Security Assessment in IoT Ecosystems

Sotirios Evangelou
swtevag@gmail.com
Dept. of Electrical and Computer Engineering
University of Thessaly, Greece

Charilaos Akasiadis
cakasiadis@iit.demokritos.gr
Institute of Informatics and Telecommunications
N.C.S.R. ‘Demokritos’, Greece

ABSTRACT

The Internet of Things (IoT) and "Smart Everything" trend is a reality that is becoming part of our daily lives. Consequently, there is a gradual increase in the deployment of real world IoT systems that attempt to make use of the various possibilities and benefits the IoT offers. However, the connection of billions of—usually inherently insecure—devices in a network, paired with the lack of a clear security framework for the development of IoT systems and platforms has widened the attack surface of these systems leading to them being targeted by malicious actors. In this paper, we explore the problem and related research, devise an assets taxonomy and focus on the security requirements for each asset category. Then, we discuss countermeasures and good practices as well as new approaches based on AI that improve security and intrusion detection capabilities. We also introduce a metric that can be incorporated by automated security auditing methods. The relevance of this metric is evaluated with respect to correlation across findings from a real-world study.

KEYWORDS

Security, Internet of Things, IoT Ecosystems, Artificial Intelligence, Asset Taxonomy

1 INTRODUCTION

The Internet of Things (IoT) is a complex network that interconnects "things", i.e. uniquely identifiable programmable devices with physical sensing and/or actuation capabilities that form cyber-physical systems. Such devices mainly sense data from the physical world and take actions, with the possibility to also inter-operate with processing services [15]. The benefits offered are quite a few and they are currently being used in a wide range of use-cases, including healthcare [20, 26], fitness [41], manufacturing [57, 58], and agriculture industry [32, 49] among others. Ideas that would be previously deemed far-fetched and futuristic, such as self driving cars [17] and smart cities [34], are now realized.

The statistics related to the IoT are so far remarkable, and more or less depict the impact they induce in the modern life. According to IoT Analytics [30], in the end of 2019 the number of active IoT devices was estimated to be 9.5B, without counting mobile devices, or inactive ones; this number is continuously increasing. During the period of 2017-2025 the Compound Annual Growth Rate (CAGR) for the IoT connections is estimated to be 17% reaching 25 billion in 2025 and a 1.1 Trillion USD global market revenue according to FICCI/EY [48]. The total data volume by 2025 is projected to be 79.4 ZettaBytes (ZB) [38], and the number of IoT products is also rising, with publicly known IoT platforms in particular counting to 620 in 2019 [29]. Such information illustrate the size of the IoT potential. Adoption and usage rates are continuously rising and such solutions are used to reinforce important aspects of the production processes, including automation, monitoring and data analytics, towards sustainable and cost-effective processes.

Now, as with every disruptive technology, there are some challenges regarding IoT adoption as well. An important issue, that mainly comes up due to efforts in reducing investment costs, is increased security risks. Throughout the years, multiple vulnerabilities and security incidents have affected IoT ecosystems. Thus, focus is put into mitigating existing weaknesses and improving the security posture of such products. Research on IoT Cybersecurity covers a wide range of aspects, including the incorporation of security in the SDLC, auditing methodologies, surveys on attacks and common vulnerabilities, studies on good practices, as well as physical, hardware, software, and network security [1, 36].

In this work, we examine past research in the domain of security for IoT, and present a high-level taxonomy of the assets that compose a typical IoT ecosystem. Then, we briefly describe methods for evaluating the security posture by focusing in each of the identified assets, exploring insecure factors to assess desired requirements and highlight the aspects that could be reinforced. We cover a variety of ecosystem entities, since each of the assets performs differently in the ecosystem, and provides diverse security propositions due to the different nature of the various technology stacks incorporated. We establish a security baseline for each asset and collectively for the ecosystem itself. Additionally, we devise an index that combines aggregate real-world vulnerability data and their respective standardized scores (CVSS) into a single numerical value. Such an index can be incorporated in automated security assessment processes to compare security awareness and preparedness capacity of large IoT ecosystems. To illustrate applicability and effectiveness, we perform a correlation analysis with data from a real-world study providing cybersecurity statistics from many countries.

This paper is further structured as follows: In Section 2 we explore the previous related research. Section 3 provides a typical Internet of Things ecosystem asset taxonomy, and highlights the security requirements that need to be put in place, proposing controls, countermeasures, and best practices that can be applied to make each asset more secure. Section 4 presents a metric for cybersecurity awareness comparison between large device groups based on cumulative vulnerabilities to known attacks as well as the results from an analysis on real-world data that validates the metric’s applicability Finally, in Section 5 we conclude and discuss our future intentions.

AIT-CPS2020, September 02–04, 2020, Athens, Greece

2 RELATED WORK

Given the widespread adoption of IoT in business processes and the every-day lives of individuals, an IoT product should not be deemed ready to enter the market unless it fulfils some baseline security requirements. Here, we provide an overview of related work describing such sets of requirements and recommendations.

