TECHNICAL REPORT

A Structured Review on Security Vulnerabilities in IoT Environments

January, 2025

1. Introduction

Security is one of the main factors impacting both traditional systems and complex system environments, as it is closely tied to the level of attention and care with which data must be handled.

In IoT environments, security demands increased attention to both software systems and devices due to the nature of data being collected and shared by various devices, capturing a wide range of information that requires a certain level of privacy. However, we are aware of the fragility and dangers lurking within the network, creating many threats and highlighting vulnerabilities within these systems.

Nevertheless, understanding the vulnerabilities that exist in these scenarios ensures that threats can be anticipated and mitigation strategies can be developed to minimize the risks of invasion or data theft. For this reason, in an attempt to address this critical gap in IoT environments and in response to concerns about the vulnerabilities present in IoT system layers, our primary objective is to identify and categorize known vulnerabilities in IoT environments. This approach provides a knowledge base of vulnerabilities highlighted by studies in the field.

To achieve this, this Structured Review was planned and executed to identify, through detailed analysis, the existing security vulnerabilities in IoT environments. We emphasize the use of the Snowballing technique (Forward and Backward) to ensure greater precision in the results achieved.

2. Definitions

The definitions of basic security vulnerability concepts are derived from ISO/IEC 27000 (Information technology — Security techniques — Information security management systems — Overview and vocabulary), where vulnerability is defined as:

- *"Weakness of an asset or control, that can be exploited by one or more threats."*

3. Research Questions

3.1. Objective

The objective of this study is to identify security vulnerabilities in IoT software systems and devices.

3.2. Questions

3.2.1. Problem

Currently, there seems to be no unified solution that provides the necessary security requirements for developing IoT software systems. Therefore, understanding the main vulnerability points in such systems can help mitigate a significant portion of the common risks associated with these software systems.

3.2.2. Main Research Question

What vulnerabilities affect and can be identified in IoT software systems?

4. Search Strategy

The data extracted and analyzed in this study will be identified through the SCOPUS digital library, as it integrates a vast collection of other libraries in its database. Snowballing will be used to complement the search process.

4.1. Language and Search Expression

English was chosen as the language for search and selection of the studies.The search was refined using specific keywords to find relevant publications. The search expression was defined following the PICOC principle (Petticrew & Roberts, 2006), where synonyms are separated by the logical operator "OR," and the terms that make up the search string are separated by "AND." This approach uses the parameters "Population," "Intervention," "Comparison," "Outcome," and "Context."

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	*No Avaliable*
Outcome	*"taxonomy" OR "categories" OR "classification" OR "Catalog"; AND*
Context	*"internet of things" OR "Internet of Everything" OR "IoT"*

For Scopus, the search string used was:

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")) AND PUBYEAR > 2010 AND PUBYEAR < 2025 AND (LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar")

4.2. Snowballing

Snowballing was applied with the selected sources for data extraction from the automated search strategies. We employed both Forward and Backward Snowballing techniques using Scopus as a tool to identify citations and other references from works that contribute to the objective of this study.

5. Study Selection Process

The following selection procedures were implemented during the execution of the Scopus search string:

a. Application of selection criteria based on the title, abstract, and keywords of the articles;

b. Application of selection criteria based on the full reading of the articles selected in the previous step;

After finalizing the selection through the search engine, we used the set of included articles to perform backward (one level) and forward snowballing, following this flow:

a. Application of selection criteria based on the titles of the articles;

b. Application of selection criteria based on the abstracts of the articles;

c. Application of selection criteria based on the full reading of the accepted articles.

6. Selection Criteria

6.1. Inclusion Criteria

- Present scenarios focused on security in IoT software systems;
- Identify vulnerabilities within these scenarios;
- The work must be written in English;

6.2. Exclusion Criteria

- Not available or fully accessible;

- Duplicate studies.

7. Extraction Process

For each candidate source, the extraction procedure is performed using the model presented in Section 7.1.

7.1. Extraction Model

A) Publication Data:	
Title:	Indicates the title of the work
Author(s):	Names of the authors
Source of Publication:	Place of publication
Year of Publication:	Year of publication
Abstract:	Text containing a description of the abstract
B) Data Derived from the Objective:	
Vulnerabilities	What vulnerabilities in IoT software systems are highlighted in the study?

8. Execution Report

- Scopus Execution Date: August 2022 (updated 01/20/25)

Initially, 638 document results were identified. After eliminating proceedings and books, 491 remained. With the update of the search string, 321 more studies were included, resulting in a total of 812 identified articles.

- Included for Data Extraction:

After analyzing the title, abstract and keywords, the number of selected documents was reduced to 85. We then applied the full-text reading filter, reducing it to 44 final documents, used for the extraction and analysis of information relevant to the study.

- Included through Snowballing
    - Backward Snowballing: A total of 90 articles were identified and included;
    - Forward Snowballing: A total of 45 articles were identified and included;

Final Set of Selected Articles in the Review:

- By the search engine (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.

[A40]. Zhukabayeva, T., Zholshiyeva, L. and Karabayev, N. (2024). Future Directions of Cybersecurity in Industrial Internet of Things Through Edge Computing. 9th International Conference on Computer Science and Engineering (UBMK), Antalya, Turkiye, pp. 1-6, doi: 10.1109/UBMK63289.2024.10773586.

[A41]. Alguliyev, R., Aliguliyev, R. and Sukhostat, L. (2024). Radon Transform Based Malware Classification in Cyber-Physical System Using Deep Learning. Results in Control and Optimization, volume 14, 100382, ISSN 2666-7207, https://doi.org/10.1016/j.rico.2024.100382.

[A42]. Bharathi V., Vinoth Kumar C. (2024). Vulnerability Detection in Cyber-Physical System Using Machine Learning. Scalable Computing: Practice and

Experience, ISSN 1895-1767, Volume 25, Issues 1, pp. 577–591, DOI 10.12694/scpe.v25i1.2405.

[A43]. Peggs, C., Jackson, T., Tittlebaugh, A., Olp, T., Tyler, J., Reising, D., Loveless, T. (2023). Preamble-based RF-DNA Fingerprinting Under Varying Temperatures. 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, pp. 1-8, doi: 10.1109/MECO58584.2023.10155035.

[A44]. Ajao, L. and Apeh, S. (2023). Blockchain Integration with Machine Learning for Securing Fog Computing Vulnerability in Smart City Sustainability. 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, pp. 1-6, doi: 10.1109/ICAISC56366.2023.10085192.

8.1 Data Extraction

Following the extraction model described in the previous section, the desired data was identified and extracted from the selected articles. The data extraction can be reviewed in the appendix of this report.

This section presents the listing of vulnerabilities identified during the review. A total of 69 vulnerabilities were identified, excluding the results from snowballing, as highlighted in Table 1. The vulnerabilities were initially organized into four categories: Device, Application, Network, and Peopleware.

Table 1 - List of Vulnerabilities

Articles	Vulnerabilities	Category
13, 5, 23, 4, 17	Broken Authentication	Application
9, 31, 38, 1, 25, 17, 6	Buffer Overflow	Application
8	Data Inconsistency	Application
8, 13, 11, 21, 9, 37, 27, 18, 4, 24	Insecure Access Management	Application
11, 31	Insecure Interface Configuration	Application
11, 5, 37, 33, 26	Insecure Management of Data	Application
5, 23, 31, 33, 15, 24	Insecure Software	Application
5	Lack of Active Device Monitoring	Application
5	Lack of Standardization	Application
9	Low Quality Level Code	Application
19, 21, 2, 24	Non-repudiation	Application
32, 18, 33, 17, 6, 24	SQL Injections	Application
11, 27	Weak/lack In-app Encryption	Application
38, 26, 24	Malicious code in-app	Application
24	Systems Low-cost	Device
8, 19	Channel Voice	Device

19, 10, 23, 35, 24	Default Configuration	Device
8, 5, 21, 39, 18, 25	Device Spoofing	Device
19, 10, 30, 20, 24	Electromagnetic Emanations Leaking	Device
16, 22, 30, 24, 26	Energy Restraints	Device
8, 11, 19, 10	Heterogeneous Interaction	Device
11, 19, 10, 5, 16, 9, 37, 39, 38, 30, 25, 26, 36	Insecure Data Transfer and Storage	Device
10, 5, 23, 35, 31, 1, 4, 24	Insecure Firmware	Device
31, 30, 24	Insecure Initialization	Device
5, 37, 3, 36	Insecure Password	Device
5, 24	Insufficient Testing	Device
8, 23, 16, 29, 30, 4, 12, 6, 20, 24	Lack of Side Channel Protection	Device
10, 5, 23, 28, 21, 35, 29, 9, 37, 30, 4, 33, 25	Lack of Strong Authentication	Device
11, 10, 28, 16, 9, 37, 30, 33, 25, 12, 6, 24	Low Computing Power	Device
35, 9	Low Data Transmission Range	Device
8, 34, 35, 29, 33, 24	Malicious Code Injection	Device
35, 39, 7, 12, 20, 24	Obtaining Console Access	Device
16, 39, 33, 12, 17, 24	Physical Damage	Device
8, 19, 5, 34, 23, 39, 7, 33, 25, 17, 20, 24, 36	Physical Tampering	Device
8, 31, 37, 33, 12, 17, 6, 24	Sleep Deprivation	Device
35, 38	Tag Cloning	Device
11, 23, 35, 16, 39, 38, 7, 4, 33, 12, 6, 24	Unprotected Physical Access	Device
5, 23, 28, 21, 35, 29, 37, 38, 30, 27, 18, 4, 25	Weak Access Control	Device
10, 5, 29, 31, 38, 30, 27, 25, 36	Weak/leak of Encrypt	Device
31	Insecure physical interface	Device
8, 19, 34, 35, 29, 31, 38, 7, 33, 6, 36	Channel Interference	Network
32	Communication Overhead	Network
8, 13, 34, 23, 22, ´14, 37, 7, 30, 1, 25, 26, 36	Data Leak or Breach	Network
11, 19, 5, 23, 22, 39, 38, 33, 17, 24	Eavesdropping	Network
8, 11, 10, 34, 38, 7, 4, 33, 12, 17, 6, 24	Fake/Malicious Node	Network
11, 19, 10, 35, 30, 25, 26	Heterogeneous Communication	Network
14, 30, 18	Insecure Server	Network

