Figueiredo, S., Silva, P., Iacovazzi, A., Holubenko, V., Casal, J., Calero, J. M. A., Wang, Q., Colarejo, P., Armitt, R. L., Inches, G., & Raza, S. (2023). ARCADIAN-IoT - enabling autonomous trust, security and privacy management for IoT. In A. González-Vidal, A. Mohamed Abdelgawad, E. Sabir, S. Ziegler, & L. Ladid (Eds.), *Internet of Things - 5th The Global IoT Summit, GIoTS 2022, Revised Selected Papers* (pp. 348-359). (Lecture Notes in Computer Science; Vol. 13533). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-20936-9_28

This is a post-peer-review, pre-copyedit version of a chapter accepted for publication in *Internet of Things - 5th The Global IoT Summit, GIoTS 2022, Revised Selected Papers* on 24/05/2022.

ARCADIAN-IoT - Enabling Autonomous Trust, Security and Privacy Management for IoT*

Sérgio Figueiredo[1], Paulo Silva[1,2], Alfonso Iacovazzi[3], Vitalina Holubenko[1], João Casal[4], Jose M Alcaraz Calero[5], Qi Wang[5], Pedro Colarejo[6], Ross Little Armitt[7], Giacomo Inches[8], and Shahid Raza[3]

[1] Instituto Pedro Nunes, Portugal
sfigueiredo@ipn.pt
[2] University of Coimbra, Centre for Informatics and Systems of the University of Coimbra (CISUC), Portugal
[3] RISE Research Institutes of Sweden, Sweden
[4] SCNL Truphone S.A., Portugal
[5] University of the West of Scotland, UK
[6] LOAD Interactive, Portugal
[7] ATOS, Spain
[8] Martel Innovate, Switzerland

Abstract. Cybersecurity incidents have been growing both in number and associated impact, as a result from society's increased dependency in information and communication technologies - accelerated by the recent pandemic. In particular, IoT. technologies, which enable significant flexibility and cost-efficiency, but are also associated to more relaxed security mechanisms, have been quickly adopted across all sectors of the society, including critical infrastructures (e.g. smart grids) and services (e.g. eHealth). Gaps such as high dependence on 3rd party IT suppliers and device manufacturers increase the importance of trustworthy and secure solutions for future digital services.
This paper presents ARCADIAN-IoT, a framework aimed at holistically enabling trust, security, privacy and recovery in IoT systems, and enabling a Chain of Trust between the different IoT entities (persons, objects and services). It builds on features such as federated AI for effective and privacy-preserving cybersecurity, distributed ledger technologies for decentralized management of trust, or transparent, user-controllable and decentralized privacy.

Keywords: ARCADIAN-IoT · Cybersecurity · Trust · IoT.

1 Introduction

The increased penetration of Internet of Things (IoT) technologies, devices and services has, along with other technologies such as cellular networks or AI, a

* This work was carried out in the scope of the ARCADIAN-IoT - Autonomous Trust, Security and Privacy Management Framework for IoT, Grant Agreement Number: 101020259. H2020-SU-DS02-2020.

profound impact in society. Thus, the potential threats associated with IoT and the need to reduce risks are important cybersecurity topics. IoT-related cyber-attacks spiralled in 2021, showing the pandemic has aggravated IoT-based vulnerabilities (e.g. with prolonged multi-device usage in household settings). Recent projections estimate 75.44 billion connected devices will be deployed by 2025, supporting sectors such as education, transport, energy, health and security, which emphasizes how threats and risks associated with IoT devices and systems can have huge consequences on both cyber and physical domains. As the number of IoT devices and the data shared between them grows, so does the number of attacks and vulnerabilities associated with them. A report by Gartner estimates over 25% of cyber-attacks against businesses will be IoT-based by 2025 [1]. Attacks like Mirai [2] highlight that weak security measures in the development, adoption and usage of IoT devices can have a tremendous impact - for instance, attackers can orchestrate a large set of devices to launch Distributed Denial of Service (DDoS).