To begin, ENISA, the European Union Agency for Cybersecurity, offers two significant reports providing baseline recommendations, good practices, and guidelines for IoT product development, maintenance, and end-of-life management. In both of the reports, a detailed asset and threat taxonomy is presented, with a special emphasis in the most critical parts, along with the impact and the stakeholders that they affect. The first report [1] also performs a gap analysis, and offers good practices and recommendations. However, the recommendations mostly focus on non-technical aspects and serve a development, maintenance, and management strategy purpose. The good practices report [2] of 2019 emphasises on the incorporation of security in the software development life cycle of IoT products, analysing each cycle phase, and presenting good practices. Three types are recognized, the "People" which affect all stakeholders and phases, the "Processes" that affect the mechanisms surrounding the software project's environment , and “Technologies” that consist of countermeasures and development good practices.

In another approach, the Infocomm Media Development Authority presents an IoT Cybersecurity Guide that offers suggestions for the implementation and operational phase of the product and two checklists, a threat modelling checklist and a vendor disclosure checklist [3]. By using such checklists, potential vendors and developers can perform a self-assessment on the security posture of a product in development, evaluating if it is secure and market-ready. Here, we provide links to a thorough checklist, categorized by the taxonomy of the IoT ecosystem.

These works offer to vendors a defined set of requirements and guidelines that should be applied to a newly developed IoT product, so that it operates securely, adhering to privacy and safety needs. This paper combines the identification of assets, the security requirement assessment, and insecurity exploration, as well as a proposition of measures to address such insecurities. We approach the IoT ecosystem from a higher-level cyberphysical system's viewpoint and address all the types of co-existing stakeholders, including developers, system administrators, deployment infrastructure and end-users. We also focus on AI-related tools and programming techniques that can be applied by the responsible teams to improve the ‘marginal’ security of each asset.

2.1 The Attack Surface of IoT

An important aspect in the cybersecurity domain, is the “attack surface”, i.e. the sum of insecure entry points that a malicious actor could utilize in order to enter or attack an IoT system.

In [46], there is a focus on the network aspect of IoT deployments. They decompose a network into trust zones, and categorize existing devices into IoT domains (Finance, Home, Wellness etc.). Then, 14 common vulnerabilities are mapped to common attacks like Denial of Service, Ransomware, and SCADA Trojan horses. Finally, security controls to mitigate these weak spots are presented, and a detailed map of IoT domains with the vulnerabilities, attacks and security controls associated with these domains is also given.

In [16], the Internet of Things security challenges is analysed and security requirements are presented such as the CIA triad - Confidentiality, Integrity, Availability. Then, a decomposition of the IoT architecture into three basic domains is performed, the cloud domain containing the IoT applications and services, the sensing domain containing the devices and their communication means, and the fog domain including everything that stands between the sensing and cloud domains. Authors delve into security vulnerabilities and common attacks regarding these three domains, and propose countermeasures for each of the cases explored.

Security is examined in different IoT layers in [51]. They assess security based on systems software and hardware controls, as well as anti-tampering physical security techniques. Emphasis is given on the network layer, and in particular on encryption, authentication, secure routing, and key management for the encryption mechanisms. Denial of service (DoS) and distributed denial of service (DDoS) techniques are also referenced as a “popular” attack against IoT devices. The application layer security is also examined, and methods for security-by-design and run-time monitoring of the new Internet of Things products are proposed.

Finally, [36], performs an in-depth survey on IoT vulnerability research. The paper sums up a variety of research focused into the attack surface of IoT architectures, and presents a taxonomy of the collected results depending on different aspects—i.e., Layers, Impact, Attacks, etc.—and maps the corresponding research to these classifications. An empirical overview of the vulnerabilities is also presented, and the survey concludes with a presentation of the most important security challenges, paired with possible future initiatives to fight against each one.

These threat analyses cover a wide range of the possible threats concerning IoT infrastructures and products. Taking them into consideration, in Section 3 we create a picture of the baseline security requirements, and consequently the security measures that need to be in place in order to protect IoT deployments from such threats.

2.2 Artificial Intelligence-based Approaches

Artificial Intelligence (AI) and Machine Learning (ML) techniques are employed in a variety of methods for IoT security. Although manual labour and configuration are not yet fully replaceable in this domain, there is a number of aspects where AI techniques can provide great results towards a secure IoT ecosystem. In [5], the use of artificial neural networks (ANNs) as an intrusion detection system to combat DDoS attacks is evaluated. A multilayer perceptron neural network (MLP) is used to create an anomaly-based intrusion detection system. Experiments in a custom IoT deployment shows a great detection rate of 99%, while also providing a low false positive rate, which is one of the most significant goals of an intrusion detection system. Other than neural networks, techniques that perform well into network intrusion detection are k-NN, Random Forest, and Support Vector Machines [35, 61].

Local malware scanning is also an aspect where artificial intelligence techniques can be a great supplement to existing signature-based techniques. While signature-based approaches can protect against known malware, monitoring behaviour with AI techniques can often protect against new or unknown malware. In [56] there is a proposition for the use of k-NN and Random Forest classification algorithms on collected traffic data to identify malware with a high accuracy on standard datasets. The lack of resources in constrained devices is also addressed, where the solution is to collect application traces locally, and appoint the model training and predictions to a capable and trusted external server.

