GHOST - Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control

A.Collen[1], N.A.Nijdam[1], J.Augusto-Gonzalez[2], S.K.Katsikas[3], K.M Giannoutakis[4], G.Spathoulas[3], E.Gelenbe[5], K.Votis[4], D.Tzovaras[4], N.Ghavami[6], M.Volkamer[7], P.Haller[8], A.Sánchez[9], and M.Dimas[10]

[1] University of Geneva, Geneva, Switzerland
[2] Televes SA, Santiago de Compostela, Spain
[3] Norwegian University of Science & Technology, Gjøvik, Norway
[4] Centre for Research & Technology, Hellas, Greece
[5] Impertial College London, London, UK
[6] Exus Innovation, London, UK
[7] Technical University of Darmstadt, Darmstadt, Germany
[8] Kalos Information Systems AS, Oslo, Norway
[9] Spanish Red Cross/Tescos, Madrid, Spain
[10] Obrela Security Industries SA, Athens, Greece

Abstract. We present the European research project GHOST, (Safe-guarding home IoT environments with personalised real-time risk control), which challenges the traditional cyber security solutions for the IoT by proposing a novel reference architecture that is embedded in an adequately adapted smart home network gateway, and designed to be vendor-independent. GHOST proposes to lead a paradigm shift in consumer cyber security by coupling usable security with transparency and behavioural engineering.

Keywords: smart home, security, IoT, gateway, risk assessment

1 Introduction

According to [1], the average IoT device was attacked once every two minutes in 2016. Unfortunately, Botnets such as Mirai take advantage of the fact that security is still not a priority for device manufacturers, leading to the lack of possibility of automatic firmware upgrades, exposing the devices to simple attacks such as account enumeration and open ports scanning up to unpatched vulnerabilities presence and their exploitation to gain full control.

In addition to forcing the integration of security aspects into IoT devices at the manufacturer level, it is evident that a monitoring solution is essential to protect the end-users. IoT devices are often completely closed, not standardised or openly developed. Hence, the user does not have a clear idea of the potential risks involved. On top of the purely technological and operational cyber security challenges, the end-user behaviour becomes a determinant factor, with the human typically portrayed as the weakest link in security. Indeed, consumers tend to exhibit low tolerance and fatigue in using sophisticated cyber security solutions or practices, while the cyber security industry often addresses usability as at trade-off on security rather than as a security enhancing component. Thus, combining or integrating usability and security requirements is a major research challenge, which recently has been brought forward [2,3], while turning end-user behaviour in favour of cyber security remains a field with a promising exploitation potential [4].

This paper gives an overview of the European Union Horizon 2020 Research and Innovation project GHOST (`https://www.ghost-iot.eu/`). GHOST aims to increase the level and the effectiveness of automation of existing cyber security services and to enhance system self-defence while prioritising the opening up the cyber security blackbox to consumers and building trust through advanced usable transparency tools derived from end-users mental models. Related work from the GHOST project can be found in [33,34,35,36]. The rest of the paper is structured as follows. Section 2 discusses related work. Section 3 presents the GHOST system, while Section 4 presents the GHOST validation process. Conclusions are summarised in Section 5.

2 Related work

In traditional cyber security, Intrusion Detection Systems (IDS) are taking the main role in detecting any anomalous activity on the network. Best known solutions are Snort [5], Suricata [6] and Bro [7]. While Snort and Suricata are based on pattern matching detection, Bro is relying on semantic matching of the network events. However, these solutions are designed for professional use and are not explicitly aimed at the IoT environment in terms of protocol analysis availability. Global scale architecture with distributed data storage and correlation for IDS was proposed in [8]. While taking advantage of novel technologies and providing wide coverage of monitored data for expert users, this system is not adapted for smart home installation where regular citizens have to understand the usage of this tool. Graphical representation of attack and threats scenes was greatly advanced in [9]. These works are targeting professional analysts with the deep technology knowledge though. Modelling uncertainties in the cyber threat arena was presented in [10], Grey theory application for threat prediction was analysed in [11] and a framework assessing the impact of cyber attacks was described in [12]. Once again, all these advancements are focusing on the expert users, not regular citizens.

