN protocol implements a priority-based broadcasting communication scheme. For example, messages from the anti-lock braking system, which are critical to the safety of the passengers, are given higher priority for transmission on the bus than messages from climate control sensors." "Since the CAN protocol is bereft of authentication schemes and time-stamp verification, the recorded frame packets can be sent on the CAN bus at inconvenient time instances to launch various attacks." "The other vulnerabilities that we consider in our experiments are ECU buffer overflows" "and malware injection through ECU firmware updates"

A) Dados da publicação:	
Título:	Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach
Autor(es):	Abuemera, E.A. and Elzouka, H.A. and Saad, A.A.
Fonte de Publicação:	2nd International Conference on Consumer Electronics and Computer Engineering, ICCECE
Ano da Publicação:	2022
Resumo:	Cyber security is still the main argument in any system development lifecycle that needs more concern. There are still numerous challenges associated with conducting a threat modeling approach for smart manufacturing systems. One of these challenges is the lack of a threat database based on the expertise of highly skilled researchers in this field. Hence this study attempts to address this gap by developing a

	components catalog and a rule-based threat database to address potential security threats in smart manufacturing systems saving time and effort. Specifically, it performs STRIDE-based threat modeling against a smart factory use case using Microsoft Threat Modelling Tool. The threat evaluation process is conducted with this research to determine the severity of threats and give a preliminary estimation of the overall system's risk
B) Dados derivados do objetivo:	
Vulnerabilidades	“Due to a lack of authentication across communicating processes, spoofing the processes” “In the use case, there is no method for logging and recording events. As a result, the processes are vulnerable to repudiation threats and might deny previous events” “Information disclosure threats are due to the lack of encryption. Attackers can simply decode and understand unencrypted messages.” “Although most elevation of privilege threats is due to the lack of access control rules based on authorization, the elevation of privilege on EE-1 by tricking the operator into opening a crafted PowerPoint document is due to Windows OLE Remote Code Execution vulnerability”

A) Dados da publicação:	
Título:	Security in IoT-based smart homes: A taxonomy study of detection methods of mirai malware and countermeasures
Autor(es):	Auliar, R.B. and Bekaroo, G.
Fonte de Publicação:	International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME
Ano da Publicação:	2021
Resumo:	During recent years, there has been widespread adoption of the Internet and swift digitization within various sectors, including smart homes. These also led to the rapid growth of the Internet of Things (IoT), which is expected to proliferate further, where 50 billion IoT devices are estimated to be connected to the Internet by 2030. However, the growth in connected IoT devices to the Internet has not been without challenges. IoT devices are known to have various vulnerabilities that could be exploited by

	attackers, thus hindering security of devices and users. Recently, the use of Mirai malware by attackers gained significant attention as it has the capability to transform IoT connected devices into remotely controlled bots, which can be utilized as part of a botnet in large-scale network attacks. Taking cognizance of the importance to secure against this type of malware, this study presents a taxonomy review on the techniques that can potentially be used to detect Mirai malware along with countermeasures for securing against such malware
B) Dados derivados do objetivo:	
Vulnerabilidades	“Strengthening Password Protection - Each device must consist of a unique password instead of common passwords for specific model since Mirai botnets target lists of hardcoded passwords” “Disabling Unused Ports - Unused ports such as SSH, and Telnet among others should be disabled by default for end users might not be aware of open ports and could hence be targeted by Mirai botnets.” “Monitoring Open Ports - Open ports should be monitored to analyze traffic that could source from a malicious origin.” “Restructuring Device Firmware - Device firmware are often exploited via the use of various methods and tools that analyze firmware for issues pertaining to authentication and to bypass backdoors” “Ensuring Proper Configuration - In addition, open connections must not be with default configuration for wireless communications.”

A) Dados da publicação:	
Título:	SoK: Investigation of security and functional safety in industrial IoT
Autor(es):	Tomur, E. and Gulen, U. and Soykan, E.U. and Akif Ersoy, M. and Karakoc, F. and Karacay, L. and Comak, P.
Fonte de Publicação:	IEEE International Conference on Cyber Security and Resilience, CSR
Ano da Publicação:	2021

Resumo:	There has been an increasing popularity of industrial usage of Internet of Things (IoT) technologies in parallel to advancements in connectivity and automation. Security vulnerabilities in industrial systems, which are considered less likely to be exploited in conventional closed settings, have now started to be a major concern with Industrial IoT. One of the critical components of any industrial control system turning into a target for attackers is functional safety. This vital function is not originally designed to provide protection against malicious intentional parties but only accidents and errors. In this paper, we explore a generic IoT-based smart manufacturing use-case from a combined perspective of security and functional safety, which are indeed tightly correlated. Our main contribution is the presentation of a taxonomy of threats targeting directly the critical safety function in industrial IoT applications. Besides, based on this taxonomy, we identified particular attack scenarios that might have severe impact on physical assets like manufacturing equipment, even human life and cyber-assets like availability of Industrial IoT application. Finally, we recommend some solutions to mitigate such attacks based mainly on industry standards and advanced security features of mobile communication technologies.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Unauthorized physical access of any malicious party to the devices belonging to the safety control system may present a threat to take control of a safety-related asset like Safety Program” “Manipulation of Software - Attacks are possible on assets which can be used to configure and parameterize the safety systems like Engineering Workstation. Malicious modifications of safety programs, safety parameters or any other software/hardware on safety controller, safety actuator and safety sensor can be done to adversely affect the operation of functional safety” “There can be attacks that aim malicious intervening with cyclic communication between Safety Controller (Safety Program), Safety Actuator and Safety Sensor. Attacker may aim to obstruct, destruct or modify” “Attacks can be performed on the Safety Controller over network via its remote programming or monitoring interfaces. Similar to the reported weaknesses in IoT

	devices, safety controllers are also prone to weak authentication and authorization practices." "If they are accessible remotely, any type of attacker may try to break authentication, for instance, by using unchanged default passwords or applying a brute force attack" "Vulnerabilities in built-in security features of safety devices (actuator, sensor or controller) can be exploited because of weak credential management, firmware update from untrusted source or lack of side channel protection". "Malware injected into Safety Program either directly or indirectly via Engineering Workstation can allow attackers to manipulate safety program code in such a way that it does not command switching into fail-safe mode when there is potentially dangerous situation or it commands to do so when there is no such situation." "(Denial of Service): Injection of a high volume of packets in the OT network or flooding of malicious traffic to overload system resources in Safety Program by attackers can cause disruption in timely operation of the overall safety function."