In [56], two unique use-cases are also reported, where ML can play a significant role in IoT devices. The first is for secure IoT off-loading as a method to combat jamming and Man In The Middle (MITM) attacks. Using reinforcement learning, and specifically the Q-learning technique, the model takes into consideration the task priority, channel bandwidth, gain, and jamming power in order to decide on off-loading policies according to a Q-value that indicates the long term reward from choosing this policy. Using this approach, the device can choose optimal offloading channels and subbands in order to avoid interference and jamming as well as spoofing attacks. Convolutional neural networks can also be used for the same purpose but they require more computational resources than Q-learning. The second case of [56] regards authentication using ML methods in order to avoid spoofing attacks. By using physical layer indicators, such as the received signal strength or the channel state information, learning techniques are able to exploit the indicators' connection to spatial characteristics in order to lure out connections that are initiated from outside a threshold proximity, reducing this way spoofing rates. Other than Q-learning, both supervised (distributed Frank Wolfe and incremental aggregated gradient) and unsupervised algorithms (Infinite Gaussian Mixture Model - IGMM) are used. For more resourceful devices, deep neural networks can also be applied to further improve the accuracy rates. IGMM is also reported as a useful algorithm for authentication by fingerprinting [24], where it is used to validate the credibility of the device by comparing the IGMM result with an expected value depending on the device's nature and shape. With respect to environmental changes, the model is able to distinguish a normal from a malicious one.

ML and essentially supervised learning methods usually require significant volumes of information termed as "Big Data" populating datasets used in security AI [60]. Information, apart from being the input that affects a model's decision, also plays a significant role in training, improving prediction accuracy and validating its efficiency. In order to leverage the advantages AI has to offer, we need to establish a way to collect, clean, and format corresponding data. An infrastructure for collecting, storing and analysing big data in IoT systems is presented in [47]. A data collection and actuation layer is introduced, with the collection aspect comprised of system- and application-level probes, a probe registry listing all the used probes, and a data routing middleware to route the data to the respective recipients. The actuation aspect includes Security Policy Enforcement where the data collected can be used to drive security decisions (e.g. disabling a service or closing a port) and visualizations where collected data and analyses are being displayed. The infrastructure also offers management agents and configuration tools.

2.3 Security Evaluation on Existing IoT Solutions

As IoT continuously evolves, it is useful to frequently perform security evaluations of widely used IoT platforms, frameworks, devices, products, and protocols. By reviewing the security controls in products that are currently in use or available for sale across the world, we can both see the common trends in security and their impact, as well as highlight the needs for more robust solutions.

In [9] a survey is presented on the architecture, hardware and software specifications, and security features regarding authentication, authorization, and secure communications in multiple IoT frameworks developed by popular vendors. These products are AWS IoT (Amazon), ARMbed (ARM), AzureIoT (Microsoft), Brillo/Weave (Google), Calvin (Ericsson), Homekit (Apple), Kura (Eclipse) and Smart Things (Samsung). Considering the conclusions, authors compare the chosen security controls and discover trends, such as the universal use of TLS/SSL and the popularity of AES cryptography and X.509 certificates.

The security of IoT products created for the Smart Home domain is examined in [7], including televisions, bulbs, etc. After decomposing deployments into 4 parts, namely the device, the mobile application, the cloud endpoint, and the communications, they proceed to explore existing research to identify the attack vectors of each part. These are cross-referenced to a wide variety of home IoT products. Next, by using the CVSS (Common Vulnerability Scoring System) standard [33] and associating every product with known CVEs (Common Vulnerabilities and Exposures) that are publicly known, they evaluate each product's security posture.

Meanwhile, there is research focusing in other domains as well, such as the Healthcare domain, e.g. in [42], where an evaluation of medical devices' resiliency is performed to a plethora of attacks with an emphasis on the significance of cryptography. In the case of Industrial IoT domain the work of [4] focuses on the security of such deployments to explore a method of continuous risk assessment.

3 SECURITY AUDITING METHODOLOGY FOR IOT ECOSYSTEMS

The Internet of Things is a complex ecosystem that consists of multiple significant components that one should be aware of. Moreover, as far as cyber-security is concerned, each of these components introduces its own security concerns resulting to a wider attack surface. In this section we present a coordinated methodology for decomposing complex Internet of Things ecosystems into simpler categories, and identify essential security controls and practices that should be applied in these components in order to improve the security of the overall ecosystem.