IoT devices and applications have an increased risk of becoming victims of cyber-attacks due to a lack of security measures in the IoT ecosystem, exposing IoT devices to malicious attacks that leave them vulnerable. This results e.g. from the lack of computational capacity for efficient built-in security mechanisms, limited budget for properly testing and improving firmware security, lack of regular updates due to limited budgets and technical limitations of IoT devices, or discontinued updates, restricting vulnerability patching (e.g. resulting in lack of encryption integrated in end-to-end communications between IoT devices).

Other technological advances (e.g. 5G or AI) will tend to further intensify cybersecurity issues, in particular in SMEs, where skills for managing the security of business-critical IoT systems are limited. The increased dependency on third party IT suppliers (e.g., cloud providers), and IoT device manufacturers puts in evidence the need for trustworthy and secure solutions for future (and current) digital services powered by IoT systems. New attack surfaces are introduced by the evolving IoT ecosystem, caused by the interdependent and interconnected IoT systems, which results in added complexity and challenging security maintenance. IoT devices mostly work in an unattended environment, where an intruder may physically access these devices easily, and are wirelessly connected, where an intruder may access private information from a communication channel through eavesdropping.

The dependency on the aforementioned technologies, the growing complexity of cyberattacks, and the rise in incidents (e.g. ransomware, loss of data, disruption to public or critical services) exposes the need for designing and implementing effective cybersecurity mechanisms spanning threat prevention, detection and mitigation. In order to ensure that the transformation brought by IoT will benefit all citizens in a way that warrants security and privacy, the definition and development of innovative and advanced security and privacy management mechanisms and technologies that can seamlessly be integrated across different sectors and use cases are required.

This paper presents ARCADIAN-IoT, a framework for enabling decentralized management of trust, identity, privacy and security in IoT systems considering persons, objects and services. ARCADIAN-IoT intends to enable security and trust in the management of object's and persons identification, establish a Chain of Trust through distributed and autonomous models for trust, security and privacy, and provide self and coordinated recovery and healing upon threat detection.

The paper is organized as follows: Section 2 describes related work on cybersecurity for IoT; the ARCADIAN-IoT framework, its planes and main functionalities are described in Section 3; Section 4 presents three distinct use cases which demonstrate the framework intended benefits; finally, Section 5 concludes the paper and lists future work.

2 Related Work

Cybersecurity in IoT systems has been extensively studied during last decades and several surveys on the achievements, challenges, and open issues in this area have been produced [12, 11, 6]. As highlighted by Lu et al. [12], IoT systems are susceptible to various security attacks at different levels, and for this reason, most of the measures deal with cyber attacks and protection with layer-level perspectives: "sensing," "network," "middleware," and "application" layers.

Protection of end-nodes/sensors is generally obtained at the sensing layer by providing lightweight tools directly embedded (built-in) into the end-devices for encryption, access control, and node authentication [17, 4]. Tiburski et al. defined a security architecture that integrates trust mechanisms with embedded virtualization providing security from hardware to applications [15]. Instead, a lightweight and hybrid system merging Physically Unclonable Functions (PUFs), Arbiter, and Read-Only PUFs was proposed by Sankaran et al. [13].

Cybersecurity at the network layer aims to monitor and protect IoT communications by means of firewalls and Network Intrusion Detection/Prevention Systems (NIDS/NIPSs) [19]. Although lightweight NIDSs can quickly process the huge amount of traffic in IoT networks (e.g., the solution proposed by Jan et al. [9]), the hybrid systems that rely on both pattern matching and deep learning models are more suitable for detecting the more recent and advanced cyber attacks targeting IoT [14, 10].

The middleware layer, which is often affected by security and privacy issues, offers an important perspective for cyber protection [8, 7]. For example, Da Cruz et al. suggest a reference model for designing IoT middleware platforms based on modules that reflect main IoT requirements: (i) interoperability, (ii) persistence and analytics, (iii) context, (iv) resource and event, (v) security, and (vi) graphical user interface [7].

Finally, cybersecurity at the application layer explores those threats, and corresponding mitigation mechanisms, that relate to the system functionalities and services for the final users [16]. Given the significant amount of use cases and applications in IoT, the state of the art shows a proliferation of domain-

specific cybersecurity solutions. An example of a cybersecurity tool for healthcare ecosystem is the architecture proposed by Abie [3]; on the other side Bringhenti et al. provided a personalized cybersecurity approach for smart homes [5], and Vijayakumaran et al. built an architecture for smart industry [18].