A) Dados da publicação:	
Título:	A Review of Security Standards and Frameworks for IoT-Based Smart Environments
Autor(es):	Karie, N.M. and Sahri, N.M. and Yang, W. and Valli, C. and Kebande, V.R.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2021
Resumo:	Assessing the security of IoT-based smart environments such as smart homes and smart cities is becoming fundamentally essential to implementing the correct control measures and effectively reducing security threats and risks brought about by deploying IoT-based smart technologies. The problem, however, is in finding security standards and assessment frameworks that best meets the security requirements as well as comprehensively assesses and exposes the security posture of IoT-based smart environments. To explore this gap, this paper presents a review of existing security standards and assessment frameworks which also includes several NIST special publications on security techniques highlighting their

	primary areas of focus to uncover those that can potentially address some of the security needs of IoT-based smart environments. Cumulatively a total of 80 ISO/IEC security standards, 32 ETSI standards and 37 different conventional security assessment frameworks which included 7 NIST special publications on security techniques were reviewed. To present an all-inclusive and up-to-date state-of-the-art research, the review process considered both published security standards and assessment frameworks as well as those under development. The findings show that most of the conventional security standards and assessment frameworks do not directly address the security needs of IoT-based smart environments but have the potential to be adapted into IoT-based smart environments. With this insight into the state-of-the-art research on security standards and assessment frameworks, this study helps advance the IoT field by opening new research directions as well as opportunities for developing new security standards and assessment frameworks that will address future IoT-based smart environments security concerns. This paper also discusses open problems and challenges related to IoT-based smart environments security issues. As a new contribution, a taxonomy of challenges for IoT-based smart environment security concerns drawn from the extensive literature examined during this study is proposed in this paper which also maps the identified challenges to potential proposed solutions.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Data and Information Leakage: In any IoT smart environment, without proper security mechanisms that protect data and information from malware and other malicious intruders, personal information could easily be leaked resulting in security breaches.” “With information moving in and around IoT-based smart environments and over to the Internet, malicious attackers can take advantage of unsecured network communications and steal data as it is being transmitted between the connected IoT devices which can lead to other serious security breaches.” “Many cloud-based IoT devices and systems are known to have security vulnerabilities and can easily be victims of hacking and cyberattacks as data transmission like video data from cameras may not even be encrypted when sent over the internet.”

	“Because of the lack of standardization in many IoT-based smart environments, rogue software can easily find its way into IoT devices through firmware upgrade and trusted boot, device acquisition as well as apps and services.” “Because of the lack of specialized universal approved IoT security standards or security assessment frameworks, some devices may be manufactured with poor security baselines such as old and unpatched embedded operating systems and software, weak, guessable, or hard-coded passwords, insecure data transfer and storage, among others. This makes such IoT devices vulnerable to different security threats and attacks.” “With the growing innovation of IoT technologies, many users are yet to understand how modern IoT devices are designed and function. This makes it easy for attackers to use social engineering to trick IoT device users into providing sensitive data or information which can be used to gain access into smart environment networks, such as smart homes and smart cities, putting everyone’s life at risk.” “Insufficient IoT Device Testing and Updates: Most of the IoT devices are produced quickly to meet the increasing market demands and hence do not undergo proper testing or follow any acceptable security standards or assessment frameworks” “Users mostly put their trust in the manufactures to test the IoT devices as well as provide security control measures. However, due to high demands, many manufacturers focus more on creating and releasing new products to the market without having proper testing or putting security control measures in place.” “Lack of Active Device Monitoring: Monitoring IoT devices can be challenging. This is because most of the existing monitoring tools and practices especially those focusing on the cloud were traditionally designed to monitor time-series metric data with no focus on modern IoT devices or their processes.” “The lack of efficient and robust security protocols including proper IoT security standards, assessment frameworks and safeguards could lead to security breaches in smart environments leading to personal data exfiltration.”

	“With many IoT devices in smart environments lacking strong authentication or access control mechanisms, it becomes easy for intruders to impersonate a legitimate user and use the credentials or any other information that gives them access to existing IoT resources in an IoT-based smart environment.” “Denial of Service (DoS/DDoS): With the advancement in technology, hackers can try to cause a DoS/DDoS to existing hubs in IoT-based smart environment networks or the sensors themselves.” “With the rapid growth in the number and usage of IoT devices, other security threats may also exist in IoT-based smart environments such as home invasions, trespass, falsification rogue and counterfeit IoT devices, botnet attacks, physical attacks, unintentional damage or loss, disasters and outages, failures or malfunctions, dynamic systems, authentication, unsecured wireless network problems, side-channel attack, man-in-the-middle, identity theft, advanced persistent threat (APT), jamming, function creep, buffer overflow, large-scale unauthorized data mining, surveillance, unauthorized access or deletion or modification of data, worms, viruses and malicious code, the openness of the networked systems, weak passwords, fixed firmware, resource constraints, headless nature of IoT devices, tamper-resistant packages, heterogeneous protocols, dynamic characteristics, longevity expectations among many other security threats.”

