

CITATION REPORT

List of articles citing

Cyber-physical systems information gathering: A smart home case study

DOI: 10.1016/j.comnet.2018.03.024
Computer Networks, 2018, 138, 1-12.

Source: <https://exaly.com/paper-pdf/69363007/citation-report.pdf>

Version: 2024-04-20

This report has been generated based on the citations recorded by exaly.com for the above article. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

| # | Paper | IF | Citations |
|----|---|------|-----------|
| 49 | An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. <i>Future Generation Computer Systems</i> , 2018 , 89, 685-697 | 7.5 | 74 |
| 48 | A taxonomy of cyber-physical threats and impact in the smart home. <i>Computers and Security</i> , 2018 , 78, 398-428 | 4.9 | 38 |
| 47 | Multimedia learning platform development and implementation based on cloud environment. <i>Multimedia Tools and Applications</i> , 2019 , 78, 35651-35664 | 2.5 | 4 |
| 46 | . <i>IEEE Transactions on Cloud Computing</i> , 2019 , 1-1 | 3.3 | 8 |
| 45 | . 2019 , | | 6 |
| 44 | Privacy-Preserving Multi-Receiver Certificateless Broadcast Encryption Scheme with De-Duplication. <i>Sensors</i> , 2019 , 19, | 3.8 | 2 |
| 43 | Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. <i>Digital Investigation</i> , 2019 , 28, S40-S49 | 3.3 | 19 |
| 42 | How Do I Share My IoT Forensic Experience With the Broader Community? An Automated Knowledge Sharing IoT Forensic Platform. <i>IEEE Internet of Things Journal</i> , 2019 , 6, 6850-6861 | 10.7 | 20 |
| 41 | IoT Forensics: Amazon Echo as a Use Case. <i>IEEE Internet of Things Journal</i> , 2019 , 6, 6487-6497 | 10.7 | 50 |
| 40 | Remotely Access My Smart Home in Private: An Anti-Tracking Authentication and Key Agreement Scheme. <i>IEEE Access</i> , 2019 , 7, 41835-41851 | 3.5 | 20 |
| 39 | . <i>IEEE Access</i> , 2019 , 7, 177241-177253 | 3.5 | 5 |
| 38 | Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch. 2019 , | | 3 |
| 37 | An Efficient Authentication Protocol for RFID-Based Supply Chains. <i>Advances in Intelligent Systems and Computing</i> , 2019 , 28-37 | 0.4 | |
| 36 | Detection of Anomaly in Firewall Rule-Sets. <i>Advances in Intelligent Systems and Computing</i> , 2019 , 422-431. | 0.4 | 1 |
| 35 | Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. <i>Future Generation Computer Systems</i> , 2019 , 92, 265-275 | 7.5 | 134 |
| 34 | Secure and Efficient Two-Party Signing Protocol for the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020 , 17, 1124-1132 | 3.9 | 25 |
| 33 | A Survey on Digital Forensics in Internet of Things. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 1-15 | 10.7 | 23 |