11	Insecure Update Mechanisms	Network
8, 11,5, 28, 21, 16, 37, 38, 30, 27, 18, 25, 6, 2, 36	Lack of Proper Authenticatication Mechanisms	Network
23, 18, 4	Lack of Strong Password	Network
19, 5, 22, 31, 25, 24	Lack Secure Communication Protocols	Network
10	Configure network repeatedly	Network
32, 8, 11	Spoofing Signal	Network
32, 8, 11, 19, 28, 21, 29, 14, 37, 39, 38, 7, 30, 27, 33, 25, 2, 24	Unauthorized Access	Network
5, 23, 18	Unsecured Network	Network
23, 7, 3, 18, 15	Unused Ports Enable	Network
19, 5, 29, 14, 31, 37, 39, 30, 27, 18, 1, 2, 26	Weak/lack Encryption in Communication	Network
22, 36	Physical properties of the power system	Network
19	Wifi De-authentication	Network
29	Insecure traffic control	Network
24, 32, 36	Centralized architecture	Network
8, 35, 17	Access Malicious Link	Peopleware
19	Identifying the Product Vendor	Peopleware
5, 15, 12	Knowledge the System	Peopleware
10	Lack of Technical Support	Peopleware
19, 10, 28, 39, 17	Personal and Social Circumstances	Peopleware
34, 23, 39, 38, 18, 33, 12, 6, 24, 36	Phishing	Peopleware
19, 5, 39, 7, 33, 6	Social Engineering	Peopleware
5	Untrusted Device Acquisition	Peopleware
5	Vendor Security Posture	Peopleware

Additionally, through the merging process of vulnerabilities identified in both the ad-hoc and structured reviews, it was observed that four vulnerabilities from the ad-hoc review were not present in the structured review. These are: Account Lockout, Insecure 3rd Party Components, Overly Large Attack Surface, and Username Enumeration. All of these vulnerabilities were classified under the Application category, highlighting specific gaps that the structured review alone failed to capture.

9. Conclusion

Given the significant expansion that IoT devices have undergone in recent years, their potential for engagement across various sectors is evident. This expansion necessitates special attention to how these devices handle and manage data, as the range of sensitive information involved in IoT technologies is indeed vast.

For this reason, security in IoT environments becomes a crucial component for the proper functioning of such technologies. Among the primary security vectors, vulnerabilities stand out as a field of study with a significant impact on mitigating damage associated with threats or attacks that may directly interfere with the performance of IoT technologies.

This report aims to present a set of vulnerabilities identified within the context of IoT, initially classified into four categories related to the main layers of IoT (Physical, Application, and Network), with the addition of Peopleware, which addresses vulnerabilities directly associated with human agents. A total of 69 vulnerabilities were cataloged from the studies identified through the search engine alone. The Snowballing process data helped support and reinforce the findings of the review, as no new points of vulnerabilities were identified during the extraction phase. It is worth noting that the study resulted in a total of 73 cataloged vulnerabilities, including those identified through both the structured review and the ad-hoc review.

We hope that this report will enable researchers working in the field of IoT system development to anticipate security risks associated with their projects based on this list of vulnerabilities and even estimate mitigation strategies to make their systems increasingly secure.

.

APPENDIX A – DATA EXTRACTION FROM THE STRUCTURED REVIEW

A) Publication Data:	
Title:	SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems Based on Machine Learning
Author(s):	Saha, T. and Aaraj, N. and Ajjarapu, N. and Jha, N.K.
Source of Publication:	IEEE Transactions on Emerging Topics in Computing
Year of Publication:	2022
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach
Author(s):	Abuemera, E.A. and Elzouka, H.A. and Saad, A.A.
Source of Publication:	2nd International Conference on Consumer Electronics and Computer Engineering, ICCECE
Year of Publication:	2022
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	Security in IoT-based smart homes: A taxonomy study of detection methods of mirai malware and countermeasures
Author(s):	Auliar, R.B. and Bekaroo, G.
Source of Publication:	International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME
Year of Publication:	2021
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	SoK: Investigation of security and functional safety in industrial IoT
Author(s):	Tomur, E. and Gulen, U. and Soykan, E.U. and Akif Ersoy, M. and Karakoc, F. and Karacay, L. and Comak, P.
Source of Publication:	IEEE International Conference on Cyber Security and Resilience, CSR
Year of Publication:	2021
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	A Review of Security Standards and Frameworks for IoT-Based Smart Environments
Author(s):	Karie, N.M. and Sahri, N.M. and Yang, W. and Valli, C. and Kebande, V.R.
Source of Publication:	IEEE Access
Year of Publication:	2021
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study
Author(s):	Davis, B.D. and Mason, J.C. and Anwar, M.
Source of Publication:	IEEE Internet of Things Journal
Year of Publication:	2020
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	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) Publication Data:	
Title:	Securing Cyberspace of Future Smart Cities with 5G Technologies
Author(s):	Akhunzada, A. and Islam, S.U. and Zeadally, S.
Source of Publication:	IEEE Network
Year of Publication:	2020
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT
Author(s):	Sengupta, J. and Ruj, S. and Das Bit, S.
Source of Publication:	Journal of Network and Computer Applications
Year of Publication:	2020
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	DDoS in IoT: A roadmap towards security countermeasures
Author(s):	Roohi, A. and Adeel, M. and Shah, M.A.
Source of Publication:	25th IEEE International Conference on Automation and Computing
Year of Publication:	2019
Abstract:	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) Data Derived from the Objective:	

Vulnerabilities	“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) Publication Data:	
Title:	A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors
Author(s):	Akbar, M.A. and Alsanad, A. and Mahmood, S. and Alothaim, A.
Source of Publication:	IEEE Access
Year of Publication:	2021
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges
Author(s):	Mahapatra, S.N. and Singh, B.K. and Kumar, V.
Source of Publication:	Arabian Journal for Science and Engineering
Year of Publication:	2020

Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	Towards an Extensible IoT Security Taxonomy
Author(s):	Wüstrich, L. and Pahl, M.-O. and Liebald, S.
Source of Publication:	IEEE Symposium on Computers and Communications , Vol. 2020-July
Year of Publication:	2020
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	A survey of IoT security based on a layered architecture of sensing and data analysis
Author(s):	Mrabet, H. and Belguith, S. and Alhomoud, A. and Jemai, A.
Source of Publication:	Sensors (Switzerland)
Year of Publication:	2020
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	Data Security and Privacy Protection for Cloud Storage: A Survey
Author(s):	Yang, P. and Xiong, N. and Ren, J.
Source of Publication:	IEEE Access
Year of Publication:	2020
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	Toward an applied cyber security solution in iot-based smart grids: An intrusion detection system approach
Author(s):	Yin, X.C. and Liu, Z.G. and Nkenyereye, L. and Ndibanje, B.
Source of Publication:	Sensors (Switzerland)
Year of Publication:	2019
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	"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) Publication Data:	
Title:	Authentication in cloud-driven IoT-based big data environment: Survey and outlook
Author(s):	Wazid, M. and Das, A.K. and Hussain, R. and Succi, G. and Rodrigues, J.J.P.C.
Source of Publication:	Journal of Systems Architecture
Year of Publication:	2019
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	Vpnfilter malware analysis on cyber threat in smart home network
Author(s):	Sicato, J.C.S. and Sharma, P.K. and Loia, V. and Park, J.H.
Source of Publication:	Applied Sciences (Switzerland)
Year of Publication:	2019
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures
Author(s):	Panchal, A.C. and Khadse, V.M. and Mahalle, P.N.
Source of Publication:	IEEE Global Conference on Wireless Computing and Networking, GCWCN
Year of Publication:	2019
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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) Publication Data:	
Title:	A taxonomy of cyber-physical threats and impact in the smart home
Author(s):	Heartfield, R. and Loukas, G. and Budimir, S. and Bezemskij, A. and Fontaine, J.R.J. and Filippoupolitis, A. and Roesch, E.
Source of Publication:	Computers and Security
Year of Publication:	2018
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	“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 “