A) Dados da publicação:	
Título:	Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study
Autor(es):	Davis, B.D. and Mason, J.C. and Anwar, M.
Fonte de Publicação:	IEEE Internet of Things Journal
Ano da Publicação:	2020
Resumo:	Internet-of-Things (IoT) technology has revolutionized our daily lives in many ways-whether it is the way we conduct our day-to-day activities inside our home, or the way we control our home environments remotely. Unbeknownst to the users, with the adoption of these 'smart home' technologies, their personal space becomes vulnerable to security and privacy attacks. We conducted studies of vulnerabilities and security posture of smart home IoT devices. We started with a

	literature review on known vulnerability studies of the IoT devices, considering four categories of attacks: 1) physical; 2) network; 3) software; and 4) encryption. We then conducted our own vulnerability experiments that compared security postures between well known and lesser known vendors through misuse and abuse case analysis, followed by a review of coverage in major vulnerability databases. Based on our analysis, the main finding was the need for a stronger focus on the security posture of lesser known vendor devices as they are often less regulated and faceless scrutiny.
B) Dados derivados do objetivo:	
Vulnerabilidades	1) Physical: “Some physical attacks are as follows: node tampering, radio-frequency (RF) interference on RF identifiers (RFIDs), node jamming in wireless sensor networks, malicious node injection, physical damage, social engineering, sleep deprivation, and malicious code injection.” 2) Network: “The network attacks identified in [9] are traffic analysis, RFID spoofing/cloning/unauthorized access, sinkhole, man in the middle, Denial of Service (DoS), routing information, and sybil.” 3) Software: “Some of the software attacks that have been presented in [9] are phishing, malicious scripts, Trojan horse, spyware, adware, and DoS that exploit buffer overflows, SQL injections, and other types of vulnerabilities.” 4) Encryption: “Because IoT devices have limited computing power to support strong cryptographic protocols, they are vulnerable to the side channel, cryptanalysis, and man-in-the-middle attacks.” “The main vulnerability that exists is the “motherboard hack” vulnerability. The motherboard hack is an attack where the bulb is cracked open gaining access to the motherboard within the smart light bulb. Some manufactures store unencrypted information, e.g., WiFi SSID and encryption key in plaintext, in this location.”

A) Dados da publicação:	
Título:	Securing Cyberspace of Future Smart Cities with 5G Technologies
Autor(es):	Akhunzada, A. and Islam, S.U. and Zeadally, S.
Fonte de Publicação:	IEEE Network
Ano da Publicação:	2020
Resumo:	Future smart cities promise to dramatically improve the quality of life and have been attracting the attention of many researchers in recent years. The integration of IoT with their corresponding service delivery models to manage a city's asset securely remains a significant challenge. The deployment of diverse IoT technologies and several architectural components and novel entities of emerging ICT solutions opens up new security threats and vulnerabilities. Large-scale, seamless communication among multiple IoT technologies is highly dependent on the operations of the underlying wireless access technologies such as WSNs, SDR, CR and RFID. We present thematic layered taxonomies to highlight the potential security vulnerabilities, attacks, and challenges of key IoT enabling technologies which underpin the development of smart cities. We also identify potential requirements and key enablers that play a vital role in the development of secure smart cities. Finally, we discuss various open issues that need to be addressed to unlock the full potential of 5G for future smart cities.
B) Dados derivados do objetivo:	
Vulnerabilidades	“To start with, the wide deployment of SDR requires an adequate level of physical safety and security. SDR (Software Defined Radio) has reconfiguration capabilities which enable it to download various new radio applications and diverse communication links. Consequently, SDR is vulnerable to malicious modifications and injections due to its open communication without any integrity checks on the transmitted data.” “Device cloning is a frequently used term in traditional wireless communications. It represents unauthorized access to diverse services offered by another SDR device. Device cloning is a major security threat to the emerging 5G communication networks.” “Moreover, SDR devices and components are easily programmable and accessible in an open environment and are vulnerable to sophisticated MATE attacks.” “The physical layer is vulnerable to sophisticated attacks such as unauthorized access, which

	subsequently leads to alteration of cognitive messages, and jamming attacks that severely affect spectrum sensing and sharing abilities. Moreover, the physical layer is also vulnerable to disruption of the cognitive engine as well as masquerading both as a primary user and a cognitive node." "Moreover, the physical layer is also vulnerable to manipulation of various control messages and system commands. The physical layer is also vulnerable to channel interference." "The strategic layer of RFID is vulnerable to location privacy attacks and social engineering attacks." "The network layer can also experience spoofing attacks, selective forwarding attacks, and is vulnerable to a variety of DoS attacks." "For instance, to ensure the availability of the SDR, the underlying operating system must be designed with features that do not allow backdoor accounts and patches with vulnerable open ports and services."

A) Dados da publicação:	
Título:	A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT
Autor(es):	Sengupta, J. and Ruj, S. and Das Bit, S.
Fonte de Publicação:	Journal of Network and Computer Applications
Ano da Publicação:	2020
Resumo:	In recent years, the growing popularity of Internet of Things (IoT) is providing a promising opportunity not only for the development of various home automation systems but also for different industrial applications. By leveraging these benefits, automation is brought about in the industries giving rise to the Industrial Internet of Things (IIoT). IoT is prone to several cyberattacks and needs challenging approaches to achieve the desired security. Moreover, with the emergence of IIoT, the security vulnerabilities posed by it are even more devastating. Therefore, in order to provide a guideline to researchers, this survey primarily attempts to classify the attacks based on the objects of vulnerability. Subsequently, each of the individual attacks is mapped to one or more layers of the generalized IoT/IIoT architecture followed by a discussion on the countermeasures proposed in literature. Some relevant real-life attacks for each of