| | | | |
|----|---|------|----|
| 32 | HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 818-829 | 10.7 | 65 |
| 31 | Deep video-to-video transformations for accessibility with an application to photosensitivity. <i>Pattern Recognition Letters</i> , 2020 , 137, 99-107 | 4.7 | 0 |
| 30 | Key-Free Authentication Protocol Against Subverted Indoor Smart Devices for Smart Home. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 1039-1047 | 10.7 | 10 |
| 29 | PowerHammer: Exfiltrating Data From Air-Gapped Computers Through Power Lines. <i>IEEE Transactions on Information Forensics and Security</i> , 2020 , 15, 1879-1890 | 8 | 7 |
| 28 | The need for Internet of Things digital forensic black-boxes. <i>Wiley Interdisciplinary Reviews Forensic Science</i> , 2020 , 2, | 2.6 | |
| 27 | CyberPhysical Systems Forensics: Today and Tomorrow. <i>Journal of Sensor and Actuator Networks</i> , 2020 , 9, 37 | 3.8 | 8 |
| 26 | Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review. <i>Smart Cities</i> , 2020 , 3, 894-927 | 3.3 | 11 |
| 25 | Incidents Are Meant for Learning, Not Repeating: Sharing Knowledge About Security Incidents in Cyber-Physical Systems. <i>IEEE Transactions on Software Engineering</i> , 2020 , 1-1 | 3.5 | 1 |
| 24 | Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. <i>Advanced Sciences and Technologies for Security Applications</i> , 2020 , | 0.6 | 4 |
| 23 | Provably Secure and Lightweight Identity-Based Authenticated Data Sharing Protocol for Cyber-Physical Cloud Environment. <i>IEEE Transactions on Cloud Computing</i> , 2021 , 9, 318-330 | 3.3 | 19 |
| 22 | Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey. <i>Wireless Communications and Mobile Computing</i> , 2021 , 2021, 1-30 | 1.9 | 10 |
| 21 | IoT Cloud Security Review. <i>ACM Computing Surveys</i> , 2021 , 54, 1-36 | 13.4 | 2 |
| 20 | . 2021 , | | |
| 19 | AI-enabled device digital forensics for smart cities. <i>Journal of Supercomputing</i> , 1 | 2.5 | 3 |
| 18 | Smart City Healthcare Cyber Physical System: Characteristics, Technologies and Challenges. <i>Wireless Personal Communications</i> , 2021 , 1-21 | 1.9 | 4 |
| 17 | . <i>IEEE Access</i> , 2021 , 9, 26388-26419 | 3.5 | 8 |
| 16 | Edge Intelligent Joint Optimization for Lifetime and Latency in Large-Scale Cyber-Physical Systems. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1 | 10.7 | 4 |
| 15 | Digital Twins for Precision Healthcare. <i>Advanced Sciences and Technologies for Security Applications</i> , 2020 , 133-158 | 0.6 | 15 |

| | | | |
|----|--|-----|---|
| 14 | IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. 2022 , 7-39 | | 0 |
| 13 | Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges. <i>Sensors</i> , 2021 , 21, | 3.8 | 1 |
| 12 | Open Challenges of Communication Security in an IoT Environment: A Survey. <i>Smart Innovation, Systems and Technologies</i> , 2022 , 107-116 | 0.5 | |
| 11 | K stliche Intelligenz [multiskale und cross-dom ne Synergien von Raumfahrt und Bauwesen. 2022 , 607-690 | | 1 |
| 10 | Assessing Vulnerabilities and IoT-Enabled Attacks on Smart Lighting Systems. <i>Lecture Notes in Computer Science</i> , 2022 , 199-217 | 0.9 | 1 |
| 9 | Assessing smart light enabled cyber-physical attack paths on urban infrastructures and services. <i>Connection Science</i> , 2022 , 34, 1401-1429 | 2.8 | 1 |
| 8 | Cyber-physical system for intelligent control of infrared heating. 2022 , 55, 37-41 | | 0 |
| 7 | Forensic analysis of the Xiaomi Mi Smart Sensor Set. 2022 , 42, 301451 | | 0 |
| 6 | A Detection Technique Using Dual Authentication Stages Framework for Rogue Access Point Identification. 2022 , 1083, 012091 | | 0 |
| 5 | Diagnosis of Health Monitoring Systems in Smart Homes Using Discrete Event System Theory. 2022 , , | | 0 |
| 4 | Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes. 2022 , 12, 12688 | | 0 |
| 3 | A Survey of Cyber-Physical Systems From a Game-Theoretic Perspective. 2023 , 11, 9799-9834 | | 0 |
| 2 | The digital harms of smart home devices: A systematic literature review. 2023 , 145, 107770 | | 0 |
| 1 | Online Voice based Smart Security and Automation System for Real Time Application using Artificial Intelligence. 2022 , | | 0 |