2.1 Advancements in IoT Cyber Security Monitoring

Similarly to traditional cyber security IoT ecosystem is vulnerable to the analogous issues as in web, sensor and mobile communications networks, with particular focus on privacy, authentication and access control network configuration, information storage and management, standardisation and data integrity. The most complete classification of the IoT attack vectors is described in [13], referring to the IoT ecosystem as a Web3 or Web of Things phenomenon, where four main categories are provided: Device, Application Service, Network, Web Interface and Data integrity. Developing a cyber security solution targeting to protect all of the identified vectors is a very challenging and crucial task. [14] is raising a necessity to apply the Negative selection and Danger Theory to traditional IDS, to cover ubiquitous nature of the IoT devices and target all attack vectors specified above. Such systems, however, encounter serious limitations in terms computational power and storage requirements. An overview of the Real-time IoT security solutions was provided in [15]. The authors conclude that existing approaches can be divided into two major classes: hardware and software based security. Alternative to IDS approach is described in [16], where SIEM system for IoT environment is proposed.

2.2 Smart Home Cyber Security Frameworks

The authors of [17] analyse existing architectures of smart homes from the security perspective, concluding that gateway architectures are the most suitable to provide key technologies for cyber protection: auto-configuration and automatic update installation. An overview of existing tooling for the implementation of cyber protection in smart homes is also included in their work, however, all these tools are applicable only for newly designed devices to be included in a future smart homes. On contrary, the IDS framework [18], based on Anomaly Behaviour Analysis, approaches this problem for existing and hardly changeable smart home installations. Their focus is given to measuring the activities of installed sensor devices a smart house is equipped with, and detecting any anomalies in the quantity and quality of the collected measurements. The limitation of their work relies in the ability to apply their analysis only on the primitive IoT devices without direct internet access. Similarly to GHOST, traffic monitoring and inspection solution IoTGuard, based on Bro, is presented in [19]. The main drawback of their framework is the requirement to forward all router's traffic to IoT Controller and link each IoT device with the IoT Watchdog. On the contrary, GHOST provides all-in-one solution to be deployed in the existing smart home installations with key focus given to user's experience and understanding of a cyber security solution.

The great interest of developing smart home cyber security solutions is also given by the commercial entities. Already a wide selection of the commercial products is available on the market: F-Secure SENSE [20], Luma smart Wi-Fi router [21], Dojo [22], CUJO [23], Bitdefender [24], Norton Core [25].

3 The GHOST System

The GHOST system is being realised by analysing existing technical infrastructure and existing software components corresponding to the aims of the project. Usability studies have been defined with the aim to establish mental models of the end users. This allows systematical and effective addressing of the human factor with the aim to facilitate end-users proper decision making in relation to security and privacy issues and adequate usage of the GHOST solution. It also allows the definition of a first set of end-user requirements, which in turn facilitate better specification of the development and integration of core technologies. Since human participants will be involved in the evaluation phase of the project and personal data will be collected, special emphasis is given on elaborating a data management plan for respecting privacy according to national and EU legislation. It should be noted that the access to the collected data will only be provided only to members of the consortium for development and demonstration purposes.

To keep up with cyber-security issues and threats GHOST follows guidance documents, best practices and standards (issued by international, European and national stakeholders) at all stages of design and development, and also scans for emerging threats/issues. To this end, it makes use of security intelligence available within the consortium and outside (e.g. through mining insightful security blogs), as well as related information collected directly from the end-users and the smart home pilots. The development of GHOST follows an iterative approach. Three iterations have been specified for the implementation of the technical components of the infrastructure. These will be evaluated through real life trials and feedback will be reflected back for further refinement and acceptance, according to the validation process discussed in Section 4.

3.1 GHOST Software Architecture

GHOST's conceptual design involves advanced data flow analysis on a packet basis to build the context of communication. From this context, data are classified into user and device profiles, which in turn are used in the automated real-time risk assessment. The assessment is based on evaluation, comparison and matching with safe data flow patterns, utilising a self-learning approach. Data analytics and visualisation techniques are deployed to ensure enhanced user awareness and understanding of the security status, potential threats, risks, associated impacts and mitigation guidelines.