	these categories are also discussed. We further discuss the countermeasures proposed for the most relevant security threats in IIoT. A case study on two of the most important industrial IoT applications is also highlighted. Next, we explore the challenges brought by the centralized IoT/IIoT architecture and how blockchain can effectively be used towards addressing such challenges. In this context, we also discuss in detail one IoT specific Blockchain design known as Tangle, its merits and demerits. We further highlight the most relevant Blockchain-based solutions provided in recent times to counter the challenges posed by the traditional cloud-centered applications. The blockchain-related solutions provided in the context of two of the most relevant applications for each of IoT and IIoT is also discussed. Subsequently, we design a taxonomy of the security research areas in IoT/IIoT along with their corresponding solutions. Finally, several open research directions relevant to the focus of this survey are identified.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Refers to the act of physically modifying a device (e.g. RFID) or communication link.” “Here the attacker injects malicious code onto a physical device by compromising it which may help him/her launch other attacks too.” “RF Interference/Jamming: Attacker creates and sends noise signals over the Radio Frequency (RF)/WSN signals to launch DoS attacks on the RFID tags/sensor nodes thereby hindering communication.” “Fake Node Injection: Attacker drops a fake node between two legitimate nodes of the network to control data flow between them.” “Sleep Denial Attack: Attacker keeps the battery powered devices awake by feeding them with wrong inputs. This causes exhaustion in their batteries leading to shutdown.” “Side Channel Attack: In this attack, the attacker collects the encryption keys by applying timing, power, fault attack etc.” “Permanent Denial of Service (PDoS): Also known as phlashing, is a type of DoS attack, wherein an IoT device is completely damaged via hardware sabotage.

	The attack is launched by destroying firmware or uploading a corrupted BIOS using a malware." "For example, using device spoofing attack, attackers can obtain a camera's password of any length and combination. Also by enumerating all possible MAC addresses the attacker can launch device scanning attack to find all online cameras." "Their experiments reveal that the home automation system is vulnerable to brute force attacks revealing the passwords. It also reveals that the smart meters can be hijacked to launch ransomware attacks against other systems." "security vulnerabilities of Virtual Personal Assistant (VPA) based IoT devices such as Amazon Echo and Google Home. These systems are vulnerable to attacks like voice squatting and voice masquerading." "RFID Spoofing: The attacker first spoofs an RFID signal to get access of the information imprinted on the RFID tag." "RFID Unauthorized Access: An attacker is able to read, modify or delete data present on RFID nodes because of the lack of proper authentication mechanisms. "In a wormhole attack, an attacker maliciously prepares a low-latency link and then tunnels packets from one point to another through this link." "Here, a single malicious node claims multiple identities (known as sybil nodes) and locates itself at different places in the network." "An attacker may capture a signed packet and resend the packet multiple number of times to the destination. This keeps the network busy leading to a DoS attack. "in DDoS multiple compromised nodes attack a specific target by flooding messages, or connection requests to slow down or even crash the system server/network resource." "Data Inconsistency: In IoT, attack on data integrity leading to inconsistency of data in transit or data stored in a central database is referred to as Data Inconsistency."

	“Access control implies giving access to authorized users and denying access to unauthorized users. With unauthorized access, malicious users can gain data ownership or access sensitive data.” “Data breach or memory leakage refers to the disclosure of personal, sensitive or confidential data in an unauthorized manner.”

A) Dados da publicação:	
Título:	DDoS in IoT: A roadmap towards security countermeasures
Autor(es):	Roohi, A. and Adeel, M. and Shah, M.A.
Fonte de Publicação:	25th IEEE International Conference on Automation and Computing
Ano da Publicação:	2019
Resumo:	In this era of digitization, more and more technologies are spurring up but are failing to make a successful impact due to the security and privacy issues. Internet of Things (IoT) has made its mark recently and being end-consumer oriented, makes it more prone towards being exploited. There are many types of security attacks in the IoT which can compromise the end user data and services. The most common and devastating security attack in the IoT is a Denial of Service (DoS)/Distributed Denial of Service (DDoS) attack. In this paper, the contributions are: we provide a structured comprehensive overview of the existing research on DDoS Attacks, its security countermeasures in the context of IoT. We survey latest vulnerabilities and their security solutions over the period 2014-2019. With elaborate discussion on IoT architecture and underlying security threats impacting each layer in the IoT, we have grouped existing approaches and derived taxonomy. With this concise overview, the paper seeks to provide an understanding of the pertaining models adopted by different researchers.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Devices being used at Perception Layer experience resource constraints with respect to their application at the user end. Moreover, technologies such as RFID, NFC, Bluetooth, ZigBee e.t.c lack data transmission range which can be exploited by the intruder.” “Middleware layer is responsible for analyzing the data which has been collected via the sensor nodes. Computational and processing resources are required

	extensively on this layer. Securing data in this layer which is usually referred as cloud and authentication are concerns which are to be addressed” “Attacker usually targets unauthorized access towards the Application being used which is usually available via the Internet. This User Interface extends attackers access to sensitive data of the user which through different penetration techniques, vulnerabilities, bugs in the programs, low quality level code, inducing buffer overflow e.t.c.”

A) Dados da publicação:	
Título:	A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors
Autor(es):	Akbar, M.A. and Alsanad, A. and Mahmood, S. and Alothaim, A.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2021
Resumo:	Internet of things (IoT) is leading a new digital age. IoT is regarded as the significant frontier that can improve almost all aspect of our lives. Currently, the IoT technology faces several challenges to academic researchers and industry practitioners, mainly that related with security of data. The objective of this study is to develop a prioritization-based taxonomy of the challenging factors that could hinders the security of IoT. By conducting the literature review and questionnaire survey studies 21 challenging factors were identified that are reported in existing literature and in real-world practices. Moreover, the identified challenging factors are mapped in the core domain of IoT (i.e. smart city, smart home, smart wearable's and smart health care); and apply the fuzzy-AHP approach to rank the identified challenging factors with respect to their criticality for security of IoT technology. The application of fuzzy-AHP is novel in this research area as it is successfully applied in other domains of information technology to address the multi-criterion decision making problems. This study is contributing by providing a prioritization-based taxonomy of the IoT security challenging factors that could help the practitioners and research community to revise and develop the new strategies for the secure IoT.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Smart cities comprised of several heterogenous IoT devices in order to achieve various objectives. However, malicious IoT node could be connected to