A) Publication Data:	
Title:	A taxonomy of cyber-physical threats and impact in the smart home
Author(s):	Heartfield, R. and Loukas, G. and Budimir, S. and Bezemskij, A. and Fontaine, J.R.J. and Filippoupolitis, A. and Roesch, E.
Source of Publication:	Computers and Security
Year of Publication:	2018
Abstract:	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) Data Derived from the Objective:	
Vulnerabilities	A consequence of technology convergence in the smart home is the cascading effect of compromise of one system to others. For example, a breach of confidentiality, integrity and availability resulting from a vulnerability in a single device may result in shared exploitation across interdependent systems. A secure system may be rendered vulnerable by the insecurities of a lesser protected platform on which it relies.[...] 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.[...] As of May 2018, an initial report by Cisco Talos dramatically reinforced the growing vulnerability of home internet gateways by identifying a large scale advanced persistent threat against SOHO routers titled VPNFilter.[...] [...], 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. [...], 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. Whilst the vulnerability in question was addressed in 2009 by introduction of the 802.11w RFC, which strengthened the authenticity and integrity of WiFi management packets, consumer-based router manufacturers do not often implement this extension into their WiFi protocol stack. So, even though 802.11w is available in most recent Linux kernels and Windows OS (since Windows 8), often this feature must be disabled in order for it to be compatible with household WiFi routers. [...] 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 (Rahmati et al., 2018), personal and social circumstances[...] For the immediate future, the smart home technology landscape is likely to be volatile, consisting of both legacy and emerging IoT platforms, each with their own security risks. 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. However, due to a lack of definable NFC wireless communication standards and a proliferation of NFC-enabled systems, a number of vulnerabilities have been found across a range of NFC implementations. For example, NFC is vulnerable to remote eavesdropping attacks assuming that an attacker has a powerful enough receiver to capture a NFC signal (Kennedy and Hunt, 2008) (by design, NFC requires extremely close proximity between the transponder and receiver, e.g., up to 10 cm).[...] 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 (Heartfield and Loukas, 2016). Whilst an attacker may not necessarily target a specific vulnerability in workflow automation platforms themselves, a successfully crafted phishing email that deceives a user into divulging their account's username and password potentially provides an attacker with the ability to edit, delete and create new workflow automation rules in the target household.[...] Here, an example would be the electromagnetic emanations leaking from unfiltered powerlines. Enev et al. (2011) have demonstrated the viability of measuring a home's powerline activity with such accuracy that they could identify what the occupants were watching on television. Their method was reproducible and accurate enough across a wide range of modern television sets. Increasingly, smart home devices come equipped with Internet access which are left poorly secured and as a result expose vulnerabilities over physical privacy. For example, Internet device scanning search engines (such as Shodan), allow attackers to identify open ports of nodes, indexing the header or banner information of responsive nodes; which

	can include information such device type, model, vendor, firmware version other open protocols.[...] [...] 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 past, threats to this communication medium were low as only very targeted attacks (such as physical bugging) posed a risk. 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 (e.g., Google Home, Amazon Echo), children toys and other voice-controlled house-hold appliances.

A) Publication Data:	
Title:	Introduction to em information security for IoT devices
Author(s):	Hayashi, Y. and Verbauwhede, I. and Radasky, W.A.
Source of Publication:	IEEE International Symposium on Electromagnetic Compatibility
Year of Publication:	2018
Abstract:	With the advent of the Internet of Things (IoT), many electronic devices (e.g., smart meters, surveillance cameras, mobile devices, and multiple sensors) are interconnected. Each device gathers data and uploads it to servers via communication networks. Servers store the large volumes of received data in databases. Applications analyze this data and extract valuable information. Finally, based on this information, new services (in domains such as smart cities, public safety, e-commerce, medical, healthcare, or automobile) are provided. In this data flow, systems and applications in the upper layer trust the hardware in the lower layer, which includes data-gathering devices. If the collected information is intentionally modified by adversaries, services in the upper layer could be disrupted. Therefore, to ensure service continuity in the IoT, it is important to secure the hardware layer in which data are harvested and transmitted. In this paper, we focus on hardware-level security in IoT systems and classify the schemes proposed for physical security of IoT into three categories. We also provide examples for each of these and explain threats and countermeasures.
B) Data Derived from the Objective:	
Vulnerabilities	The vulnerability due to electromagnetic waves can be largely classified into three categories: (1) electromagnetic emanation resulting from information processing within devices, (2) intentional electromagnetic interference to devices, and (3) intentional modification of system circuit configuration

A) Publication Data:	
Title:	A taxonomy of security and privacy requirements for the Internet of Things (IoT)
Author(s):	Alqassem, I. and Svetinovic, D.
Source of Publication:	International Conference on Industrial Engineering and Engineering Management

Year of Publication:	2014
Abstract:	Capturing security and privacy requirements in the early stages of system development is essential for creating sufficient public confidence in order to facilitate the adaption of novel systems such as the Internet of Things (IoT). However, security and privacy requirements are often not handled properly due to their wide variety of facets and aspects which make them difficult to formulate. In this study, security-related requirements of IoT heterogeneous systems are decomposed into a taxonomy of quality attributes, and existing security mechanisms and policies are proposed to alleviate the identified forms of security attacks and to reduce the vulnerabilities in the future development of the IoT systems. Finally, the taxonomy is applied on an IoT smart grid scenario.
B) Data Derived from the Objective:	
Vulnerabilities	Access control mechanisms limit access to various system's resources (e.g., data, services, hardware, etc.) by identifying who can access what resources, and constrain what a legitimate user can do by controlling who is doing what in the system. - 1) Identification The focus of the identification is to uniquely identify objects and manage their identities while considering security and high scalability aspects of the IoT. Reaching a consensus on how to identify objects involved in the IoT and managing their identities is fundamental for constructing robust authentication and authorization mechanisms. - 2) Authentication While authorization defines the rights and privileges after an entity gains access to a system, authentication, i.e., identity verification, plays a vital role before establishing a communication channel between two entities. In the IoT, authentication protocol should be developed to confirm mutual trust between different objects, users or systems by verifying their identities - 3) Authorization Authorization is the process of granting, denying or limiting access to data, resources or applications within a system. One possible approach for object and user authorization in the IoT is Role-Based Access Control (RBAC). RBAC is an access management technique for multi user and multi-application online systems. In RBAC each role has different functions, an entity can have one or more roles and management of permission is carried out based on entity's role(s) Dealing with transaction disputes to assure fair exchange is a common security concern in the business field which will be engaged in the IoT. Thus, it is necessary to build in non-repudiation into the design of the appropriate transport protocol that deals with network failures and prevents a dishonest entity from cheating, deceiving about its real identity or aborting a transaction (i.e., roll-back attack)

A) Publication Data:	
Title:	Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts
Author(s):	Reda, H.T. and Anwar, A. and Mahmood, A.

Source of Publication:	Renewable and Sustainable Energy Reviews
Year of Publication:	2022
Abstract:	Smart Grid is organically growing over the centrally controlled power system and becoming a massively interconnected cyber–physical system with advanced technologies of fast communication and intelligence (such as Internet of Things, smart meters, and intelligent electronic devices). While the convergence of a significant number of cyber–physical elements has enabled the Smart Grid to be far more efficient and competitive in addressing the growing global energy challenges, it has also introduced a large number of vulnerabilities in the cyber–physical space culminating in violations of data availability, integrity, and confidentiality. Recently, false data injection (FDI) has become one of the most critical types of cyberattacks, and appears to be a focal point of interest for both research and industry. To this end, this paper presents a comprehensive review in the recent advances of the FDI attacks, with particular emphasis on adversarial models, attack targets, and impacts on the Smart Grid infrastructure. This review paper aims to provide a thorough understanding of the incumbent threats affecting the entire spectrum of the Smart Grid. Related literature are analyzed and compared in terms of their theoretical and practical implications to the Smart Grid cybersecurity. In conclusion, a vast range of technical limitations of existing false data attack research is identified, and a number of future research directions is recommended.
B) Data Derived from the Objective:	
Vulnerabilities	[...] Moreover, as attacks from cyber criminals on the power grid continue to rise in complexity and frequency, it is inevitable that various parts of the Smart Grid are vulnerable to the incumbent attacks. Therefore, it is required to provide strong attack defence across the EMS and to deploy secure communication protocols. [...]For example, in wireless sensor networks (WSNs), the inherent wireless communication and broadcast channels between the nodes increase the vulnerability of adversaries that may eavesdrop on all traffic, inject false data reports containing erroneous sensor readings, or can even deplete the already limited energy capacity of sensor nodes[...] [...]The vulnerability issues in the SE problem can be investigated with respect to the various cyber-and physical elements, including Physical properties of the power system, communication systems, IEDs, and AMIs. Related attack targets also include transmission lines [101], [112], topology [69], [99], [132], and system observability [106].

A) Publication Data:	
Title:	A survey on Classification of Cyber-attacks on IoT and IIoT devices
Author(s):	Shah, Y. and Sengupta, S.
Source of Publication:	Annual Ubiquitous Computing, Electronics and Mobile Communication Conference
Year of Publication:	2020
Abstract:	Internet of Things (IoT) devices have gained popularity in recent years. With the increased usage of IoT devices, users have become more prone to Cyber-attacks. Threats against IoT devices must be analyzed thoroughly to develop protection mechanisms against them. An attacker's purpose behind launching an attack is to find a weak link within a network and once discovered, the devices connected to the network become the primary target for the attackers. Industrial Internet of Things (IIoT) emerged due to the popularity of IoT devices and they

	are used to interconnect machines, sensors, and actuators at large manufacturing plants. By incorporating IIoT at their facilities companies have benefited by reducing operational costs and increasing productivity. However, as IIoT relies on utilizing the Internet to operate it is vulnerable to Cyber-attacks if security is not taken into consideration. After seeing the advantages of IIoT, a new version of smart industries has been introduced called Industry 4.0. Industry 4.0 combines cloud and fog computing, cyber-physical systems (CPS), and data analytics to automate the manufacturing process. This paper surveys the different classifications of attacks that an attacker can launch against these devices and mentions methods of mitigating such attacks1
B) Data Derived from the Objective:	
Vulnerabilities	[...]However, if the data is encrypted and the attackers obtain the key that's used to encrypt the data, the information can be modified.[...] Once the malicious firmware has been transferred to the intended device the only other piece of information that the attacker needs is the architecture of the device's processor which can be easily located by looking at the device's manual. The attacker uses the flaws which exist in the verification of firmware updates to their advantage and the malicious code runs once the firmware updates are installed. Software failure: Smart home systems depend on software to be controlled and operated upon. Any existence of vulnerabilities in the implementation of the software makes those systems a primary target for attackers. [...]DoS and DDoS attacks target a vulnerability that is found in the Transmission Control Protocol (TCP) [11]. In order to connect to the Internet, devices use the TCP's three-way handshake methodology. These attacks exploit TCP's handshake by directing a high volume of requests to establish a TCP connection with the target server. Eavesdropping involves illegally listening to personal conversations in real-time by monitoring emails, phone calls, or video conferences [...]An attacker can listen in on the conversations when the data is being transferred through unsecured servers, when unwanted ports are left open, or when the device is connected to unsecured public Wi-Fi networks. Passwords are often considered as important keys which are used to unlock personal information. Password attacks are carried out using various methods such as password guessing, password resetting, and password capturing. Password guessing, as the name suggests, involves the attacker inputting commonly used password combinations until they find a match. Password re-usage is also another major problem as once the attacker knows the password they can use it to access multiple accounts[...] Side Channel Attacks: Performing side channel attacks on M2M machines requires physical access to these machines. Attackers can use the peripheral information of the physical devices to extract confidential information from them. These types of attacks can also help attackers retrieve cryptography algorithms keys from the devices [...]