3.1 Asset taxonomy on a typical IoT Ecosystem

Despite the heterogeneity of IoT ecosystems that are currently deployed in the real-world, there are some components that are essentially the same in whichever ecosystem one decides to examine, and by identifying these components we can create an image of a typical IoT ecosystem, and this way generalise on its various assets and functionality. Figure 1 presents a typical IoT ecosystem and enumerates its basic assets, providing an asset taxonomy; we identify nine different basic assets, each with a separate role in the

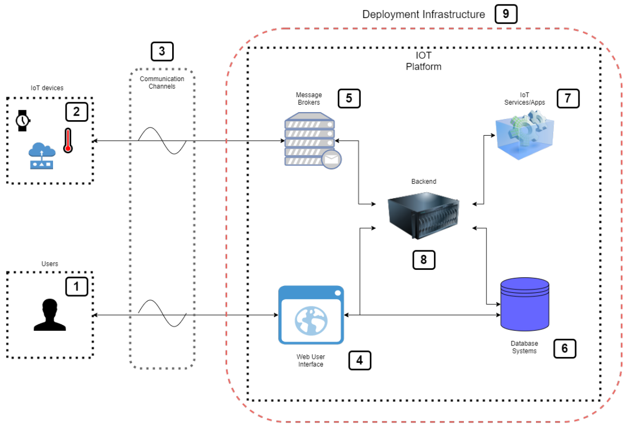

Figure 1: Asset Taxonomy of a typical IoT ecosystem

ecosystem, associated with different stakeholders, and introducing its own security risks. The asset taxonomy approach is definitely not new [1]. Our taxonomy, however, takes into consideration the human factor, as well as further decomposes the platform aspect for more structured assessment of its parts, distinguishing the following asset categories:

Users. The entities that constitute the end-users of the ecosystem, and who benefit from its use. Users can be individual persons, organizations, companies, or even whole countries. Apart from profit makers, this category also includes participants beyond development or marketing professions.

Devices. Smart watches and smart home equipment, sensors, surveillance cameras, and generally low-resource internet connected devices, all fall under this asset category. The devices can have both sensing and actuating capabilities.

Communication Channels. Communication channels are intangible entities and present the mechanisms that allow the interconnection and communication of users and devices to remote storage and computation spaces called the cloud.

Message Brokers. The message brokers are entities that reside in the platform part of the ecosystem and are the main entrypoints for data coming from IoT devices. The message brokers typically support many application protocols in order to promote interoperability and allow communication with other IoT devices.

Web Applications. The web applications are the IoT platform's entry points for Users, i.e. typical web interfaces that allow logging in and performing the various actions that each platform provides. Examples include adding/removing devices, handling data and incorporating logic, or exporting respective data from the platform.

Database Systems. The database systems are responsible for storing data. They can be relational or non-relational, depending on the platform, and they are key components for various mechanisms, such as authentication and authorization, data management, and the provisioning of data to IoT applications.

Internet of Things services/applications. This asset refers to applications that perform logical operations on data provided by IoT devices, or databases and output results that benefit the Users. Most platforms provide a set of predefined services, and some of them also allow the creation of custom applications which are usually executed into virtualized environments.

Back-end Servers. The back-end orchestrates the functionality of IoT platforms. It handles the interconnection and logical operation of the different assets, specifically the databases, the message brokers, the web applications, and other IoT services.

Deployment Infrastructure. This layer constitutes the basis of IoT platforms, either on edge, or cloud level. It refers to the physical servers where the platforms run, and the network deployment (routing, DNS etc.) that allows the communication between users and devices, with the remote platform services. It also provides connectivity capabilities to the platforms as well as bandwidth management.

3.2 Asset security requirements and countermeasures

The assets of this taxonomy can be found in the majority of IoT ecosystems and can be used to decompose a specific ecosystem respectively, regardless of the different implementation and technical specifications. Such an approach makes the security assessment simpler, as it focuses on the sub-surface that a researcher has to audit each time. Now, each asset should be assessed sequentially and the methodology should inform the researcher of requirements that need to be satisfied. Next, recommendations and best practices can be provided that will make each individual asset, and collectively the whole ecosystem, more secure. The propositions should provide a secure and trusted baseline that the stakeholders of each asset can build upon. Overall, there are some security measures and practices that are applicable to almost any asset category, and for that reason we discuss them first, in order to avoid repetition.

1. **Keep everything up to date.** Commercial systems and programs are constantly updating with new versions and patches, often addressing one or more CVEs. Thus, it is important to update the software versions regularly, since an internet search is enough for a malicious actor to inspect and possibly harm a vulnerable system.
2. **Backups.** Frequent backups is an essential good practice that needs to be followed. Source code, database information, configurations and other data that might be deleted by mistake or malice should be kept in separate storage medium, as backups with controlled access. This allows for quick recovery of production and even identification of a vulnerability in the event of a security incident.
3. **Monitoring and Logging.** Keeping information about change in states of assets is important. Logging significant events is useful for debugging, or, in our case, for inspecting security incidents. Monitoring is similar to logging, nevertheless presenting results in more intuitive ways (e.g. real-time graphs), and raising alerts when behaviour deviates. Often, ML techniques build models based on such values to predict and avoid unwanted situations, such as DoS attacks.

Based on the security control propositions that follow, we have compiled thorough checklists that summarize these measures.[1]

3.3 Users

In the ICT domain, the human factor is widely assumed to be the most weak and exploitable one. The occasions in which the human factor becomes the reason for a security breach, mainly fall under three categories: insider threats, careless and unaware personnel or users, and lack of business security culture/strategy.