3 ARCADIAN-IoT framework

3.1 Overview

The concept of ARCADIAN-IoT represents an integrated approach to manage identity, trust, privacy, security and recovery of IoT devices, persons and services. It relies on specialised components laid out on vertical and horizontal planes (described in Sections 3.2 and 3.3) to address those aspects. The vertical planes cover identity, trust and recovery management. The horizontal planes are in charge of managing privacy and security across the framework.

Figure 1 depicts ARCADIAN-IoT Concept, its horizontal and vertical planes, as well as the components that support the framework. The different entities (i.e., persons, IoT devices and apps/services) covered by ARCADIAN-IoT enable a way to interact with IoT systems and its operations (e.g., data collection, data processing, or data transmission) in a safe, secure and privacy-preserving manner.

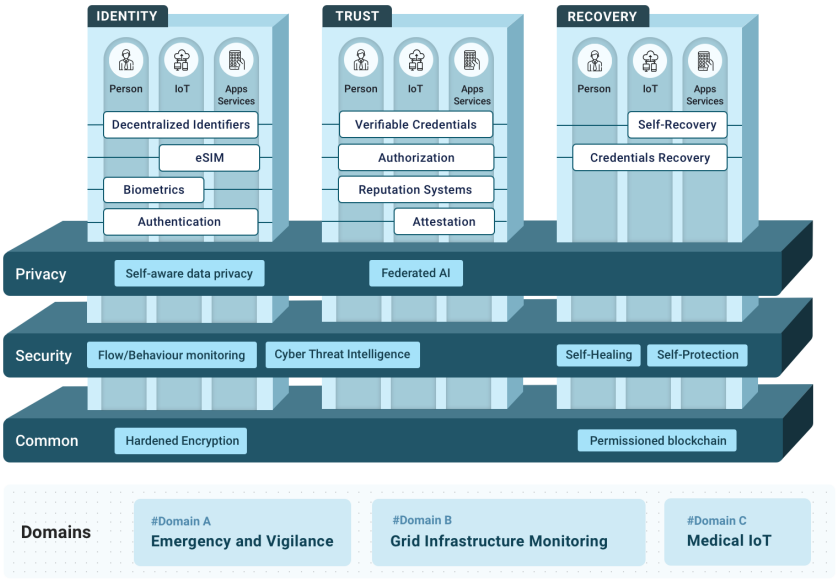

Fig. 1. ARCADIAN-IoT conceptual representation.

The main objective of ARCADIAN-IoT is to enable a holistic framework with components leveraging Federated AI, Distributed Ledger Technologies (DLT), functional encryption, eSIM technologies, Cyber Threat Intelligence (CTI), and several other approaches for autonomous trust, security and privacy management for IoT systems. There are six specific objectives to achieve with the development of ARCADIAN-IoT framework:

1. Enable security and trust in the management of objects' identification.
2. Enable distributed security and trust in management of persons' identification.
3. Provide distributed and autonomous models for trust, security and privacy – enabling a Chain of Trust.
4. Provide hardened encryption with recovery ability.
5. Self and coordinated healing with reduced human intervention.
6. Enable proactive information sharing for trustable CTI and IoT Security Observatory.

3.2 Horizontal Planes

The Privacy Plane aims to provide functionalities for the privacy-preserving management of confidential or sensitive data involving persons' entities, and includes the (i) Self-aware Data Privacy and (ii) Federated AI components. The Self-aware Data Privacy component will enhance the way data privacy is managed by allowing the user to define privacy policies for data, and by crowdsourcing policies specified on similar data. The Federated AI component will provide dependable and privacy preserving federated learning (FL) capabilities to the machine learning (ML)-based components.