	An attacker requires physical access to an M2M device and takes full control of it. This form of attack is achieved by physically damaging or replacing a node in the device.[...] When accessing cloud services a user must enter authentic credentials. However, the authentication process and mechanisms are highly vulnerable and often targeted. Many cloud services still utilize single-factor authentication and a simple username and password requirements. Attackers use this vulnerability to their advantage when trying to disrupt services or steal information from an enterprise taking advantage of cloud computing. Phishing is used to trick people into entering their personal information or downloading malicious software that is capable of spreading malware. The most common form of phishing attacks are emails that contain links to fake websites, and/or malicious attachments [...] Implementing poor password requirements is the primary reason IoT/IIoT networks are targeted. Outdated software may contain flaws that allow attackers to gain access to personal information. Companies often release software updates when the current version contains security vulnerabilities or bugs that can be exploited by attackers. Always ensure to download updates from trusted sources and if possible enroll the device to automatically install updates from the manufacturer's website. When setting up the environment for IoT/IIoT devices ensure that they are kept separate from the rest of the devices to limit the possibility of an external device causing problems. Keeping these devices in a separate private network also eliminates the possibility of an attacker infecting other devices and spreading the malware in the network. Another benefit of this implementation is that only authorized users are going to have the ability to access and modify data. Changing default settings: Many times the default settings that are assigned by the device manufacturers benefit the company rather than its users. Manufacturers often add or enable features that are not essential in the operation of the device that aids attackers in launching their attacks. These settings should be checked and changed immediately after the device is purchased and setup.

A) Publication Data:	
Title:	On Threat Analysis of IoT-Based Systems: A Survey
Author(s):	Zhao, W. and Yang, S. and Luo, X.
Source of Publication:	IEEE International Conference on Smart Internet of Things, SmartIoT
Year of Publication:	2020
Abstract:	In this paper, we provide a survey on threat analysis of systems based on Internet of Things (IoT), and how the blockchain technology can help mitigate the threats. Although the topic of IoT security (and previously the security of wireless sensor networks) has been reviewed extensively, we believe that the topic deserves a more in-depth examination towards a more systematic threat analysis, which is not only necessary to better understand the threats against IoT-based systems, but also paves the way to effectively improve the security of IoT-based systems by integrating

	with the blockchain technology. The major research contributions of this paper include a new taxonomy of the threats against IoT-based systems, identify what threats can be effectively mitigated by integrating IoT with with blockchain technology, the challenges faced by the blockchain-enabled IoT-based systems, and the likely approaches to overcoming these challenges.
B) Data Derived from the Objective:	
Vulnerabilities	At the sensing layer: Eavesdropping. Because the IoT devices are transmitting wirelessly, it is easier to intercept the transmitted signals even if the IoT devices are protected with physical security. Sleep deprivation. Many IoT devices use battery as the power sources, hence, they only sense and transmit periodically and go to a sleep state in between. The aim of this attack is to somehow prevent the devices from going to sleep or to minimize the sleep period, thereby drain the batter much faster than normal usage. Eventually, this attack will lead to the battery-drained IoT devices to be out of the service. Side channel attacks. This kind of attacks aim to gather sensitive information without actually intercepting the message transmitted. Instead, the information gathering is based on observing the electromagnetic fields from the IoT devices, or the power assumption of the IoT devices. Booting attacks. Because the firmware/operating systems used by low-cost IoT devices might not have been as robustly tested as desktop/server operating systems, the boot process might be exploited to compromise the device. Obviously, this would require the device to be physically captured first. Malicious code injection. An adversary aims to install a compromised version of the software/firmware during wireless updates of the IoT device, which could give the adversary full remote control over the compromised device. The network layer: Phishing site attack. It is no different from the regular phishing attack where a link is sent to a user pretending to be a legitimate site and if the user clicked the link, the user might be tricked to provide confidential information. We are puzzled as to why this is classified as a network layer attack. Access attack. It is also called advanced persistent threat, which refers to the gaining of unauthorized access to the IoT network with the aim of collecting sensitive information. Denial of service (DoS) or distributed denial of service attacks (DDoS). These types of attacks aim to overwhelm the target system with network traffic to essentially make it unable to provide services to legitimate clients. Like any other online systems, IoT devices are vulnerable to DoS/DDoS attacks as well. The middleware layer:

	Signature wrapping. This attack exploits a vulnerability exists in XML signatures, which effectively invalidate the properties offered by the digital signature, such as non-repudiation. Man-in-the-middle. This attack would be successful if the MQTT publish-subscribe protocol is used and the proxy for the protocol is compromised. At the application layer: Access control attack. This attack exploits the vulnerability in access control and an adversary may gain access to resources illegally, which could lead to the theft of confidential information or compromise the integrity of the entire system. Physical Layer: Insecure configuration. If the IoT software configuration and initiation are not done properly, the devices might be compromised remotely. Not only the data collected by the devices may be stolen, the devices themselves could be used to launch a DDoS attack, as the malware Mirai has demonstrated. Physical security. Low-cost IoT devices that must be deployed in unprotected field are inevitably facing physical threats. Network Layer: Resource depletion. This includes all attacks that aim to render the device unavailable due to exhaustion of available memory to perform its normal operations, such as the replay, duplicate, and fragmentation attacks that exploit the vulnerabilities of the 6LoWPAN protocol used by IoT devices. Routing protocols. This include all attacks on routing protocols used by IoT devices. One routing protocol is the RPL, which was designed to run on top of low power and lossy networks.

A) Publication Data:	
Title:	Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms
Author(s):	Kamaldeep and Dutta, M. and Granjal, J.
Source of Publication:	IEEE Access
Year of Publication:	2020
Abstract:	The Internet of Things (IoT) exemplifies a large network of sensing and actuating devices that have penetrated into the physical world enabling new applications like smart homes, intelligent transportation, smart healthcare and smart cities. Through IoT, these applications have consolidated in the modern world to generate, share, aggregate and analyze large amount of security-critical and privacy sensitive data. As this consolidation gets stronger, the need for security in IoT increases.

	With first line of defense strategies like cryptography being unsuited due to the resource constrained nature, second line of defense mechanisms are crucial to ensure security in IoT networks. This paper presents a comprehensive study of existing second line of defense mechanisms for standardized protocols in IoT networks. The paper analyzes existing mechanisms in three aspects: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Intrusion Response Systems (IRS). We begin by providing an overview of standardized protocol stack, its layers and defensive security systems in IoT. From there, we build our narrative by presenting an extended taxonomy of IDS, IPS and IRS classifying them on their techniques, deployment, attacks, datasets, evaluation metrics and data pre-processing methods. We then thoroughly review, compare and analyze the research proposals in this context, considering the unique characteristics involved in these systems. Based on the extensive analysis of the existing defensive security systems, the paper also identifies open research challenges and directions for effective design of such systems for IoT networks, which could guide future research in the area.
B) Data Derived from the Objective:	
Vulnerabilities	6LoWPAN mechanisms often suffer a bottleneck in processing and forwarding fragmented packets that further lead to problems of buffer overflow in constrained devices. UDP, being an unreliable, connectionless and lighter protocol, has been accepted as de facto standard in IoT. But, UDP has inherent weakness whereby attackers can launch DDoS attacks, one them being the UDP flooding attack. The most promising standard application layer protocol for small IoT devices is CoAP [14]. As an extremely heterogeneous technology, security is a critical aspect of IoT on multiple levels of securing data, communication and networks. Attacks on IoT have become extremely targeted and sophisticated. As already discussed, first line of defense mechanisms like cryptography are insufficient due to the resource constrained nature of IoT devices which limits their ability to host and implement sophisticated cryptographic algorithms in real time. Also, the ad hoc nature of IoT networks lets devices connect to each other at runtime, typically for shorter durations, consequently creating a collaborative network. Denial of Service (DoS) Attacks: The second most common and the easiest to launch is the DoS attack and when this attack is launched by multiple compromised systems on a single victim, it is termed as Distributed Denial of Service (DDoS) attacks. Also present in the IoT, DoS tries to put a node or a network out of operation by flooding it with (possibly incorrect) requests, preventing the node to accept and process legitimate requests.[...] Spoofing Attacks: Various other classes of attacks detected in the IoT include impersonation or spoofing attack, physical tampering of devices, man-in-the-middle, data integrity, authentication and adversarial attacks. Penetration Attacks: Penetration attacks exploit vulnerabilities in the system and involve any unauthorized access or modifications to system's resources and data. In such attacks, attackers gain control of the system by exploiting a number of software flaws.[...]