One measure that is applied at scale for this type of asset, is the signing of NDAs (Non Disclosure Agreements), legal contracts signed by the employees, that forbid them from disclosing information regarding the company to third parties, protecting this way the intellectual property of the organization. Another measure is the strict access control over the company's assets; this can be achieved by monitoring access, logging, and analysis. Company-wide policies for least privilege and segregation of duties can also be applied, so that access is given to only the assets that are absolutely necessary for the completion of each employee's function. In this regard, AI technology can also contribute through User and Entity Behavioral Analytics (UEBA), that monitor user behaviour to identify anomalies and potentially prevent malicious actions. Tools like IBM QRadar UBA are able to monitor human factor behaviour, assign roles and identify role behaviour deviations to alert on occasions like tool misconfigurations, sharing of credentials, or admins changing user attributes [39].

Security awareness training is used to cultivate the personnel's security culture, awareness of good practices and sense of responsibility. Occasional briefing on security and simulation of attacks such as phishing from the security teams of companies to the rest of the teams, can help create good practice habits on the employees that can collectively improve the security posture of the company. The power of machine learning can also be leveraged here, as algorithms such as kNN, SVM, Random Forest, Neural Networks as well as unsupervised and similarity learning techniques perform well into detecting social engineering attacks such as phishing [6, 43] and malicious URL links [50, 52].

Regarding management strategies, which are not purely technical but could improve the security of the company significantly, responsible vulnerability disclosure programs can be incorporated. Here, external researchers or regular users that manage to find a bug in a product can disclose it to the engineering teams of the product so that it is quickly patched before it is exploited. In such cases, the individual can be rewarded financially, or in another way, depending on the severity of the found bug. This gives an incentive for researchers to disclose the bugs responsibly and not personally profit from them with malicious activities. Another significant measure is periodic company-wide risk and threat assessment, by either the company's internal security team or employment of external "red" teams and penetration testers. Finally, security incident scenario strategies should be in place in order to define the actions that will take place in the worst case of a security breach so that the company can identify a potential security hole, patch it and recover from the breach as soon as possible.

3.4 Devices

The Devices asset consists of every IoT device in the ecosystem. From a security perspective, the aspects of hardware, software architecture and physical security of the device should be examined.

Physical security is defined by the controls that exist in place to protect against malicious activities from actors with physical access. There are a lot of techniques that users and device vendors can apply in order to improve the physical security of their product, e.g. make sure that the device is not accessible, or not leave physical ports exposed. AI biometric access control to the IoT devices is encouraged when combined with rule-based access such as passwords, as AI substantially improves the accuracy of fingerprint, facial or iris scans [59]. Additionally, tampering prevention mechanisms [19] should be considered, that make it difficult for someone to physically tamper the device, e.g. boards encapsulated, or coated with specific materials such as epoxy or silicone. Security fuses are also widely used, and they are mechanisms of access control to the on-chip memory. These mechanisms are usually built in a way that they destroy stored data in the case that someone attempts to erase or reprogram them, as can happen for example with UV lights in semi-invasive attacks. In many cases, tampering detectors are also installed into the device. This way many types of physical attacks can be detected and be handled accordingly. Side channel attacks [8] are also a major threat for embedded devices. Passive Side channel attacks resort to analysing times, power consumption and temperature during cryptographic operations in order to identify properties, algorithms used or even keys. Countermeasures insert randomness in order to render the analysis useless, by time skewing, random heating, cache flushing, disabling or bypassing and many more methods.

Internet of Things devices can also be severely susceptible to Denial of Service attacks. Vampire attacks [55] attempt to drain the battery of ad-hoc wireless devices to induce DoS, where the nodes shut down and do not communicate with the rest of the deployment. Mitigation controls include the ability to reroute at each node if a shorter route is known or introducing a no-backtracking metric that ensures the gradual progress network packets and avoids loops. DoS can also be avoided through frequency hopping, using directional antennas, or by spectrum spreading [16].

Trusted computing [54] is another aspect of the embedded IoT devices' security. Trusted Execution Environments (TEEs) are processing units that ensure the protection of included code and data. Usually this is achieved by dedicated co-processors where security tasks are being offloaded from the main processor, and secure memory (dedicated on-chip RAM). Also, since outside the TEE data are not secure, there should be integrity checks for detecting modifications while outside. Secure booting is a significant feature of a TEE, as it verifies an image before it is executed, and in order to be successful secure storage of signatures and secure code for verification must be ensured. Therefore, the keys and signatures are written into protected read-only memory called hardware root of trust, that usually is on-SoC (System on chip) OTP (one-time-programmable) hardware that acts as anchor for the chain of trust.

Firmware updates is another issue that should be addressed. It is suggested that firmware updates should be encrypted and authenticated as well as be installed over the air (OTA) via secure

[1] https://github.com/EvangelouSotiris/Security-Assessment-in-IoT-Ecosystems_Summary-tables/raw/master/Summary_tables.pdf

protocol channels. Finally, application whitelisting is a popular method for avoiding malware installed inside the device. In [21], a store of binary checksums collected at a clean device state is used to block untrusted software execution and prevent its spreading. Malware detection in IoT devices can also be performed by static analysis of high level features using multiple classifiers like RIPPER, SVM, neural networks and more [37].