The architecture of the GHOST system, shown in Figure 1, follows a layered approach that allows independent development of the separate components, while preserving a high interdependency within the framework. A brief outline of each layer and its main functionality is presented in this subsection.

Core Layers **Data Interception and Inspection (DII)** Data related to traffic of all network interfaces in a smart home environment is gathered directly from the network. This data is analysed and stored in order to be used by GHOST components. Significant data extracted from traffic packets is stored to a shared data storage. Additionally traffic packets are aggregated into groups related to specific communications or actions. These groups of packets

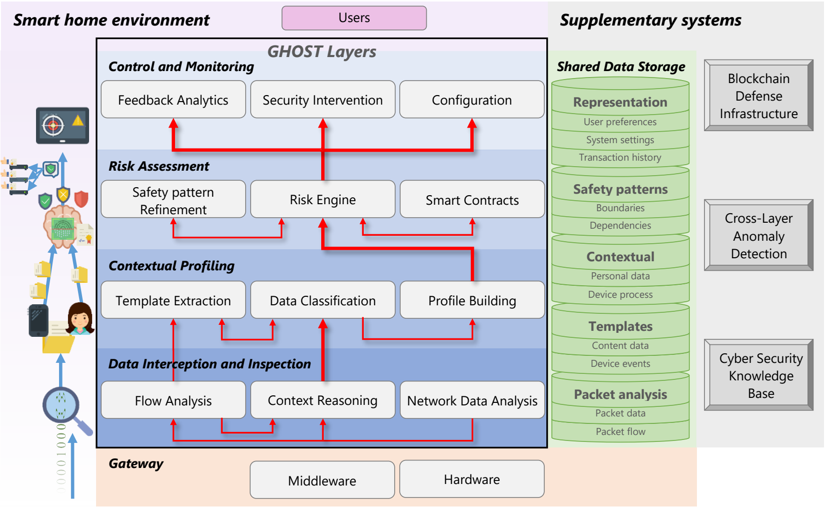

Fig. 1: GHOST architecture

are also analysed to extract information of a higher abstraction level and store it along with the information produced by single packets analysis. Additionally context information is extracted from traffic data. Recurring patterns of traffic are detected and the causes they are produced by are identified and an initial classification of the data type of traffic is performed. The network traffic may be correlated to actions of people or events in the smart home and the data in the packets are categorised accordingly as personal data or device data.

Contextual Profiling (CP) The classification templates and actual profiles of the typical devices' behaviour are built in this layer, by extracting valuable data from the local network communication already prepared by DII profiles for the normal behaviour of the devices are built in a tree based format for further processing by the risk assessment component. This layer also monitors the communications occurring between any combination of devices including the gateway, along with the status of each device and the status of the gateway. Monitoring is learning based, and models are trained to recognise the normal status of devices and the normal status of communication between them. Random Neural Networks are employed for each pair of devices and reinforcement learning is used to update them through time.

Risk Assessment (RA) This a core layer, which gathers information about the current risks and analyses in real-time current network traffic flows. It correlates device activity on the network with the profiles available from CP layer. The automatic decision making of the Risk Engine presents transparency of the cyber security solution, informing the end-user only about urgent decisions. Its capabilities is enhanced with the use of Smart Contracts (SC) to ensure the reliability and trustworthiness of decisions. RA is also designed for controlling users privacy and making them aware of the associated risks.

Control and Monitoring (CM) Three types of the user interfaces are forming this layer: Feedback Analytics (advanced professional-alike interfaces, Security Intervention (daily decision-making support tooling) and Configuration. The input data include historical and current packet flow behaviours, risk levels, device profiles, packet classification score, etc. The layer provides visual and intuitive presentations and reports of the smart home security status, including visualisations of packet features through time, visual monitoring and distinction of packet behaviours, and visual identification of potential anomalies and vulnerabilities. The appropriate visualisation and human-machine interaction mechanisms are put in place to allow users to effortlessly and effectively review security issues and take key decisions that affect their privacy and security.