A) Publication Data:	
Title:	Security and Privacy of Smart Cities: Issues and Challenge
Author(s):	Sookhak, M. and Tang, H. and Yu, F.R.
Source of Publication:	International Conference on High Performance Computing and Communications
Year of Publication:	2019
Abstract:	Smart city has been emerged as a new paradigm to dynamically optimize the resources in cities and provide better facilities and quality of life for the citizens. Despite the potential vision of smart cities, security and privacy issues remain to be carefully addressed. In this paper, we present a comprehensive survey of security and privacy issues of smart cities, and categorize the present and future developments within this area. We also describe a thematic taxonomy of security and privacy issues of smart cities to highlight the requirements for designing a secure smart city, identify the existing security and privacy solutions, and present open research issues and challenges of security and privacy in smart cities.
B) Data Derived from the Objective:	
Vulnerabilities	Heterogeneous Interaction and the Requirement of the Lightweight Cryptographic Algorithm: The connected devices and smart objects usually interact in heterogeneous environments due to the diversity of manufacturers and enterprises for designing such devices under different standards, protocols, and technical requirements. As a result, it is very difficult to propose a security method that can meet the requirements, homogeneity, and interoperability criteria of all smart city devices. Secure Storage and Transaction Logging: [...]because of the presence of unverified storage services and mismatched security policies, there are several vulnerabilities that threaten the security of auto-tiering databases: (i) The auto-tiering databases automatically reallocate the data based on the rate of the access requests with the range of rarely accessed to critical information. Data and Computation Outsourcing: Cloud computing provides an effective way to store the huge amount of collected data and perform the computation with minimum overhead on connected devices in the smart cities. However, by outsourcing the data in the remote servers, the physical control over the data is taken away and the management of data is delegated to an untrusted CSP. Anonymity: [...]Designing an efficient end-to-end anonymity method to protect user privacy on the basis of concealing data communication paths is still a critical challenge in smart cities because of the large number of IoT devices (e.g., sensors) for data collection.[...]

A) Publication Data:	
Title:	Security Challenges in IoT enabled Smart Grid: Taxonomy of Novel Techniques and Algorithm
Author(s):	Prakash, S. and Jaiswal, S.
Source of Publication:	International Conference on Inventive Computation Technologies
Year of Publication:	2018
Abstract:	The traditional power system network is under a process of evolution to Smart Grids (SGs) to take care of the issues like uni-directional communication, energy wastage, information flow, security and resource sharing. Smart grid is an electrical grid which provides energy to the end users with effectiveness efficiency. Smart grid offer bi-directional

	information flow between service providers and consumers, including power generation, transmission, consumption, distribution and its use frameworks. Due to its vast usage and huge network electronic power conditioning, power distribution, control of the production of energy and its distribution becomes difficult. To overcome such problems Internet of Things will provide the necessary support to smart grid so that easy transmission and power distribution will take place with much needed convenient system to operate. Smart grid is also using the internet facility for exchange of data which makes the system more vulnerable and prone to cyber-attack. In this paper, there has been a constant effort to analyse the different methods to solve the above problems by employing different strategies algorithms.
B) Data Derived from the Objective:	
Vulnerabilities	Access control-it is a security technique that can be used to provide physical and technical security. It is the process of limiting unauthorized or unwanted indulgence of any unauthorized access. Cryptography techniques for securing IOT aided SG. Cryptography is science art and study of hiding essential information from the perspective of keeping information safe.

A) Publication Data:	
Title:	A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges
Author(s):	Sfar, A.R. and Chtourou, Z. and Challal, Y.
Source of Publication:	International Conference on Smart, Monitored and Controlled Cities
Year of Publication:	2017
Abstract:	Securing data, objects, networks, systems and people in the Internet of Things (IoT) will have a prominent role in the research and standardization activities of the next years. The high connectivity of intelligent objects and their severe constraints lead to many security challenges, which are not included into the classical formulation of security problems and solutions. To help interested researchers to contribute to this research area, an IoT security roadmap overview is presented in this work based on a novel cognitive and systemic vision. The role of each component of the approach will be explained and relations with the other elements and their impact on the overall system will be detailed. According to the novel taxonomy of IoT vision, a case study of military live simulation will be presented to highlight components and interactions of the systemic and cognitive approach. Then, a discussion of security questions about privacy, trust, identification and access control will be provided, and different research challenges will be highlighted.
B) Data Derived from the Objective:	
Vulnerabilities	Their behavior depends on their personalities, skills, knowledge, motivations, expectations, visions, etc. To address security questions related to people in loT context, it is meaningful to handle them within a systemic approach by providing a global revision of rules and practices. For example, we consider different types of human profiles such as consumers, end users, service or technology providers, etc. All of them are necessary in controlling and improving security issues. Identification/Access Control: Used to identify and localize objects, systems and persons. Due to its specific features (size, ubiquity, heterogeneity, etc.), IoT architecture has to consider access and

	identification of any intelligent object by any remote system through a global identification and addressing system would be mandatory. Auto-Immunity: Concerns exclusively intelligent objects because they may be exposed to physical attacks in hostile areas (absence of communication channel, limitations of memory and calculation capacity, limited physical defense, etc.).

A) Publication Data:	
Title:	Autonomous Vehicle Security: A Taxonomy of Attacks and Defences
Author(s):	Thing, V.L.L. and Wu, J.
Source of Publication:	local de publicação
Year of Publication:	2017
Abstract:	texto contendo uma descrição do Abstract
B) Data Derived from the Objective:	
Vulnerabilities	An attack vector is a path or means by which an adversary can gain unauthorized access to a target system. It is also an enabler for adversaries to carry out vulnerability exploitation on the target systems. Adversaries could gain unauthorized access to autonomous vehicles via either physical access (or close proximity access) or wireless remote access. - Side-channel attacks: A side-channel attack refers to attacks that result in revealing useful information regarding the transmitted data or the internal working of the system through alternative paths. - Code Modification: [...]Defences against such attacks is to ensure connections to the vehicle are password-protected so that only authorized personnel are granted access, and that only authorized and verified code modification can be carried out. - Code Injection Jamming attacks are availability attacks against the wireless medium or the external facing sensors. Consequently, the authorized communication is disrupted[...] Encryption is fundamental and crucial in protecting vehicular data transmission. Through encryption, the confidentiality of the data transmission can be assured. To ensure that the controllers of the AV can be trusted, certificates can be issued to support the authentication process

A) Publication Data:	
Title:	Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges
Author(s):	nome dos autores
Source of Publication:	local de publicação
Year of Publication:	ano de publicação
Abstract:	texto contendo uma descrição do Abstract
B) Data Derived from the Objective:	

Vulnerabilities	[...]One of the best ways to secure the smart cities communications is to develop lightweight cryptographic methods for encrypting and decrypting data and creating a shared secret key among various nodes.[...] Viruses, worms, and other malware have the capability to overwhelm the systems through the boot sectors where in the such viruses are located as an executable code and are able to be distributed to the other systems through the Internet connection or upon booting the other system using infected disks.[...] Indeed, secure boot is designed as an additional layer to protect the system against the pre-boot process. Secure booting is a technology for helping the system firmware to check the existence of a cryptographic signature for the system boot loader. Autenticação, Identificação e Controle de Acesso Secure Authentication and Access Control for IoT-Based Objects: The smart devices, like smart phones and sensing nodes, are responsible to collect data in the smart cities, suffer from resource limitation, e.g., energy resources and processing power. As a result, protecting the security of data in such devices requires proposing a lightweight cryptographic algorithm that incurs minimum computation cost on them

A) Publication Data:	
Title:	Internet of Things-Based Security Model and Solutions for Educational Systems
Author(s):	Patnaik, R. and Raju, K.S. and Sivakrishna, K.
Source of Publication:	Studies in Big Data
Year of Publication:	2021
Abstract:	Today the applications of Internet of things (IoT) are progressing rapidly in variety of domains. This encouraged to develop new applications (e.g., smart grid, smart home, smart cities, wearables, and vehicle networking) advancement as well. The emerging application of IoT is exposed toward security, privacy issues, and its challenges. The main objective of this work is to enhance security in the educational system (ES) using IoT devices. We propose several techniques to avail device identification, authenticate the user, and collect the data from various devices. As the IoT sensors are easily negotiable, it allows unauthorized users/devices that are able to steal and override the data from the cloud. This paper represents a brief summary of IoT security threats and challenges and their classification based on the application domain. The authors identified challenges in security issues in IoT-based educational systems and some probable solutions on security. In this research, the authors propose the incremental Gaussian mixture model (IGMM), blockchain, and EdgeSec as a probable solution for security and machine learning (ML) techniques. In this model, few solutions, like IGMM for authorizing the device, blockchain for the encryption of data during transfer in the information network, ML algorithms for identifying and authorizing devices, and EdgeSec, offer a security profile to collect a huge amount of data about each device in the connected IoT environment. The identified model is used for enhancing security in IoT-based educational systems.
B) Data Derived from the Objective:	

Vulnerabilities	Physical Level: Jamming Adversaries: This kind of attack is done by decreasing of network that sent frequency signal without following the any protocols. Insecure Initialization: To ensure a proper and secure network service in IoT, we must initialize and configure IoT devices in the physical layer without deviating secrecy and obstacle to the network. Insecure Physical Interface: Debugging exploits to negotiated nodes in the network by the poor physical security with the help of physical interface and tools Sleep Deprivation Attack: IoT devices are designed to consume low power so these are getting into sleep mode. The attackers are trying to not enter the device into sleep mode. It is known as sleep deprivation Middle Level Buffer Reservation Attack: Nodes are accessing the buffer to send or receive packets and reserving buffer for regathering of storing of packets, by sending broken packets it may be exploited by an attacker [...] It is ensured that the use of cryptographic mechanisms secure data communication over IoT devices Logical Level [...]Application layer is consisting of various types of applications for a different purpose, which is sometimes vulnerable. Insecure Interfaces: The IoT service interfaces used in cloud, Web, and mobile are responsible for susceptible to several attacks, which causes loss of privacy of the data Insecure of Software/Firmware: The software/firmware may cause several susceptibilities which make IoT insecure