	IoT system in order to collect and exchange data from other devices.“ “Increasing number of IoT devices connected to smart city will generate huge amount of data. However, these devices do not have potential to store and process data, therefore data generated by these devices need to be sent to cloud in order to process and analyze.” “Thus, IoT devices do not have enough capability to encrypt and decrypt data that pose the integrity and authenticity of data as critical challenge.” “Generally, cryptographic algorithms are used to ensure data privacy from unauthorized access. Due to low power and computation of IoT devices there is a risk of malicious attacks and leakage of personal information, as advanced cryptographic techniques could not be employe” “The smart world anticipated that several smart home appliances will be interconnected to home network. However, these devices need to be configured to home network repetitively and may prone to different security attacks. This could be tedious task for householder in order to manage these devices manually so external expert need to be called to control several security threats.” “However, IoT devices consisting of software and hardware are less in numbers and due to heterogeneous nature, firmware is not updated frequently that causes a variety of security threats.” “Thus, firmware of IoT devices for smart homes need to be updated automatically in order to cope with novel security vulnerability, as there is lack of technical support.” “Smart home network could be compromised by attacker and permit them to send RTS (Request to send)/CTS (clear to send) messages in bulk. Thus, smart devices should be capable enough to stop these devices from receiving messages in bulk and deplete their resources.”

	“Interdependence Behavior of Devices - Various smart home devices connected each other in a network in order to achieve a particular objective. “ “However, location could be altered by attackers if he/she could receive radio signal and analyze them, if the location information altered by attacker this could impede emergency services.” “Smart devices come without any built-in security mechanism and these devices store data locally without any encryption method.” “Furthermore, strong cryptographic algorithm could not be implemented because these devices are resource constrained.”

A) Dados da publicação:	
Título:	A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges
Autor(es):	Mahapatra, S.N. and Singh, B.K. and Kumar, V.
Fonte de Publicação:	Arabian Journal for Science and Engineering
Ano da Publicação:	2020
Resumo:	Internet of things (IoT) is one of the emerging paradigms in the current era that has attracted many researchers due to its widespread applications. Due to the open nature of the device accessibility and heterogeneity, a rapid increase in connected devices leads to several vulnerabilities and threats in the IoT devices. Hence, security is one of the important concern and main challenge to be addressed for the guaranteed data transmission in IoT environment. In this review work, we analyze the secure transmission of data in IoT and investigate the recent approaches in IoT security and their requirements and open issues. We present a taxonomy model for the secure transmission in IoT security which includes architecture/layers, communication topology, and classification techniques which are categorized under cluster, trust, routing, blockchain, and location-based approaches. First, we briefly discuss the architecture of the IoT ecosystem that consists of three layers namely perception, network, and application layer

	which support the basic task such as transmission, sensing, and processing. Next, we classify the communication mechanism into different scenarios involved in the various network for the transmission of data in the IoT environment. Then, we investigate the recent approaches for secure communication to overcome certain attacks in IoT and analyze their strength and limitations. Finally, we discuss the security requirements, threats, and vulnerabilities faced by the current IoT system, and numerous open research challenges that are needed to be addressed for the efficient transmission of data as future research directions.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Currently, security factors such as privacy, secure storage and management, authorization, and communication as well as access control are the critical and challenging issues in the IoT environment.” “Due to the limited processing capability, traditional security methods suffer from various setbacks and often do not detect the physical threats in the network.” “So, proper authentication and encryption are required for preventing such attacks from the spiteful users.” “In this technology, there are some of the possible vulnerabilities, unauthorized tag cloning, attacks on availability and authenticity, spoofing, counterfeiting, DoS attack, eavesdropping, and replay attacks.” “However, there are several security threats and vulnerabilities faced by cloud users, such as identity management, and heterogeneity issues in IoT devices that makes the data transmission unreachable to an user identity authentic node, physical and infrastructure security, encryption, data access controls, system complexity, and misconfiguration of software.” “There are several reasons in observing the cyber-attacks are: Many IoT devices can be operated by unattended humans, thus it is easy for an attacker to access and an adversary can steal sensitive data over wireless networks by eavesdropping.” “Some of the security issues with IoT devices such as insecure mobile interface, insufficient authentication, and insecure network service, and poor physical

	security, lack of transport encryption, privacy concerns, and insecure web interface insufficient security configurability.” “The IoT connected resources have more demand for updating and the frequency of the messages causes latency which results in network vulnerabilities.” “Due to the hardware limitations on storage, processing, and energy, high overhead and data traffic is a critical criterion in the field of secure data transmission.”

A) Dados da publicação:	
Título:	Towards an Extensible IoT Security Taxonomy
Autor(es):	Wüstrich, L. and Pahl, M.-O. and Liebald, S.
Fonte de Publicação:	IEEE Symposium on Computers and Communications , Vol. 2020-July
Ano da Publicação:	2020
Resumo:	Security is essential in the Internet of Things (IoT). IoT threat classifications are often non-intuitive to use. Identifying relevant properties of an attack is difficult and requires reading details of the attack. We therefore propose a simple-to-use naming scheme for IoT threat classification. It is based on the affected layers and the affected security goals. We evaluate the usefulness of the chosen approach by applying it to common IoT threats.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Access to devices and the capability to record and replay a signal are sufficient for this attack. As the attacker then impersonates a legitimate sender” “In order to save energy, some devices have a sleep mode. The attacker interacts with the device to prevent it from entering the low powered mode to drain its battery.” “This renders the device unavailable (CP.AVAIL). For a success, adversary needs network access to interact with the node. It also needs knowledge about the commands it can send to the node to keep it from the sleep mode.”