3.5 Communication Channels

Inside an IoT ecosystem, devices need to communicate. The data exchanged within the communication channels can be sensitive and private, thus eavesdropping and tampering must be avoided. Cryptography is the method that is widely used in order to avoid typical MITM attacks, and Transport Layer Security (TLS) is the standardized solution for secure encrypted communication. Specifically, TLSv1.2 and TLSv1.3 are the standardized (defined in RFC5246 [44] and RFC8446 [45] respectively) non-deprecated protocol versions used at the moment. The use of TLS assures confidentiality, authentication, and integrity. TLSv1.3 provides faster and more secure communication than 1.2, with more features such as Forward Secrecy. Lastly, TLS provides the capability for two-way authentication. Servers carry X.509 certificates to be trustworthy but clients can also carry certificates signed by a trusted CA. This can be useful in the ecosystem of IoT in order to authenticate devices that send data to the cloud applications. When TLS client certificates are not preferred, the devices can be authenticated through the use of AI algorithms for proximity-based or fingerprint-based authentication, where IGMM, Q-learning and neural networks are found to produce highly accurate results [24, 56].

The use of cryptography, however, presents the engineers with a significant tradeoff in the case of Internet of Things devices. Overheads in time and processing power happen during the calculations for encrypting, decrypting and key generating and exchanging. Consequently, there is a need to use lightweight algorithms for these security tasks that will not compromise the security posture of a potential IoT device, neither will it compromise the device's performance and latency in performing its functionalities.

Starting off with assymetric cryptography, between the two options in Diffie-Hellman (DH) and RSA, the first is preferred, and mostly its version leveraging elliptic curves (ECC) and featuring forward secrecy - Elliptic Curves Diffie Hellman Ephemeral (ECDHE). On symmetric cryptography, AEAD algorithms that encrypt and authenticate in one pass are gaining popularity, with AES-GCM and the ChaCha20-Poly1305 combination being the most secure, fast and least resource intensive options. ChaCha20-Poly1305 is proposed in [10] as the favorable option for smart devices in TLSv1.3, but in TLSv1.2 AES-GCM is proposed, especially with the performance spike in devices with specific instructions for hardware acceleration in specific cryptographic steps.

Regarding hashing algorithms, the performance evaluation generally seems to have minimal significance compared to e.g. the latency and energy consumption of asymmetric algorithms. Nevertheless, in [40] there is a study on hashing algorithms in IoT platforms and embedded devices, where Blake2 [12] is found to be more lightweight, energy efficient and fast. Other lightweight hashing families of algorithms are Photon [23] and Quark [11].

So far, we have assumed that the devices have the capabilities of establishing a TLS connection with a remote server. In some low-resourced devices though this is not the case, and the minimum threshold for TLS-based solutions is 10KBs of RAM and 100KBs of ROM. In these situations a middleware is needed to provide the TLS-based communication for the constrained IoT devices [27].

3.6 Message Brokers

Message brokers are the entry points of IoT device data to the IoT platform, and they usually work with multiple application layer protocols such as HTTP (REST), MQTT and CoAP. TLS and X.509 certificates are the way to secure communication between devices and message brokers, as already discussed. If mutual authentication is configured, this is the asset to perform device authentication and determine access rights. Otherwise, authentication with passwords or tokens can also be implemented, where the broker can rely on the back-end for authentication purposes.

Another security measure that can be typically implemented here, is authorization and access control, so that IoT devices can publish to a particular topic, with their data are used by the intended subscribers alone, and vice versa so that subscribers ensure that the data originate from specific trusted publishers. Each Message Queue/Broker server usually provides a certain way of defining access control and authorization policies, but the two most common approaches are Access Control Lists (ACL) which are lists that associate users with permissions and Role-Based Access Control (RBAC) where roles are associated with permissions and users can have one or multiple roles, inheriting their permissions. Genetic Algorithms can be used for role-mining in order to automatically create roles and define RBAC policies [18]. [28] also presents some other authorization trends such as UCON (Usage control) which is used for continuously mutating authorization factors such as pay-per-view or metered payment situations and CapBAC which uses tokens to associate users with specific capabilities.

3.7 Web Application Interfaces

Web applications usually are the asset that offer the largest attack surface since they provide a wide range of functionalities triggered by user actions, and they are fully visible to the public. There are numerous ways to "harm" a web application, and there are also various tools available to help to this end. Here as well, encryption between users and the front-end is essential.

A well known category is the injection attacks. This refers to commands being passed to an interpreter or another program, where part of the commands is derived from user input. SQL, NoSQL, LDAP, and OS injections belong to this category. User input validation and sanitation is needed to constrain the choices the user has in the data entered. Moreover, access control should be implemented correctly and carefully so that users only have access to authorized content. The authorization is mostly implemented with middleware software between function calls that acknowledges whether the user is authorised to access the functionality after the middleware. General web application attacks are also relevant here, such as cross-site scripting, external XML entities (XXEs), information-exposing error reporting, unprotected assets and more.