A) Publication Data:	
Title:	A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers
Author(s):	Han, T. and Jan, S.R.U. and Tan, Z. and Usman, M. and Jan, M.A. and Khan, R. and Xu, Y.
Source of Publication:	Concurrency and Computation: Practice and Experience
Year of Publication:	2020
Abstract:	Software Defined Network (SDN) and Network Virtualization (NV) are emerged paradigms that simplified the control and management of the next generation networks, most importantly, Internet of Things (IoT), Cloud Computing, and Cyber-Physical Systems. The Internet of Things (IoT) includes a diverse range of a vast collection of heterogeneous devices that require interoperable communication, scalable platforms, and security provisioning. Security provisioning to an SDN-based IoT network poses a real security challenge leading to various serious security threats due to the connection of various heterogeneous devices having a wide range of access protocols. Furthermore, the logical centralized controlled intelligence of the SDN architecture represents a plethora of security challenges due to its single point of failure. It may throw the entire network into chaos and thus expose it to various known

	and unknown security threats and attacks. Security of SDN controlled IoT environment is still in infancy and thus remains the prime research agenda for both the industry and academia. This paper comprehensively reviews the current state-of-the-art security threats, vulnerabilities, and issues at the control plane. Moreover, this paper contributes by presenting a detailed classification of various security attacks on the control layer. A comprehensive state-of-the-art review of the latest mitigation techniques for various security breaches is also presented. Finally, this paper presents future research directions and challenges for further investigation down the line.
B) Data Derived from the Objective:	
Vulnerabilities	In SDN (Software Defined Network), all network-related functionalities are managed, controlled and secured from a centralized controller. The single-point dependency and programmable nature of an SDN controller make it a potential choice for the attackers. If security of the controller is compromised, the whole network is vulnerable to various attacks.[...] The southbound interface needs to be protected and secured against communication overhead. Therefore, unnecessary communication that results in congestion at this interface needs to be avoided for the smooth functioning of the network.[...] DoS/DDoS attacks: The denial-of-service (DoS) and distributed DoS (DDoS) are the most common attacks launched by cyber criminals, cyber extortionists, and hackers. Spoofing attacks on the SDN controller: The controller is the backbone of an SDN network as it manages and controls the whole network. Due to its centralized nature, it is vulnerable to many types of security attacks. One such attack is spoofing attack. In spoofing attacks, an adversary launches attacks on a legal entity (server/system) by mimicking a legitimate user. [...] The only thing that an attacker requires is the same privileges as a normal user. On the other hand, during SQL injection attacks, a perpetrator modifies the anticipated effect of an SQL query by injecting new SQL keywords or operators into the query. [...]

A) Publication Data:	
Title:	Study of the different security threats on the internet of things and their applications
Author(s):	Sahmi, I. and Mazri, T. and Hmina, N.
Source of Publication:	International Conference Proceeding Series
Year of Publication:	2019
Abstract:	The Internet of Things is one of the revolutions of the industry 4.0. It will change our lives mode. It will be present in every domain: healthcare, transportation, at home, agriculture generally in the city. Everyone will be connected to the Internet by the IoT. Furthermore, to realize this vision, the communication through IoT must be secure. So, it's one of the greatest challenges faced by the scientist's community today in their recent researches. This paper is a study of the different security threats on the Internet of Things by category in one hand: on data and network, on privacy and on system and IoT, and on the other hand we will details some threats on application's domain like smart home and smart city.
B) Data Derived from the Objective:	
Vulnerabilities	physical attacks :

	Node Tampering: The attacker can cause damage to a sensor node, by physically replacing the entire node or part of its hardware or even electronically interrogating the nodes to gain access and alter sensitive information [8]. RF Interference on RFIDs: The attacker by creating and sending noise signals over the Radio Frequency signals [9], the noise signals will interfere with the RFID signals hindering communication. Malicious Node Injection: The attacker deploy a new malicious node between two or more nodes of the IoT system, hence controlling all data flow; this is also known as Man in The Middle Attack [8]. Physical Damage: The attacker can physically damage devices of the IoT network with the purpose of impacting the availability of service [8]. Sleep Deprivation Attack: This attack, keeps the nodes awake which will result in a more power consumption, and will cause the nodes to shut down [8]. Malicious Code Injection: The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system [8]. Social Engineering: The attacker manipulates users of an IoT system, to extract private information [8]. network's attacks: RFID Cloning: An attacker clones an RFID tag by copying data from the victim's RFID tag, onto another RFID tag [8]. RFID Unauthorized Access: The attacker can read, modify or even delete data on the RFID nodes, Because of the lack of proper authentication mechanisms in most RFID systems [11]. The attacker over the network manages to interfere between two sensor nodes, accessing restricted data, violating the privacy of the two nodes by monitoring, eavesdropping and controlling the communication between the two sensor nodes [12]. Denial of Service: An attacker can bombard an IoT network with more traffic data that it can handle which can result in a successful Routing Information Attacks by spoofing, altering or replaying routing information can complicate the network and create routing loops [13]. IoT devices have limited resources so they are more vulnerable than the others, so it's necessary to study the different vectors of vulnerabilities: IoT Device Memory: Most of the IoT devices have a limited memory capacity and therefore external memory is needed to satisfy the demands. This will open threat points for the system in many ways [1]. IoT Web Interfaces: Most of the IoT devices may have a web interface which needs to be connected to database servers. One of the major security threats for such systems is SQL injection and cross-site scripting are some of the attacks that could impact the web interfaces IoT [17]. IoT device network services: Inability to execute high-level encryption algorithms on IoT devices make it vulnerable to information disclosure attacks. Due to the resource constraints such as computational power and data storage capacity, IoT devices are not expected to perform payload verification and integrity checking which make the system insecure [17]. IoT device software update: Software update is one process which should never fail or compromise in an IoT based system. Manually updating the patches for every IoT device may not be feasible. A cloud-based approach is one solution, but since the cloud also imposes security threats, updating the software patches for IoT devices is still under research [1].

	IoT Data storage methods: Due to limited processing power and storage capacity, the data stored in IoT devices may be unencrypted. Most of IoT devices will support only symmetric encryption [1]. IoT AAA services: IoT Authentication, Authorization, and Accounting (AAA) services will be a challenging task. Because of the distributed nature of IoT systems, the device responsible for AAA will be under great challenge [1]. Phishing Attacks: The attacker gains access to confidential data by spoofing the authentication credentials of a user, usually through infected emails or phishing websites [14]. Malicious Scripts: The user that controls the gateway can be fooled into running executable active-x scripts which could result in a complete system shut down or data theft [18]. Denial of Service: An attacker can execute DoS or distributed denial of service DDoS attacks on the affected IoT network through the application layer, affecting all users in the network [18] From physical attack, malicious code injection attack has been the dangerous attack since it is not only stopping the services but also modify the data.

A) Publication Data:	
Title:	A survey on attacks in Internet of Things based networks
Author(s):	Benzarti, S. and Triki, B. and Korbaa, O.
Source of Publication:	International Conference on Engineering and MIS
Year of Publication:	2018
Abstract:	Nowadays, the study of the security of IoT has caught many attentions of researchers. Improving our world to be a better environment building a city of dreams which is called smart city is a trend field of research. In this context, objects will be connected to the Internet interacting with each other making the world more smarter. The variety of networks building makes the IoT vulnerable. Smart home, smart grid, Smart transport, WSN, UASN, UWASN, etc make our lives more easier by offering intelligent services that save time and effort. However, each network is exposed to some attacks that can disturb its performance. In this paper, we present a classification of attacks from various networks involved in IoT. This classification distinguish common and specific attacks from each network and use some criteria like the security attributes, congestion, disturbance. Also, some existing security solutions are presented in details in order to expose the security requirements to protect IoT.
B) Data Derived from the Objective:	
Vulnerabilities	COMMON ATTACKS IN IoT NETWORKS: Jamming: In physical layer, jamming is considered as the primary DOS attack [10]. It has the ability to disturb the communication of an appliance or a network by a powerful jamming source like diffusing radio signals [3]. Sinkhole attack: The attacker becomes attractive by offering optimal paths to reach the base station with powerful connections which pushes the transmitting nodes to change their routing tables to route data by the malicious node. Tampering : It is important to mention that an adversary can tamper with the device and use it to insert impostor to the system, use the device maliciously or out of its intended functionality [3] Denial of Service attack : It refers to the property of being inaccessible when requested by an authorized user.

	especifics smart home attacks: Malicious Code Injection: As indicated by his name, this attack injects a malicious code through the debugging interface of the device. ACK Attack: The wireless channel can be eavesdropped in order to send a fake ACK[3]. Phishing/Pharming: In this case, a malicious entity attempts to guide the user of the device to another server or for marketing purposes or to try to deceive to steal personal information Specific attacks in smart grid: Access through database links: As we know, the activities of a system are saved in databases. Whereas, if these databases are configured improperly, an attacker can access to them and may control the network system[5].

A) Publication Data:	
Title:	Analysing the resilience of the internet of things against physical and proximity attacks
Author(s):	Xu, H. and Sgandurra, D. and Mayes, K. and Li, P. and Wang, R.
Source of Publication:	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
Year of Publication:	2017
Abstract:	The Internet of Things (IoT) technology is being widely integrated in many areas like smart-homes, smart-cities, healthcare, and critical infrastructures. As shown by some recent incidents, like the Mirai and BrickerBot botnets, security is a key issue for current and future IoT systems. In this paper, we examine the security of different categories of IoT devices to understand their resilience under different security conditions for attackers. In particular, we analyse IoT robustness against attacks performed under two threat models, namely (i) physical access of the attacker, (ii) close proximity of the attacker (i.e., RFID and WiFi ranges). We discuss the results of the tests we performed on different categories of IoT devices, namely IP cameras, OFo bike locks, RFID-based smart-locks, and smart-home WiFi routers. The results show that most of IoT devices do not address basic vulnerabilities, which can be exploitable under different threat models.
B) Data Derived from the Objective:	
Vulnerabilities	Physical Attack. In this threat model, an attacker can physically interact with the IoT device without notification to Alice. For example, the attacker can access the hardware, and read and modify the default IoT device's settings, which may impact the privacy and authentication credentials of Alice. [...] , the user that will scan this QR Code with their mobiles phones will be redirected to a fake website that may request downloading a trojanized app that is similar to OFo app.[...] d when the user scans the code she will download a fake app update, which gives an attacker remote access to it.