The Security Plane contains all the cyber security features required for the monitoring, prevention, management, and recovery; it comprises the (i) Network Flow Monitoring, (ii) Behaviour Monitoring, (iii) CTI, (iv) Network Self-protection, (v) IoT Device Self-protection, and (vi) Network Self-healing components. The Network Flow Monitoring will enhance existing NIDSs to get advanced detection along the entire infrastructure of the IoT network, while the Behavior Monitoring component aims at detecting anomalous behaviours occurring on IoT devices. The CTI system focuses on IoT threats and it will enhance the open source MISP[9] platform with IoT-specific functionalities for automated gathering, producing, elaborating, and sharing cyber threat data. A set of protection policies and rules aiming to safeguard the network infrastructure, IoT devices, and services are enforced (i) at network level by the Network Self-protection component and (ii) locally on IoT devices by the IoT Device Self-protection component. Finally, the Network Self-healing component is designed to mitigate the potential impact of a cyber attacks when there is no protection rule for that specific attack, thus with the potential to penetrate the IoT infrastructure.

[9] https://www.misp-project.org/

The Common Plane includes the two components that provide functionalities that will reinforce other components in both Horizontal and Vertical Planes, i.e., (i) the Hardened Encryption and (ii) Permissioned Blockchain. The Hardened Encryption component aims at providing encryption mechanisms that are more flexible, decentralized, and hardened by an hardware-based Root of Trust (RoT) which can be provided by: (i) the eSIM component, (ii) the crypto chip embedded in the IoT device, or (iii) an independent/external crypto chip module integrated as add-on module by the vendor into existing IoT device. Finally, the framework will provide a Permissioned Blockchain to (i) anchor the trust for decentralized identifiers, (ii) publish and share information in a trusted and immutable fashion with different actors in the IoT ecosystem, and (iii) support the deletion of personal data by the users.

3.3 Vertical Planes

The Identity Plane supports (i) a multi-factor Authentication component that calls upon other components to realise the required authentication as needed for the different use cases, (ii) a Decentralized Identifier component, (iii) an eSIM – Hardware-based Identity and Authentication component, and (iv) a Biometrics authentication component. The Decentralized Identifier (DID) component follows the W3C DID Core Specification[10] to support the Self-Sovereign Identity approach with support for both public and privacy preserving DIDs and supports the Verifiable Credentials in the Trust Plane through cryptographic keys associated with a DID. Proving ownership of a DID itself by cryptographic means also authenticates the user, thing or system as holder of the private key, which can serve to authenticate constrained devices that may not be able to support the whole SSI stack with Verifiable Credentials. The Decentralized Identifier component will make use of the blockchain in the horizontal plane for anchoring the trust in public DIDs that are published in Content Addressable Storage (CAS) off-chain. The eSIM component in the context of identity, will act as a Secure Element (SE) capable of storing identity and authentication credentials at devices hardware level, and use them in network-based authentication with a novel method to authenticate an eSIM-equipped device in a third-party service by leveraging cellular authentication, whose credentials and processes are securely stored at hardware level in the device eUICC. The Biometrics authentication component adds a third factor to identify persons, and will support AI/ML facial matching algorithms to match live video feed against a set of photos for particular persons and in challenging operational conditions (e.g. distance, angle between camera and individual, lighting conditions).

The Trust Plane supports (i) Verifiable Credentials component, (ii) Network-based Authorization component, (iii) Reputation System component and (iv) Remote Attestation component. The Verifiable Credentials component follows

[10] https://www.w3.org/TR/did-core/

the W3C Verifiable Credential Specification[11] and enables trusted identification of users and things through these entities being issued with claims inside a Verifiable Credential (VC) and later being able to present it with secure cryptographic proofs, supported by Decentralized Identifiers in the identity plane. The Network-based Authorization component leverages network-based policy enforcement tools, to enable novel processes of dynamic authorization throughout ARCADIAN-IoT ecosystems with respect to the entities' current trustworthiness (provided by the Reputation System). The latter component dynamically determines the current reputation score of persons, devices and services, where the score is continually updated based on data received from other entities regarding its interactions and represents its current trust level. To enable 3rd party actors that need access to this information in a trusted and distributed manner, the reputation score will be anchored on the blockchain while the actual score is stored off-chain in distributed storage. The Remote Attestation component supports support hardware-based attestation with the ability to leverage Root-of-Trust using a secure element (e.g. eSIM or crypto chip) and aligns with the standardisation effort of the IETF Remote Attestation Procedures (RATS)[12] working group, with respect to standardized formats for describing claims and associated evidence, and procedures to deliver these claims.