	“IoT devices embedded into the environment they can also be physically damaged” “Another class of attacks that predominantly affects devices on CP due to their limited computing power and level of exposure are side channel attacks” “By analyzing physical characteristics like power consumption of the device during computations the secret is inferred” “In a Sybil attack, the adversary assumes multiple identities of other nodes in the network” “In case an attacker is able modify the running application by using malware, a Trojan horse or is able to install a malicious update, the integrity on the application layer is violated”

A) Dados da publicação:	
Título:	A survey of IoT security based on a layered architecture of sensing and data analysis
Autor(es):	Mrabet, H. and Belguith, S. and Alhomoud, A. and Jemai, A.
Fonte de Publicação:	Sensors (Switzerland)
Ano da Publicação:	2020
Resumo:	The Internet of Things (IoT) is leading today’s digital transformation. Relying on a combination of technologies, protocols, and devices such as wireless sensors and newly developed wearable and implanted sensors, IoT is changing every aspect of daily life, especially recent applications in digital healthcare. IoT incorporates various kinds of hardware, communication protocols, and services. This IoT diversity can be viewed as a double-edged sword that provides comfort to users but can lead also to a large number of security threats and attacks. In this survey paper, a new compacted and optimized architecture for IoT is proposed based on five layers. Likewise, we propose a new classification of security threats and attacks based on new IoT architecture. The IoT architecture involves a physical perception layer, a network and protocol layer, a transport layer, an application layer, and a data and cloud services layer. First, the physical sensing layer incorporates the basic hardware used by IoT. Second, we highlight the various network and protocol technologies employed

	by IoT, and review the security threats and solutions. Transport protocols are exhibited and the security threats against them are discussed while providing common solutions. Then, the application layer involves application protocols and lightweight encryption algorithms for IoT. Finally, in the data and cloud services layer, the main important security features of IoT cloud platforms are addressed, involving confidentiality, integrity, authorization, authentication, and encryption protocols. The paper is concluded by presenting the open research issues and future directions towards securing IoT, including the lack of standardized lightweight encryption algorithms, the use of machine-learning algorithms to enhance security and the related challenges, the use of Blockchain to address security challenges in IoT, and the implications of IoT deployment in 5G and beyond.
B) Dados derivados do objetivo:	
Vulnerabilidades	“According to the 2017 OWASP application security flaws review, the ten most critical web application security risks are: injection, broken authentication, sensitive data exposure, XML external entities (XXE), broken access control, security misconfiguration, cross-site scripting (XSS), insecure deserialization, and using components with known vulnerabilities.”

A) Dados da publicação:	
Título:	Data Security and Privacy Protection for Cloud Storage: A Survey
Autor(es):	Yang, P. and Xiong, N. and Ren, J.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2020
Resumo:	The new development trends including Internet of Things (IoT), smart city, enterprises digital transformation and world's digital economy are at the top of the tide. The continuous growth of data storage pressure drives the rapid development of the entire storage market on account of massive data generated. By providing data storage and management, cloud storage system becomes an indispensable part of the new era. Currently, the governments, enterprises and individual users are actively migrating their data to the cloud. Such a huge amount of data can create magnanimous wealth. However, this increases the possible risk, for instance, unauthorized access, data leakage, sensitive information disclosure and privacy

	disclosure. Although there are some studies on data security and privacy protection, there is still a lack of systematic surveys on the subject in cloud storage system. In this paper, we make a comprehensive review of the literatures on data security and privacy issues, data encryption technology, and applicable countermeasures in cloud storage system. Specifically, we first make an overview of cloud storage, including definition, classification, architecture and applications. Secondly, we give a detailed analysis on challenges and requirements of data security and privacy protection in cloud storage system. Thirdly, data encryption technologies and protection methods are summarized. Finally, we discuss several open research topics of data security for cloud storage.
B) Dados derivados do objetivo:	
Vulnerabilidades	“When data is outsourced to the cloud, its security is vulnerable. Encryption is an effective technique to protect data security. The essence of data encryption is to transform the original plaintext file or data into an string of unreadable code by some algorithms, which is usually called ciphertext.” “Besides, identity and attribute leakage issues are also threatening the privacy of data owners and authorized users.”

A) Dados da publicação:	
Título:	Toward an applied cyber security solution in iot-based smart grids: An intrusion detection system approach
Autor(es):	Yin, X.C. and Liu, Z.G. and Nkenyereye, L. and Ndibanje, B.
Fonte de Publicação:	Sensors (Switzerland)
Ano da Publicação:	2019
Resumo:	We present an innovative approach for a Cybersecurity Solution based on the Intrusion Detection System to detect malicious activity targeting the Distributed Network Protocol (DNP3) layers in the Supervisory Control and Data Acquisition (SCADA) systems. As Information and Communication Technology is connected to the grid, it is subjected to both physical and cyber-attacks because of the interaction between industrial control systems and the outside Internet environment using IoT technology. Often, cyber-attacks lead to multiple risks that affect infrastructure and business continuity; furthermore, in some cases, human beings are also affected. Because of the traditional peculiarities of process systems, such

	as insecure real-time protocols, end-to-end general-purpose ICT security mechanisms are not able to fully secure communication in SCADA systems. In this paper, we present a novel method based on the DNP3 vulnerability assessment and attack model in different layers, with feature selection using Machine Learning from parsed DNP3 protocol with additional data including malware samples. Moreover, we developed a cyber-attack algorithm that included a classification and visualization process. Finally, the results of the experimental implementation show that our proposed Cybersecurity Solution based on IDS was able to detect attacks in real time in an IoT-based Smart Grid communication environment.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Attacks often happen by using steps such as reconnaissance, which consists of gathering information about the targeted system; scanning, which is about finding any weakness or vulnerability in the system by looking for any open ports; and running a service through the port.”