A) Publication Data:	
Title:	Flying through the secure fog: A complete study on UAV-Fog in heterogeneous networks
Author(s):	Gupta, A. and Gupta, S.K.

Source of Publication:	International Journal of Communication Systems
Year of Publication:	2022
Abstract:	A drone or unmanned aerial vehicles (UAVs) is becoming a trending area for researchers worldwide. UAV's contribution is increasing in day-to-day life, whether it is in a military zone, disaster management, healthcare sector, smart cities, Internet of Things (IoT), urban air mobility, and many more. In contrast, UAV's limited computational capability and low-energy sources pose significant challenges for real-time data processing, storage, networking, and security that are critical in emergencies such as floods, earthquakes, and cyclones. UAVs are rapidly used to satisfy user requirements as well as services. As the demand for UAVs aided heterogeneous wireless networks increases in critical emergencies, fog computing serves several benefits to fulfill users' demands in terms of low latency, support, data storage, mobility, availability, scalability, and so on. This study aims to present a comprehensive study with their technical aspects for understanding fog computing, security issues, privacy concerns, and risks, along with its solutions. This paper suggests the collaboration of UAV-Fog architecture based on the four-tier network consisting of smart things, local UAVs, UAV-Fog, and cloud server, to control UAV's data and also described some of the security issues faced by this cloud infrastructure. Further, this research article also sheds new light on some scenarios of UAV-Fog for such deployments, applications, opportunities, challenges, and their major security threats and their countermeasures. Afterward, we design taxonomy of the collaboration of UAV-Fog with their respective approaches.
B) Data Derived from the Objective:	
Vulnerabilities	Authentication has become one of the security problems that are most concerned in this network since large services are delivered on a wide scale.[...] Cyber-attacks: Cryptography algorithms for smart devices to tackle device tampering Man-in-the-middle attack: It is a type of attack in which an attacker intervenes in an ongoing conversation or data transmission. After placing themselves in the “middle” of the conversation or transmission, the perpetrators pose as both legal parties. DoS and DDoS attack: DoS attacks are performed by flooding the target system with traffic requests or sending more data that causes the UAV's network to crash. The DDoS deals with more devices sending traffic requests to crash the whole system. Jamming: When RF noise is actively induced to disrupt aerial and ground services or restrict devices in a network from communicating with each other, this is known as jamming. The jamming attacks will degrade the quality of services. Phishing: It is a type of cyber-attack in which the attacker sends a fraud message to ground users in order to gain the credentials and sensitive information of the network users

A) Publication Data:	
Title:	Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review
Author(s):	Ali, R.F. and Muneer, A. and Dominic, P.D.D. and Taib, S.M. and Ghaleb, E.A.A.

Source of Publication:	Communications in Computer and Information Science
Year of Publication:	2021
Abstract:	The Internet of Things (IoT), often known as the Internet of Everything, is a new technological paradigm visualized as a worldwide network of interconnected machines. IoT brings another dimension into Information Technology (IT), where machines can communicate with various machines and humans. Researchers and IT industry produced various IoT devices, architectures. Different ways are introduced to implement and use IoT concepts. IoT is getting more intention in ideas like smart homes and smart cities, raising security concerns. This article aims to gather the reported security issues, the classification of those issues, and the solutions that were provided against those IoT security issues.
B) Data Derived from the Objective:	
Vulnerabilities	Every object in the IoT platform needs to be identified by the system and other objects. Every object needs to be authenticated before interacting with the system or other objects in the IoT platform [12][13]. Ensuring the data is available to authorized persons or objects is a critical task. Management of data is also vital to protect and manage that data so that the authorized objects will get their data [14]. A key management system needs to be enabled for ensuring confidentiality. They also gave the reason for these attacks; the devices either had unpatched vulnerabilities or used default passwords. The solution to these malware's is mainly related to energy consumption patterns and OpCode.[...] IoT, as we know, has small storage and processing power, so DNS security models cannot be implemented. It poses threats like DNS Cache Poisoning and Man-In-The-Middle attacks [18, 19]. Denial of Service (DOS), Denial of Sleep (also called sleep deprivation) attacks is flooding-type attacks where the device is flooded with requests until it stops responding and consumes all its energy (battery) to respond to these flooding requests. It is sometimes called an exhaustion attack as well.[...] IoT systems are vulnerable to many vulnerabilities, including encryption, decryption mechanisms, intruding into the network, and flooding requests. Whenever an attack happens, it exploits the vulnerabilities found in the system because every attack targets some specific vulnerabilities and then exploits them. The Authors proposed a fog-based distributed attack detection mechanism for IoT. [...]

A) Publication Data:	
Title:	On the security of the 5G-IoT architecture
Author(s):	Rahimi, H. and Zibaeenejad, A. and Rajabzadeh, P. and Safavi, A.A.
Source of Publication:	International Conference Proceeding Series
Year of Publication:	2018
Abstract:	In this paper, we study the security aspects of the new 5G-IoT architecture, which is recently developed by this research team. We classify potential security attacks at each layer of the 5G-IoT architecture. As the main contribution of this work, we propose a security taxonomy for the 5G-IoT architecture in the context of smart city applications. This taxonomy consists of five layers to confront the studied attacks and to protect the privacy of clients. The number of layers is selected according to the types of attacks where each attack type affects a particular layer of the 5G-IoT architecture.

B) Data Derived from the Objective:	
Vulnerabilities	Physical Device Layer: Unauthorized Access to the Tags. The lack of effective authentication techniques for RFID systems allows attackers to easily access tags. In WSNs, if an attacker has access to the network, he can easily use the whole network. Tag Cloning. Cloning RFID tags is an effective attack in the physical layer. By this attack, the important information could be captured by reverse engineering or directly from its deployment environment. RF Jamming. In this attack, RF signals are sent to the network to disturb communication between the tags and readers. Attackers could employ RF jamming to prevent readers from communicating with all tags by interfering with all the signals within its range. Communication Layer: DoS Attack. A Denial of Service (DoS) network attacker engages the victim with flooding of requests by making a large mass of network traffic. Sybil Attack. A node in the system shows multiple pseudonymous identities to a victim node. This action is able to deceive the victim node to perform an action multiple time. Eavesdropping. Eavesdropping includes a blocking of data flow between two connected devices. In the IoT systems, it occurs on the network layer to takes the form of information sniffing. During data communication, we use privacy as a technique to provide security with efficient access control corresponding eavesdropping. Application Layer: Code Injection. In this attack, attackers for a variety of purposes such as stealing data, getting system control, and propagating worms inject malicious codes into the system to exploit program errors. Buffer Overflow. In this threat, attackers use program vulnerabilities to involve the violation of the bounds of code or data buffer. In fact, attackers put a long series of data to a specified area, to make the system overflow. Phishing Attack. In this threat, attackers act like a real user or authorized institution to receive sensitive information from users such as passwords and credit card details. Perception Layer Access Control. IoT devices largely preserve the information in the RFID tags cannot be caught at insistence, instead to block privacy leak users. In addition, it consists of label failure, processor certainty, analysis of antenna energy, etc. Data Encryption. Data security of RFID system necessitates encryption of the RFID signal, using the appropriate algorithm. According to [13], a nonlinear key algorithm based on the displacement calculation realizes RFID system data encryption Physical Security Design. This contains both node and antenna design. The node design means hardware composition design and security processor selection, processor link, radio frequency circuit design, data acquiring unit design; whereas antenna design has to have high communication range, high flexibility, stability, etc

A) Publication Data:	
Title:	IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment

Author(s):	Kariri, E.
Source of Publication:	IETE Journal of Research
Year of Publication:	2022
Abstract:	Smart farming or development in agriculture Cyber-Physical Systems has led to the development of various IOT based innovative platforms to aid automated systems for precision agriculture. There are smart devices (IoT devices, smart vehicles, UAVs, ROVs, and drones) and sensors (magnetic, electrochemical, and mechanical sensors)constantly connected at the edge and procure data that is uploaded to cloud-based interfaces for further processing. The sensors can be maneuvered using an insecure, intelligent farming system to create choreographed cybersecurity attacks on a particular farm. End-to-end system is achieved by putting together smart devices, communication media, uploading data to the cloud, intermediate nodes, and processing this data at a central unit like the cloud or intermediate processing at other nodes. Cyber-physical systems are a combination of many technologies, resulting in a large number of security threats. This chapter is to delineate the attack vectors and categories of threats that can be performed on these innovative IOT based agricultural products; if not appropriately secured, can lead to more strategized and sophisticated security attacks that can hinder production for a region under effect and thus bringing down the economy and food stocks of Nations who implemented smart agriculture.
B) Data Derived from the Objective:	
Vulnerabilities	Node Tampering/Jamming: Equipment such as actuators, sensors are generally embedded in nature, having a single task to perform. Therefore, these nodes cannot have more security forefront. Attacks like node tampering, jamming are more prevalent. Interferences/Insider Attacks: The perception layer in IoT is more susceptible to insider attacks wherein eavesdropping; interferences can be introduced by injecting an external agent in disguise. Physical Damage: Physical damage to equipment can be natural as a result of calamity or otherwise. It can lead to null values at receiving end or missed values, which can cause an imbalance in the real-time processing of data. Unauthorized Access: To provide for crops through smart IOT based agriculture deployments, it is highly important to properly monitor conditions in real-time. Denial of Service: According to [5], in precision agricultural systems, the denial of service is more frequent towards users using smart services; the threats can be due to poorly managed systems, disruption to PNT(positioning, navigation, and timing) systems that use GPS to collect information for processing. Encryption: Encryption of contents is extremely important when the data is transmitted or stored; the practice helps to secure the parameter to a vast extent Social Engineering: A naive user is often the most insecure point in the complete network; Phishing is another social engineering attack strategy that is generally used to lure the users into clicking on synonymous links to gain access;