3.2 Supplementary Features

Other features and software concerning the proposed GHOST system are listed below. **Blockchain Defense Infrastructure (BDI)** GHOST uses blockchain technology and SC for ensuring data and code integrity. At this layer the decisions made by RA are verified according to commonly agreed SC, turning the decision making into a truly decentralised and resilient system against intrusions. The integrity of the code running on smart home gateways can be certified by the use of blockchain technology. Additionally valuable security related information can be stored at a blockchain infrastructure in order to be shared between smart home gateways.

Cross Layer Anomaly Detection Framework (CLADF) Cross layer anomaly detection framework integrates existing open source solutions for traditional cyber security features. The main purpose is to collect, correlate, combine, and provide a unified output to other components in terms of possible events that require further analysis.

Cyber Security Knowledge Base (CSKB) A common cloud based knowledge repository is integrated with GHOST to collect anonymised security intelligence and insights from external web-sources to enhance the automatic decision making and improve end-user visual experience within the CM layer. It will maintain list of malicious actors and properties (IP Addresses, Domains, URLs, File Hashes).

Shared Data Storage (SDS) The data structures defined by each of the components are normalised and unified within a single storage framework. A combination of relational and non-relational databases is used to satisfy the needs of all components. There is distinction between local and cloud based storage, as some components will perform off-site analytics.

3.3 GHOST Hardware Platforms

GHOST is based on the existence of a communication gateway with network monitoring capabilities, in which GHOST modules capture and analyse the different traffic patterns by devices and users. This gateway is a trustable and secure-by-design device as far as it is located inside the home network and it has two main responsibilities: (1) to provide connectivity capabilities for the devices inside the network, (2) to run the different algorithms and mechanisms for ensuring the security and privacy of the user data. Having these in mind, this element of the GHOST solution must accomplish market requirements related with size, weight and objective cost, among others. Therefore, it is needed to find a trade-off between the different features and capabilities of the gateway, resulting in a device that can be defined as constrained node [26]. The main restrictions that a constrained device can have are the following:

- maximum code complexity and size,
- size of the memory of the system,
- processing power that the device can offer in a certain period of time,
- allowed energy consumption or battery duration,
- communication methods and interfaces of the system,
- user interfaces and accessibility to the system in deployment.

Several techniques has been proposed in the literature to keep these set of constraints controlled in different environments and specific solutions [27,28,29], including the for security and privacy applications [30,31].

GHOST is being developed and tested using two resource-constrained platforms: a proprietary IoT gateway, and a Raspberry Pi (with some expansion modules for IoT networks). The use of both devices allows several different IoT protocols, such as 802.11, Bluetooth Low Energy, Z-Wave and 802.15.4 to run on GHOST. Differences do exist between these two devices, but there are also some similarities regarding their constraints as regards processing power; memory; communications; and energy efficiency. These constraints pose a number of research challenges.

4 GHOST Validation Process

The validation strategy defined for GHOST is based on a three-fold vision that combines a complete set of robustness and laboratory testing; the specific definition of realistic testbeds; and real-life trials or pilots. First, the laboratory testing will be done with the objectives of reducing the number of possible bugs and functional errors and of checking the stability of the hardware. Therefore, unit tests will be performed over each specific GHOST module and an acceptance test plan will be defined and tested, including both software and hardware stability testing. After this first stage, two already functional testbeds will be used to deeply test the functionality of the GHOST solution in a controlled environment.The testbeds designed for two specific smart home demonstrators include more than 15 different types of devices, involving up to 25 devices that will be simultaneously connected and monitored by the GHOST suite. In order to have a broad view of the possible services and solutions, devices like smart locks, biomedical devices, companion robots or smart lights based on several communication solutions (like 802.11, 802.15.4, Z-Wave or Bluetooth

Low Energy) have been included in the testbeds. Potential threats against the smart home can be categorised into [32]: (i) Physical attacks, (ii) Unintentional damage (accidental), (iii) Disaster (natural/environmental), (iv) Damages or loss of IT assets, (v) Failures/malfunctions, (vi) Outages, (vii) Eavesdropping / interception / hijacking, (viii) Nefarious activity/abuse, and (ix) Legal. Of these, relevant to GHOST are groups (ii), (iv), (vii), and (viii). Each of these groups includes a number of threats that can exploit relevant vulnerabilities by launching different attacks. The response of GHOST when faced with those amongst the above attacks that lead to higher risks and/or are most prevalent will be assessed in the controlled environment of the GHOST testbeds.