The identification of such vulnerabilities is based into detecting the entrypoints of user input and applying validation and escaping when this input is going to be used into HTML, CSS, Javascript and generally any interpretable content, or using modern frontend frameworks that tend to provide automatic sanitization e.g. Angular. The use of security tools for web applications testing is applicable here as well, such as Arachni, OWASP ZAP, W3af and Wfuzz. Finally, web application firewalls can help mitigate lots of attacks through a mixture of the traditional signature-based approach and supervised or unsupervised Machine Learning techniques to handle unknown injection attacks [22, 31].

3.8 Database Systems

Databases are the assets that hold the majority of the data of the IoT ecosystem, as well as the functionality to access it. The information stored should be protected in terms of confidentiality and integrity. Starting with the SQL injection vulnerability mentioned previously, stored procedures was proposed as a way to limit outer effect to internal queries. Access control in query capabilities is also essential. The user that makes the queries should not be 'root', but should only have restricted authorization. Furthermore, the databases should not be directly exposed to the internet where remote malicious actors could potentially gather information, as well as send payloads for penetration testing.

Data, and essentially sensitive data should be protected, e.g. in the incident of an information leakage; credential information such as passwords should be hashed, and the authentication should be performed by comparing the hash of the password given by the login form with the password hash located in the database, so that even if the case that this hash is leaked, the malicious actor cannot discover the original password without bruteforcing. Additionally, the whole database could be encrypted though that does come with a trade-off in the latency (and potential insecurity) that the middleware application that encrypts and decrypts the data introduces.

Cryptographic key management is also an issue that should be tackled in the database asset level. Private, Symmetric and Hash keys that are used to encrypt, decrypt or digitally sign data need to be kept on a secure storage where they are accessed only by authenticated users, mostly developers. First and foremost, these keys should not be kept in the database with the data they protect, and if possible not even in the same server. In the case they are placed in the same server, they should be given appropriate read-write-execute permissions. A solution heavily proposed, although expensive, are Hardware Security Modules (HSMs) which are hardware solutions for keeping keys and performing cryptographic tasks for the server.

3.9 Processing Services

The driving force of IoT are applications and services that process incoming data from the devices and forward results to users, or other devices and applications. A range of preset applications is usually provided by the platform to the users, but most of the commercial platforms also allow users to create their own applications, deploy, and share them with the community. As with any user input and especially executable content in this case, several security risks are posed for the platform and should be carefully handled.

Whenever the execution of a process needs to be controlled, there is a need for isolated environments, and the solution is usually through virtualization. These types of environments are capable of running non-trusted programs or opening non-trusted files that could potentially be malicious inside a controlled environment without directly affecting the server in which they reside. Containers are heavily preferred for application deployment as they are fast to deploy and kill, and easier to control. Containers have some inherent security characteristics but there is a number of measures that can be taken to protect the system whenever containers run non-trusted user code. [53] propose to run containers inside a VM in order to add the virtual kernel layer of security in the case of a container escape. Other measures to increase security are running the programs created by the user as non-root and with least privileges, and in secure minimal container images containing just the necessary binaries that each program functionality requires. Also, restricted versions of programming languages are usually employed, in order to avoid language-specific capabilities such as execution of shell commands. Lastly, in some cases the spawned services might attempt to starve the host of resources for prolonged timeframes. Thus, there should be a time and resource (CPU, Memory, Storage) quota on the spawned containers in order to avoid this kind of DoS incidents. Also, the network accessibility of the containers should be controlled and constrained to the extent possible.

3.10 Backend Servers

Backend is the asset where the functionality of the different parts of the IoT platform is orchestrated. Data is received there and stored into databases, or sent to processing services. Also, communications with the Frontend Web Applications are facilitated to address user requests. The backend also provides functionality over the Internet, mostly through Application Programming Interfaces (APIs). Web application and Database Security have already been discussed in their respective sub chapters, so here the focus is to the APIs used either by other assets or external users.

First, the publicly exposed APIs should be protected with encryption in order to avoid eavesdropping. Also, authentication should be enforced in order to use the API, usually through API tokens. Authorization should also be kept in mind since, the APIs must ensure that the user only accesses and uses the content he is authorized for. The rate of the requests is another factor that needs to be accounted for in order to avoid DoS situations and make the API scalable. Rate limiting can be implemented in many ways, with the most popular being putting the request in message queues and process each one in a specific rate, or throttling of the user's connection (bandwidth limiting) upon detection of surpassing the request rate. Input parameter validation should be made in the API requests as with any entry point, using rules to enforce consistency with the API's expectations. The validation could be implemented as a middleware receiving the requests at an API gateway which could be used for other reasons as well, such as monitoring API traffic and applying machine learning and AI to find deviations from normal behaviour and flag possible attack attempts.

3.11 Deployment Infrastructure

A substantial part of the IoT ecosystem is hosted on cloud or edge infrastructure. Starting from physical security, the infrastructure is expected to have strict access control with multi-factor authentication to the machines and other assets, camera surveillance and a great resiliency to physical disasters. Device and network monitoring is also imperative, with alerts triggered in case of strange behaviour. Strict control should also exist in the application level, with secure, authenticated, and authorised management software on the provider's side. On deployment, CSPs should ensure VM quotas are met, and VMs are isolated when the deployment is not on a dedicated machine.