A) Dados da publicação:	
Título:	Future Directions of Cybersecurity in Industrial Internet of Things Through Edge Computing
Autor(es):	T. Zhukabayeva, L. Zholshiyeva and N. Karabayev

Fonte de Publicação:	9th International Conference on Computer Science and Engineering (UBMK)
Ano da Publicação:	2024
Resumo:	As Industrial Internet of Things (IIoT) technologies and edge computing continue to evolve, the volume of data processed in real-time to optimize manufacturing processes has increased. However, this increase in connected devices also amplifies the risks associated with cyber threats. This paper examines the use of edge computing in cyber-physical systems (CPSs) to ensure security in IIoT environments. The focus is on analyzing existing security issues by comparing research related to vulnerability protection in industrial networks and proposing solutions to enhance data protection. The study includes a comparative analysis of traditional IoT and IIoT systems, as well as a proposed taxonomy of solutions with future strategies aimed at improving security within industrial networks.
B) Dados derivados do objetivo:	
Vulnerabilidades	- In wireless communication, data exchange in IIoT interactions is vulnerable to numerous security and privacy issues, especially in IIoT group communication environments with many devices. - Security challenges in edge computing, such as unauthorized access and breaches of confidentiality, remain inadequately addressed in urban architecture and require furthe r research. - The implementation of IIoT faces several key challenges. Heterogeneity is a significant issue, as the variety of devices and protocols complicates compatibility and integration. - Additionally, IIoT devices often have limited resources, such as constrained power and memory, which restrict their functionality.

A) Dados da publicação:	
Título:	Radon transform based malware classification in cyber-physical system using deep learning
Autor(es):	Rasim Alguliyev, Ramiz Aliguliyev, Lyudmila Sukhostat
Fonte de Publicação:	Results in Control and Optimization
Ano da Publicação:	2024
Resumo:	The development of cyber-physical systems entails the growth and diversity of malware, which increases the scale of cybersecurity threats. Attackers use malicious software to compromise various components of cyber-physical systems. Existing technologies make it possible to reduce the risk of malware infection using vulnerability and intrusion

	scanners, network analyzers, and other tools. However, there is no perfect protection against the increasingly sophisticated types of malware. The goal of this research is to solve this problem by combining different visual representations of malware and detection models based on transfer learning. This method considers two pre-trained deep neural network models (AlexNet and MobileNet) that are capable of differentiating various malware families using grayscale images. Radon transform is applied to the resulting grayscale malware images to improve the classification accuracy of the new malware binaries. The proposed model is evaluated using three datasets (Microsoft Malware Classification, IoT_Malware and MalNet-Image datasets). The results show the superiority of the proposed model based on transfer learning over other methods in terms of the efficiency of classifying malware families aimed at infecting cyber-physical systems.
B) Dados derivados do objetivo:	
Vulnerabilidades	- CPSs consist of a large number of connected devices (e.g., sensors, smart meters, etc.) that are targeted by many malware families, such as Tsunami, Bashlite, and Mirai [7]. They take advantage of weak authentication, outdated firmware, and scanners designed to find open ports and compromise system devices - The weakest link in the CPS security chain is the human factor. Cybercriminals use this factor to gain unauthorized access, steal personal data, and infect systems with malware

A) Dados da publicação:	
Título:	Vulnerability Detection in Cyber-Physical System Using Machine Learning
Autor(es):	Bharathi V, Vinoth Kumar C N S
Fonte de Publicação:	Scalable Computing: Practice and Experience
Ano da Publicação:	2024
Resumo:	The cyber-physical system is a specific type of IoT communication environment that deals with communication through innovative healthcare (medical) devices. The traditional medical system has been partially replaced by this application, improving healthcare through efficiency, accessibility, and personalization. The intelligent healthcare industry utilizes wireless medical sensors to gather patient health information and send it to a distant server for diagnosis or treatment. The healthcare industry must increase electronic device accuracy, reliability, and productivity. Artificial intelligence (AI) has been applied in various industries, but cybersecurity for cyber-physical systems (CPS) is still a recent topic. This work presents a

	method for intelligent threat recognition based on machine learning (ML) that enables run-time risk assessment for better situational awareness in CPS security monitoring. Several machine learning techniques, including Nave Bayes (65.4\%), Support Vector Machine (64.1%), Decision Tree (89.6%), Random Forest (92.5%), and Ensemble crossover (EC) XG boost classifier (99.64), were used to classify the malicious activities on real-world testbeds. The outcomes demonstrate that the Ensemble crossover XG boost enabled the best classification accuracy. When used in industrial reference applications, the model creates a safe environment where the patient is only made aware of risks when categorization optimism exceeds a specific limit, minimizing security managers' pressure and efficiently assisting their choices.
B) Dados derivados do objetivo:	
Vulnerabilidades	- Cyberattacks can compromise the accuracy and reliability of patient data, making it difficult for healthcare providers to make informed decisions - The availability of sensitive health data can be exploited, leading to unauthorized access and potential data breaches - Cyber threats can directly affect the integrity of medical devices, which may lead to malfunction or incorrect operation, posing risks to patient safety - Vulnerabilities in environmental monitoring systems (like temperature and humidity controls in ICUs) can affect the conditions necessary for patient care

A) Dados da publicação:	
Título:	Preamble-based RF-DNA Fingerprinting Under Varying Temperatures
Autor(es):	Cinque S. Peggs; Tanner S. Jackson; Ashley N. Tittlebaugh; Taylor G. Olp; Joshua H. Tyler; Donald R. Reising
Fonte de Publicação:	12th Mediterranean Conference on Embedded Computing (MECO)
Ano da Publicação:	2023
Resumo:	A total of 30.9 billion Internet of Things (loT) deployments are expected by 2025 with most employing weak or no encryption at all, which raises concerns about loT security. This concern is exacerbated by loT-connected critical infrastructure and the successful exploitation of this security vulnerability. This led researchers to propose a physical layer-based loT security solution coined Specific Emitter Identification (SEI). However, SEI has been shown to be sensitive to temperature changes. This sensitivity is important when considering loT deployments in highly

	variable temperature environments. The presented approach shows the temperature sensitivity of SEI is mitigated when the classifier is trained using RF-DNA fingerprints drawn from waveforms collected at two temperatures. In fact, SEI performance improves the most when the two temperatures are at or near the extremes of the operating temperature range. Specifically, our work shows that training SEI classifiers using the extremes of the collected temperatures improves overall classification performance across temperature ranges. The work in this paper also shows that emitters operating in a sub-ambient, exothermic state have a more consistent fingerprint than those operating in a high-temperature, endothermic state.
B) Dados derivados do objetivo:	
Vulnerabilidades	- A total of 30.9 billion Internet of Things (loT) deployments are expected by 2025 with most employing weak or no encryption at all, which raises concerns about loT security. This concern is exacerbated by loT-connected critical infrastructure and the successful exploitation of this security vulnerability. - In light of this information, loT security remains a pressing concern because most loT devices employ weak or no encryption at all due to (i) onboard resource limitations such as power and memory, (ii) prohibitive manufacturing costs, and (iii) encryption implementation and management challenges.

A) Dados da publicação:	
Título:	Blockchain Integration with Machine Learning for Securing Fog Computing Vulnerability in Smart City Sustainability
Autor(es):	L. A. Ajao and S. T. Apeh
Fonte de Publicação:	1st International Conference on Advanced Innovations in Smart Cities (ICAISC)
Ano da Publicação:	2023
Resumo:	The advent of a smart city-based industrial Internet of Things (IIoT) is confidently built on the combined protocols of a virtual IPv6 addressing scheme and the fifth generation (5G) mobile network. For better network service and to achieve Quality of Experience (QoE) in the architecture. But this intelligent city architecture is vulnerable to several cyber-attack and malicious actors at the different layers which make it exposed to the same attacks as in the conventional IPv4 wireless sensor networks. However, this work aims to develop a blockchain-based machine learning (BML) security framework that secures the fog computing layer vulnerability in the smart city's sustainability. The machine learning approach is firstly implemented between

	the edge layer and fog server nodes of the city architecture for the variants of intrusion detection using different ML algorithms for the attack's discovery and classification. While the augmented blockchain technology is implemented between the fog layer and cloud computing to enhance the privacy and confidentiality of packet traffic broadcast to the public. The results obtained from ML-IDS show high-performance detection accuracy and low processing time. While the blockchain framework is also evaluated based on the certmcate generation, and retrieval size in bytes and time in milliseconds.
B) Dados derivados do objetivo:	
Vulnerabilidades	- This research proposed an enhanced security framework for the fog computing layer's vulnerability to attacks in intelligent city architecture. Using augmentation of a blockchain-based machine learning algorithm for intrusion detection system (BML-IDS) as illustrated in "Fig. 2". These techniques help to secure the big data transmitted from the edge computing layer through the fog server nodes to the cloud computing without information tampering or alteration. - The transmission of collected big data traffic from the edge computing layer through the fog server node is secured using Machine Learning (ML) algorithms. This ML algorithm helps to detect infiltration of abnormal activity that intends to eavesdrop on the packet traffic in the city's network. By classifying the city's traffic into normal and abnormal through the features extraction processes of a collected packet captured (PCAP).