A) Dados da publicação:	
Título:	Authentication in cloud-driven IoT-based big data environment: Survey and outlook
Autor(es):	Wazid, M. and Das, A.K. and Hussain, R. and Succi, G. and Rodrigues, J.J.P.C.
Fonte de Publicação:	Journal of Systems Architecture
Ano da Publicação:	2019
Resumo:	The Internet of Things (IoT) is composed of different networked objects (i.e., smart devices) which are interconnected to gather, process, refine, and exchange meaningful data over the Internet. These objects are assigned to their respective IP addresses, and they are able to send and receive data over a network without any human assistance. IoT offers different types of applications, such as, but not limited to, smart traffic monitoring, smart home, smart health care and smart cities, to name a few. In a Cyber-Physical System (CPS), computing elements coordinate and communicate with sensor devices, which monitor cyber and physical indicators, and actuators, and also modify the cyber and physical environment where they run. The synergy of computational as well as physical components, specifically the use of CPSs, led to the advancement of IoT implementations. In a cloud-driven IoT-based big data environment, a cloud-based platform is used to

	store the data generated by IoT devices (normally by sensor devices) which further can be considered as a big data warehouse. This environment is highly scalable and provides important real-time event processing (for example, in critical scenarios like surveillance and monitoring of an industrial plant). In IoT-based critical applications, the real-time data access is obligatory as and when it is required. Such access is possible if we permit only authorized external users to access the real-time data directly from the IoT sensors. Sometimes authorized user may also request for big data query processing and big data analytics over the data stored in cloud servers to figure out hidden patterns of some phenomena (i.e., chances of fire in an industrial plant in future). Therefore, we need secure authentication schemes for cloud-driven IoT-based big data environment in which a legitimate user and an IoT sensor can mutually authenticate each other and establish a common session key for secure communication. In this context, this paper first discusses the network and threat models of the authentication schemes for cloud-driven IoT-based big data environment. Some security requirements, issues and challenges of this environment are then discussed. A taxonomy of various existing authentication schemes applicable for cloud-driven IoT-based big data environment is also discussed, which covers a comparative study of these schemes. We identify and briefly discuss some future research challenges in designing the authentication schemes and other security protocols for cloud-driven IoT-based big data environment that need to be addressed in the future.
B) Dados derivados do objetivo:	
Vulnerabilidades	“we need secure authentication schemes for cloud-driven IoT-based big data environment in which a legitimate user and an IoT sensor can mutually authenticate each other, and then can establish a common session key for their secure communication” “Furthermore, “A” can physical capture some IoT sensors or smart sensing devices to obtain the stored credentials in those devices with the help of sophisticated power analysis attacks.” “The smart devices, such as IoT sensors, in the cloud-driven IoT-based big data environment may be failed due to energy issue or can be physically stolen by the adversary.”

	“Some identified issues and challenges include limited computation power and memory storage, energy requirement, scalability, mobility, support for heterogeneous devices, dynamic security updates, protection against physical capturing, and security and privacy of IoT sensors data at the big data warehouse.” “This phase is required when some sensing nodes are physically captured by an adversary or some sensing nodes are exhausted because of a power failure”

A) Dados da publicação:	
Título:	Vpnfilter malware analysis on cyber threat in smart home network
Autor(es):	Sicato, J.C.S. and Sharma, P.K. and Loia, V. and Park, J.H.
Fonte de Publicação:	Applied Sciences (Switzerland)
Ano da Publicação:	2019
Resumo:	Recently, the development of smart home technologies has played a crucial role in enhancing several real-life smart applications. They help improve the quality of life through systems designed to enhance convenience, comfort, entertainment, health of the householders, and security. Note, however, that malware attacks on smart home devices are increasing in frequency and volume. As people seek to improve and optimize comfort in their home and minimize their daily home responsibilities at the same time, this makes them attractive targets for a malware attack. Thus, attacks on smart home-based devices have emerged. The goals of this paper are to analyze the different aspects of cyber-physical threats on the smart home from a security perspective, discuss the types of attacks including advanced cyber-attacks and cyber-physical system attacks, and evaluate the impact on a smart home system in daily life. We have come up with a taxonomy focusing on cyber threat attacks that can also have potential impact on a smart home system and identify some key issues about VPNFilter malware that constitutes large-scale Internet of Things (IoT)-based botnet malware infection. We also discuss the defense mechanism against this threat and mention the most infected routers. The specific objective of this paper is to provide efficient task management and knowledge related to VPNFilter malware attack.
B) Dados derivados do objetivo:	

Vulnerabilidades	“This type of attack depends on the injection of data in web applications wherein it facilitates the interpretation and execution of malicious data in an unexpected way by exploiting program errors” “A buffer whose memory is allocated by a program is an example of temporary storage to deal with a surplus of data” “Authentication attack plays an important role in the protection of IoT security and privacy. The process of confirming the identity or truth of an object is known as authentication. This kind of attack is a way of exploiting and discovering security holes in web applications.” “Denial of service attack: in this type of attack, a hacker denies a service to authorize the user or even creates delays through resources, generating a large amount of data.” “Sybil attack: in this kind of attack, a single attacker can actually take over the networking, and multiple identities in the network are presented to the victim’s node, which allows the victim’s node to perform multiple operations, thus defeating the purpose of redundancy.” “Sleep deprivation attack: The perception layer is limited by the battery power in the node. To prolong the life of the battery, it is necessary for the device to sleep when not in operation. This type of attack attempts to subvert this process by constantly controlling and sending information to the network devices.” “Radio frequency jamming attack: This attack targets one of the key technologies of this layer, which consists of sensor nodes, cameras, actuators, tags / RFID readers, cell phones, tablets, GPS, and others to communicate in the smart home.” “Tampering attack: This type of attack is launched when the attacker is much closer to the network device and is forced to break hardware without any permission.” “Router platforms belonging to Linksys, TP-Link, Qnap, Netgear, and MikroTik implement home

	networks on internet gateways, making them more susceptible to the VPNFilter malware attack." "Several technical vulnerabilities are found to have been caused by human weaknesses."