The Recovery Plane supports (i) Self-recovery component and (ii) Credentials Recovery component. The Self-recovery component provides a storage server solution, that enable devices to securely store and retrieve backups making use of the ARCADIAN-IoT framework´s Authentication and Hardened Encryption components. It supports data to be encrypted in a selective way, by applying a policy that defines which stakeholders, relying on their public keys, can decrypt the data either partially or completely. The Credential Recovery component provides for the scenario where a user´s device or IoT device´s data was somehow corrupted or wiped and the user or device respectively requests a recovery of credentials and data.

4 Reference Use Cases

ARCADIAN-IoT research is supported by reference use cases from three domains, where concrete IoT solutions allow to better understand requirements, and validate the framework and its components. The selected domains are considerably different to ensure a broad view over the needs of IoT security, trust and privacy management, towards the intended holistic approach of the framework. In the next subsections, are briefly presented the IoT solutions of the three domains, making visible the needs that motivate the project. In 4.4 is provided a summary of the IoT security, trust and privacy management challenges that are common to the presented solutions.

[11] https://www.w3.org/TR/vc-data-model/
[12] https://www.ietf.org/mailman/listinfo/rats

4.1 Domain A: Emergency and vigilance using drones

Ensuring security and safety of citizens in urban environments is a complex subject that depends on the availability of considerable resources and, in many cases, the use and manipulation of sensitive data (e.g., when using street vigilance cameras). ARCADIAN-IoT domain A focuses on the use of IoT devices, in this case, drones, in novel citizen centered urban vigilance services.

Fig. 2. Drone Guardian Angel solution

The solution (see Fig. 2) consists of a mobile app where citizens can request a Drone Guardian Angel (DGA) service, e.g., to escort them in their way home. The user needs to supply personal data in the registration phase, like name, address and photos, and, when requesting the service, needs to provide its initial and final location, to ensure that the service is available in both places.

When receiving a service request with a person's data, a drone parked nearby goes to the requested location and identifies the user (e.g., by face recognition). After the identification the service starts and the drone follows the person, aware of the surroundings to detect any threat. If something abnormal is detected (e.g., an attempt of robbery), the drone calls for rescue services according to the incident type (e.g. police in case of robbery, and/or medical emergency in case injuries exist). While the rescue team(s) is/are on its/their way, some details are sent, collected by the drone camera, microphone or other appropriate sensors (e.g., GPS), to optimize the response to the incident.

DGA solution depends on the use of persons sensitive data, like location and photos. Compromised devices can endanger the users safety and their data security. The service itself depends on the trustworthiness of the data gathered and provided by IoT devices. Also, the IoT network, if vulnerable, may endanger the users security and safety (especially in emergency moments). These and other trust, security, and privacy management challenges are summarized in 4.4.

4.2 Domain B: Grid infrastructure monitoring

Grid infrastructures are the base for power utilities like electricity, gas or oil. These are critical services for most of the daily urban activities. Monitoring

these infrastructures has high importance for providing reliable services and for efficient energy management practices.

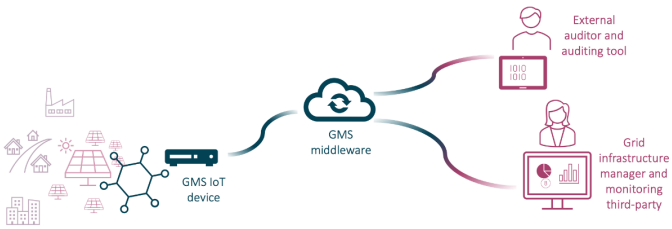

Fig. 3. Grid Monitoring Services solution

ARCADIAN-IoT domain B features an IoT solution for monitoring grid infrastructures (see Fig. 3). Typically, a grid infrastructure manager needs to be aware of factors that influence the system behaviour, like component degradation, and of aspects that allow to optimize and predict the service performance (e.g. temperature). In this sense, the Grid Monitoring Services (GMS) consist of a solution that collects and aggregates data from a set of sensors using an IoT device that acts as gateway for communication. This IoT device makes the grid data available, through a middleware, to be consumed by grid managers in a monitoring service (e.g., web). GMS also allows a grid manager to change the sensors procedures (e.g., change the reading cycle frequency). Finally, the solution is prepared for external audits, where data from devices/sensors needs to be securely provided to authorized external persons.