In addition to the testbeds, a set of pilots in real scenarios (homes of end-users) in three different countries (Spain, Romania and Norway) and with complementary use cases related with telecare, eHealth, home security and home automation will be carried out. The real-life trials have been designed to cover a varied set of application and services. Four different use cases have been defined: Ambient assisted living in smart homes for older people in Galicia, Spain; Continuous health monitoring for adult people in Galicia, Spain; Regular private homes (smart-home solutions) in Norway and Regular private homes (smart-home solutions) in Romania.

Each use case has their own set of devices to be installed and a complete test plan is being developed to simulate the possible results of specific attacks (previously validated and performed in the testbeds) to capture the response of the users to the GHOST behaviour.

5 Conclusions

GHOST brings professional security tools down to regular home users. The strategic outcome of GHOST is threefold: increased resilience of existing cyber security solutions for smart homes and the IoT; a leap forward to usability and automation in cyber security; and a boost in the competitiveness of European ICT security industry in the advent of the IoT in the connected world. From a user perspective, GHOST will help end-users to increase their control over their smart-home IoT devices and it will provide an option for smart-living service providers to use its security services to ensure that they respect the security and privacy needs of their clients. Future work will includes the iterative implementation, testing and validation of GHOST in laboratory testbeds and real-life and scale pilots in three European countries, using appropriate use case scenarios.

Acknowledgements

This work is partially funded by the European Union's Horizon 2020 Research and Innovation Programme through the GHOST project (https://www.ghost-iot.eu/) under Grant Agreement No. 740923. The contents of this paper do not engage the responsibility of the European Commission.

References

1. Chandrasekar, K., Cleary, G., Cox, O., Lau, H., Nahorney, B., O Gorman, B., O'Brien, D., Wallace, S., Wood, P., Wueest, C.: ISTR April 2017. Internet Security Threat Report - Symantec **22** (April 2017) 77
2. Nurse, J.R., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: Past and present. Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011 (2011) 21–26
3. Realpe, P.C., Collazos, C.A., Hurtado, J., Granollers, A.: Towards an integration of usability and security for user authentication. In: Proceedings of the XVI International Conference on Human Computer Interaction, ACM (2015) 43
4. August, T., August, R., Shin, H.: Designing user incentives for cybersecurity. Communications of the ACM **57**(11) (oct 2014) 43–46
5. Roesch, M.: Snort: Lightweight Intrusion Detection for Networks. LISA '99: 13th Systems Administration Conference (1999) 229–238
6. (OISF), O.I.S.F.: Suricata
7. Paxson, V.: Bro: a system for detecting network intruders in real-time. Computer Networks **31**(23-24) (1999) 2435–2463
8. Marchal, S., Jiang, X., State, R., Engel, T.: A big data architecture for large scale security monitoring. Proceedings - 2014 IEEE International Congress on Big Data, BigData Congress 2014 (2014) 56–63
9. Koike, H., Ohno, K., Koizumi, K.: Visualizing cyber attacks using IP matrix. IEEE Workshop on Visualization for Computer Security 2005, VizSEC 05, Proceedings (2005) 91–98
10. Xie, P.X.P., Li, J.H., Ou, X.O.X., Liu, P.L.P., Levy, R.: Using Bayesian networks for cyber security analysis. Dependable Systems and Networks DSN 2010 IEEEIFIP International Conference on (2010) 211–220
11. Jibao, L., Huiqiang, W., Liang, Z.: Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory. 2006 International Conference on Computational Intelligence and Security **Vol. 2** (2006) 1545–1548
12. Jakobson, G.: Mission cyber security situation assessment using impact dependency graphs. In: 14th International Conference on Information Fusion. (July 2011) 1–8
13. Tweneboah-Koduah, S., Skouby, K.E., Tadayoni, R.: Cyber Security Threats to IoT Applications and Service Domains. Wireless Personal Communications **95**(1) (2017) 169–185
14. Pamukov, M.E.: Application of artificial immune systems for the creation of IoT intrusion detection systems. In: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IEEE (sep 2017) 564–568
15. Chen, C.Y., Hasan, M., Mohan, S.: Securing Real-Time Internet-of-Things. arXiv preprint arXiv:1705.08489 (may 2017) 1–10
16. Zegzhda, P.: Safe Integration of SIEM Systems with Internet of Things : Data Aggregation , Integrity Control , and Bioinspired Safe Routing. Proceedings of the 9th International Conference on Security of Information and Networks SIN '16 (2016) 81–87
17. Lin, H., Bergmann, N.W.: IoT Privacy and Security Challenges for Smart Home Environments. Information **7**(3) (2016) 44
18. Pacheco, J., Hariri, S.: IoT Security Framework for Smart Cyber Infrastructures. In: 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), IEEE (sep 2016) 242–247