A) Dados da publicação:	
Título:	Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures
Autor(es):	Panchal, A.C. and Khadse, V.M. and Mahalle, P.N.
Fonte de Publicação:	IEEE Global Conference on Wireless Computing and Networking, GCWCN
Ano da Publicação:	2019
Resumo:	Industrial Internet of Things (IIoT) applications connect machines, sensors and actuators in high-stake manufacturing industries. Industrial systems are using the potential of IoT to reduce the unnecessary operational cost and increase the usability and reliability of the industrial assets to achieve more profits. However, such smart Industries need connectivity and interoperability to enhance performance which makes them susceptible to various attacks. Recent attacks on Cyber-physical systems raise a strong security concern as such attacks causes a huge property loss and may also lead to life threatening situations. In this paper we discuss the potential security threats to the Industries adapting to IIoT and study the various attacks that are possible on the components in the layered IIoT architecture and some of the preventive measures. Finally, we propose IIoT attack taxonomy which would help in mitigating the risks of the attacks.
B) Dados derivados do objetivo:	
Vulnerabilidades	"DoS is an attack performed on a network to restrict a server from serving its client, DoS attacks target network bandwidth or services." "Firewalls can be used to allow or deny access to the requests, DoS attack detection using IDS and better authentication and authorization system can help to avoid such attacks." "To perform a side channel attacks on cloud a malicious virtual machine is placed in cloud to target the system implementation of cryptographic algorithms."

	“Today most of the services in cloud still use simple username and password type of single factor knowledge-based authentication.” “Phishing attacks happen when the attackers trick user to interact with the original looking fake webpages or emails, and gain access to one’s confidential data. Educating people about such attack is the best way to defense against phishing.” “SQL Injection: SQLi refers to an injection attack wherein attacker injects malicious input to get confidential data stored in database, delete database and bypass authentication.” “Remote Code Execution occurs when an attacker exploits vulnerability in the system to introduce a malware that can control the target system remotely.” “IP Spoofing: An attacker purposefully impersonates as another device by modifying the packet header with a forged IP address.” “The best way to defend against sniffing attacks is to encrypt all the data passing over the communication channel.”

A) Dados da publicação:	
Título:	A taxonomy of cyber-physical threats and impact in the smart home
Autor(es):	Heartfield, R. and Loukas, G. and Budimir, S. and Bezemskij, A. and Fontaine, J.R.J. and Filippoupolitis, A. and Roesch, E.
Fonte de Publicação:	Computers and Security
Ano da Publicação:	2018
Resumo:	In the past, home automation was a small market for technology enthusiasts. Interconnectivity between devices was down to the owner's technical skills and creativity, while security was non-existent or primitive, because cyber threats were also largely non-existent or primitive. This is not the case any more. The adoption of Internet of Things technologies, cloud computing, artificial intelligence and an increasingly wide range of sensing and actuation capabilities has led to smart homes that are more practical, but also genuinely attractive targets for cyber attacks. Here, we classify applicable cyber threats according to a novel taxonomy, focusing not only on the attack vectors that can be used, but also the potential impact on the

	systems and ultimately on the occupants and their domestic life. Utilising the taxonomy, we classify twenty five different smart home attacks, providing further examples of legitimate, yet vulnerable smart home configurations which can lead to second-order attack vectors. We then review existing smart home defence mechanisms and discuss open research problems.
B) Dados derivados do objetivo:	
Vulnerabilidades	“a breach of confidentiality, integrity and availability resulting from a vulnerability in a single device may result in shared exploitation across interdependent systems” “As the vast majority of smart home platforms rely on the home Internet gateway to reach respective cloud services in order to function, if an attacker can compromise a smart home Internet gateway they may be able to disrupt or gain control of almost every Internet-connected device in the household.” “this does not protect against attacks that have penetrated the network and may originate from the Internet or from inside the network, such as malware infections and social engineering.” “as HAPCAN utilises the CAN protocol, the protocol itself is at risk to several additional CAN vulnerabilities, such as request overload and false request to send” “UPB has no encryption and therefore any attack that is able to sniff data from the powerline (such as using a rogue UPB node) is able to read and inject data in the network.” “the signals containing sensor data or actuation commands can be captured by an adversary in the vicinity, which makes strong encryption and countermeasures against replay attacks particularly important. At the same time, wireless control can be rather trivially disrupted via communication jamming.” “WiFi de-authentication is by no means new, but in the context of the smart home, the loss of WiFi means loss of Internet connectivity in the household, on which IoT platforms are increasingly dependent in order to function.”

	“then identifying the product vendor allows attackers to analyse the smart home and target known vulnerabilities in its devices.” “Within the context of the smart home, it is the occupants who make the ultimate decision to install a new wireless security lock, presence sensor or voice-controlled assistant, as privacy and security concerns are carried out according to occupants’ risk attitude, personal and social circumstances” “The threat landscape relates to the communication medium and control software used, as well as threats in the supply chain, side channel attacks and the sensory channel.” “NFC is vulnerable to remote eavesdropping attacks assuming that an attacker has a powerful enough receiver to capture a NFC signal” “As workflow automation platforms can gain significant access in defining, controlling and triggering system behaviour and interaction in the smart home, this makes them a prime target for semantic social engineering attacks.” “Here, an example would be the electromagnetic emanations leaking from unfiltered powerlines.” “Increasingly, smart home devices come equipped with Internet access which are left poorly secured and as a result expose vulnerabilities over physical privacy.” “Unauthorised access to this information would likely lead to unauthorised physical actuation as a second-order physical effect (P-UA).” “Within the smart home, non-repudiation is associated to an occupant’s ability to provide evidence that distinguishes legitimate computer activity generated by themselves or fellow occupants and activity which has been executed by a malicious actor.” “In the smart home, this information may now be picked up more easily by exploiting poorly protected IoT devices with built-in microphone systems, such as personal assistant services “