GMS solution collects data from a set of devices that inform about grid performance and related factors. The trustworthiness of the data is critical. If corrupted, the system or the manager are prone to have wrong decisions, putting at risk energetic needs of businesses and citizens. It is also confidential data, that can harm the service provider in case of unauthorized access. Furthermore, GMS provides means to interact with the sensor network, action that may compromise the infrastructure performance. The monitoring tool can also be targeted in network attacks, e.g., DDoS, making the service unavailable and delaying/hampering potentially relevant decisions. In 4.4, these and other trust, security, and privacy management challenges relevant for GMS are summarized.

4.3 Domain C: Medical IoT for remote monitoring of patients

Monitoring patients at their homes, when possible, is important for the sustainability of health systems, and for the comfort of the monitored persons. IoT systems, namely body sensor networks, provide solutions that make this possible.

ARCADIAN-IoT Medical IoT (MIoT) solution (see Fig. 4) focuses on this opportunity, making possible to reduce the number of medical appointments

from patients that need to be accompanied. MIoT is able of monitoring patients health considering a treatment protocol (readings frequency, medication, and other medical recommendations). It collects, stores, and presents the evolution of the patient vital signs, captured with medical sensors, and timely provides alerts for medical decision support. To complement these parameters, the patient can enter perceived health status in a mobile app, adding symptoms that can describe the his/her condition. The solution relies in a MIoT kit, provided to the patient at the hospital, that comprises a set of medical sensors and a smartphone that is used as gateway for the sensing devices' communication to the Cloud, and as interface for the patient to enter his/her perceived condition. The solution also includes a middleware for storing the patients' data, to provide it to medical monitoring tools, and for generating health alerts; and a monitoring tool for the medical staff to check the patient's condition and to change the monitoring protocol when needed.

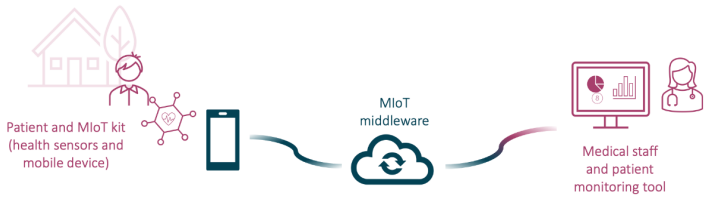

Fig. 4. Medical IoT solution

ARCADIAN-IoT MIoT solution aims to improve the conditions of follow-up of patients at home, in an active treatment process. However, by collecting patient's data and storing it in a centralized Cloud, the system deals with sensitive information security and privacy risks. Also, the trustworthiness of the data is critical for the medical staff to make right treatment decisions. Fake or manipulated diagnostic information can put the patients' well-being, or even their lives, at risk. Furthermore, MIoT provides means to update the patient monitoring protocol, which needs to be secured to avoid unauthorized control over the devices' behaviour. The mobile app and the monitoring tool for the medical staff can also be targeted in attacks that can make the services unavailable and delay/hamper potentially relevant medical decisions. These challenges and others relevant to this domain are consolidated in the next subsection.

4.4 Common trust, security and privacy management challenges

The IoT solutions aforementioned share trust, security and privacy management challenges, namely the following:

- Enable security and trust in the management of devices' and persons' identification, ensuring protection to, e.g., impersonation attacks that could endanger persons safety and data security.
- Define trust evaluation models and processes for devices, persons and services, that can trigger and support protection measures, and also keep the user in control his data privacy (who accesses what and when).
- Protect the users' and devices' sensitive data with hardened encryption mechanisms that have recovery ability in case of need.
- Detect anomalous behaviour on IoT devices, IoT network and related services, which can indicate the presence of known or zero-day vulnerabilities or threats.
- In case of an incident with a device, have self-protection, self-recovery and self-healing mechanisms that allow to protect and to recover functionalities and data to pre-defined trust levels with reduced human intervention.
- Have a CTI approach for IoT threat information generation, sharing, analysis, storage, and consumption, able of spreading and using threat knowledge in a efficient way.