19. Park, Y., Daftari, S., Inamdar, P., Salavi, S., Savanand, A., Kim, Y.: IoTGuard: Scalable and agile safeguards for Internet of Things. Proceedings - IEEE Military Communications Conference MILCOM (2016) 61–66
20. F-Secure: F-secure sense router. https://www.f-secure.com/en/web/home_global/sense
21. Inc., L.H.: Luma. https://lumahome.com/
22. BullGuard: Dojo by bullguard. https://dojo.bullguard.com/
23. CUJO: Cujo llc. https://www.getcujo.com/
24. 2, B.B.: Bitdefender. https://www.bitdefender.com/box/
25. Core^{TM}, N.: Symantec corporation. https://us.norton.com/core
26. Bormann, C., Ersue, M., Keranen, A.: Terminology for Constrained-Node Networks. Technical report, Internet Engineering Task Force (IETF) (may 2014)
27. Mittal, S.: A survey of techniques for improving energy efficiency in embedded computing systems. International Journal of Computer Aided Engineering and Technology **6**(4) (2014) 440
28. Sheng, Z., Wang, H., Yin, C., Hu, X., Yang, S., Leung, V.C.M.: Lightweight Management of Resource-Constrained Sensor Devices in Internet of Things. IEEE Internet of Things Journal **2**(5) (oct 2015) 402–411
29. Wang, H., Xiong, D., Wang, P., Liu, Y.: A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices. IEEE Access (2017)
30. Sethi, M., Kortoci, P., Di Francesco, M., Aura, T.: Secure and low-power authentication for resource-constrained devices. In: 2015 5th International Conference on the Internet of Things (IOT), IEEE (oct 2015) 30–36
31. Porambage, P., Braeken, A., Gurtov, A., Ylianttila, M., Spinsante, S.: Secure end-to-end communication for constrained devices in IoT-enabled Ambient Assisted Living systems. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE (dec 2015) 711–714
32. Barnard-Wills, D., Marinos, L., Portesi, S.: Threat Landscape and Good Practice Guide for Smart Home and Converged Media. Technical report, ENISA (2014)
33. Kouzinopoulos, C.S., Spathoulas, G., Giannoutakis, K.M., Votis, K., Pandey, P., Tzovaras, D., Katsikas, S.K., Collen, A., Nijdam, N.A.: Using blockchains to strengthen the security of internet of things. In Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D., eds.: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London, Lecture Notes CCIS No. 821, Springer Verlag (2018)
34. Gelenbe, E., Kadioglu, Y.M.: Energy life-time of wireless nodes with network attacks. In Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D., eds.: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London, Lecture Notes CCIS No. 821, Springer Verlag (2018)
35. Brun, O., Yin, Y., Gelenbe, E., Augusto-Gonzalez, J., Ramos, M.: Iot attack detection with deep learning. In Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D., eds.: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London, Lecture Notes CCIS No. 821, Springer Verlag (2018)
36. Brun, O., Yin, Y., Gelenbe, E., Kadioglu, Y.M., Augusto-Gonzalez, J., Ramos, M.: Deep learning with dense random neural network for detecting attacks against iot-connected home environments. In: Submitted for Publication. (2018)