ARCADIAN-IoT research aims to provide answers to these challenges. The hypothesis are formulated jointly with the IoT technology providers to ensure viability, and integrated for validation in their IoT solutions. The process includes as well the analysis of the legal, ethical, regulatory and social dimensions associated with the technology.

5 Conclusions

This paper presented ARCADIAN-IoT, a framework aimed at holistically managing identity, trust, privacy security and recovery capabilities in a holistic approach. Its concept and objectives have been described, along with its plane-based structure and corresponding functionalities. The future work includes the research and development of its components, and later on their integration and demonstration by supporting the described use cases.

References

1. Gartner insights on how to lead in a connected world. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf/, accessed: 2022-04-26
2. Netscout, weaponization of internet infrastructure. https://www.netscout.com/use-case/weaponization-internet-infrastructure (July 2020), accessed: 2022-04-26
3. Abie, H.: Cognitive cybersecurity for cps-iot enabled healthcare ecosystems. In: 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT). pp. 1–6. IEEE (2019)

4. Babar, S., Stango, A., Prasad, N., Sen, J., Prasad, R.: Proposed embedded security framework for internet of things (iot). In: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). pp. 1–5. IEEE (2011)
5. Bringhenti, D., Valenza, F., Basile, C.: Toward cybersecurity personalization in smart homes. IEEE Security & Privacy **20**(01), 45–53 (2022)
6. Burhan, M., Rehman, R.A., Khan, B., Kim, B.S.: Iot elements, layered architectures and security issues: A comprehensive survey. Sensors **18**(9), 2796 (2018)
7. da Cruz, M.A., Rodrigues, J.J.P., Al-Muhtadi, J., Korotaev, V.V., de Albuquerque, V.H.C.: A reference model for internet of things middleware. IEEE Internet of Things Journal **5**(2), 871–883 (2018)
8. Dhas, Y.J., Jeyanthi, P.: A review on internet of things protocol and service oriented middleware. In: 2019 International Conference on Communication and Signal Processing (ICCSP). pp. 0104–0108. IEEE (2019)
9. Jan, S.U., Ahmed, S., Shakhov, V., Koo, I.: Toward a lightweight intrusion detection system for the internet of things. IEEE Access **7**, 42450–42471 (2019)
10. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., Alazab, A.: A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics **8**(11), 1210 (2019)
11. Lee, I.: Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. Future Internet **12**(9), 157 (2020)
12. Lu, Y., Da Xu, L.: Internet of things (iot) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal **6**(2), 2103–2115 (2018)
13. Sankaran, S., Shivshankar, S., Nimmy, K.: Lhpuf: Lightweight hybrid puf for enhanced security in internet of things. In: 2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS). pp. 275–278. IEEE (2018)
14. Smys, S., Basar, A., Wang, H., et al.: Hybrid intrusion detection system for internet of things (iot). Journal of ISMAC **2**(04), 190–199 (2020)
15. Tiburski, R.T., Moratelli, C.R., Johann, S.F., Neves, M.V., de Matos, E., Amaral, L.A., Hessel, F.: Lightweight security architecture based on embedded virtualization and trust mechanisms for iot edge devices. IEEE Communications Magazine **57**(2), 67–73 (2019)
16. Tweneboah-Koduah, S., Skouby, K.E., Tadayoni, R.: Cyber security threats to iot applications and service domains. Wireless Personal Communications **95**(1), 169–185 (2017)
17. Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A., Meshcheryakov, R.: The cybersecurity in development of iot embedded technologies. In: 2017 International Conference on Information Science and Communications Technologies (ICISCT). pp. 1–4. IEEE (2017)
18. Vijayakumaran, C., Muthusenthil, B., Manickavasagam, B.: A reliable next generation cyber security architecture for industrial internet of things environment. International Journal of Electrical and Computer Engineering **10**(1), 387 (2020)
19. Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C.: A survey of intrusion detection in internet of things. Journal of Network and Computer Applications **84**, 25–37 (2017)