Cyberthreat detection is also required in order to provide appropriate protection. Multi-technology systems are deployed in strategic network locations for this purpose, such as Network Intrusion Detection systems (NIDS) and Network Intrusion Prevention Systems (NIPS) that essentially combine the NIDS real-time threat detection with linkage to firewall rules in order to block those threats. These systems are based on anomaly detection techniques to detect deviations from normal behaviour and block untrusted data packets before they reach the hosts. This approach allows not only protection against known attacks, which could very well be avoided by the firewall rules, but also against unknown attacks in some cases. Many machine learning techniques perform well in intrusion detection including Neural Networks (CNNs, MLPs), SVMs, Naive Bayes, Decision Trees and Logistic Regression [14].

Having defined the security controls for each asset in the taxonomy, in what follows, we present a metric that can be used to collectively assess the security awareness in large pools of IoT-enabled devices, in order to highlight the vulnerabilities to be addressed.

4 LACK OF SECURITY AWARENESS RATIO

We hereby define a metric that can be incorporated to show how well protected an IoT ecosystem is, by examining a number of indicators that can be retrieved without authorized access to assets.

The data used to compute our metric are collected using Shodan, a global crawler for Internet-connected devices. It scans global IPs, collects information such as the organization name, location, domain name, open ports, services, and attempts to grab the banner of the audited services to learn more specific information, e.g. version, and then map it with specific CVE vulnerabilities. Using Shodan API, we initially collect information about the number of internet connected devices globally categorised by country, for the top 200 results, excluding those with population of less than 300,000.

First, we determine the number of devices found vulnerable with specific vulnerabilities with CVE identification numbers. Next, the weighted sum of them was computed for each country using as weights their CVSS score, and their exploitability score. From the calculated vulnerabilities with less than 6.0 CVSS score or Local/-Physical attack vector were excluded in order to keep only severe and relatively easily remotely exploitable vulnerabilities. In that regard, it was assumed that devices with vulnerabilities in that category would most likely become a cyber-attack target because of the ease of exploit and impact that a malicious actor can deliver.

Dividing the weighted sum of vulnerabilities per country with the number of internet connected devices in each, results to a metric that can indicate how updated and secure against harmful remote cyberattacks a country's systems are, and, consequently, assess each country's security awareness. This measure is termed as LSAR, for Lack of Security Awareness Ratio. In theory, high values of LSAR indicate greater density of vulnerable and exploitable devices in a group of devices, deeming that group as a more possible target of malicious actors than one with a smaller LSAR.

$$LSAR = \frac{\sum_i (\#Occurences_i \times CVSSscore_i \times Exploitabilityscore_i)}{\#Devices}$$

where

$$i \in \{\text{CVE-X} | CVSSscore_i > 6.0 \cap Vector_i \notin Local, Physical\}$$

The resulting LSAR values are shown in Table 1:

Table 1: Top 20 countries by LSAR

0	HTI	1.422832	10	MYS	0.404316
1	UZB	1.164537	11	TWN	0.398422
2	ZWE	0.782047	12	PER	0.397818
3	HKG	0.721822	13	TJK	0.392794
4	ETH	0.636363	14	ZAF	0.379868
5	JOR	0.522041	15	SEN	0.372707
6	PNG	0.455162	16	GTM	0.348438
7	LBN	0.451086	17	CHN	0.331362
8	MRT	0.441238	18	SLE	0.323695
9	KGZ	0.405626	19	BTN	0.321850

Results include the countries with the biggest LSAR metrics, meaning the countries with the least security preparedness against known exploits and remote cyberattacks, hence least security awareness. To validate LSAR, we compare it with results from a survey [13] for the best and worst security in countries. The survey includes data up to March 2020, which is adequately close to data collection from Shodan for the LSAR computation (late April, 2020). In this survey, countries are ranked for the percentage of mobile devices and computers infected with malware, the number of financial malware attacks, the percentage of all telnet attacks by originating country, of users attacked by cryptominers, and the best-prepared countries for cyber attacks.

Combining this survey's results with LSAR, 65 countries belong in both of the datasets and thus can be compared. We explore the correlation between the LSAR feature and the features introduced by the Comparitech survey. Results are shown in Fig. 2 and Fig. 3, for the Pearson and Spearman correlation coefficients, respectively.

LSAR has a moderate uphill relationship with cryptomining attacks (+0.52,+0.54 correlation coefficients). This means that a high LSAR is correlated with a high percentage of cryptomining attacks. These, being one of the most popular uses of botnets, tend to target remotely exploitable devices, in order to amass computing power for mining operations in blockchain cryptocurrencies.

LSAR has a moderate uphill relationship with financial malware attacks, malware targeting bank accounts to steal money from victims (+0.58,+0.46 correlation coefficients). While this correlation validates the relationship of high LSAR with high percentage of malware targeting the victim, we require additional data which are hard to acquire to explore whether this assumption is valid.

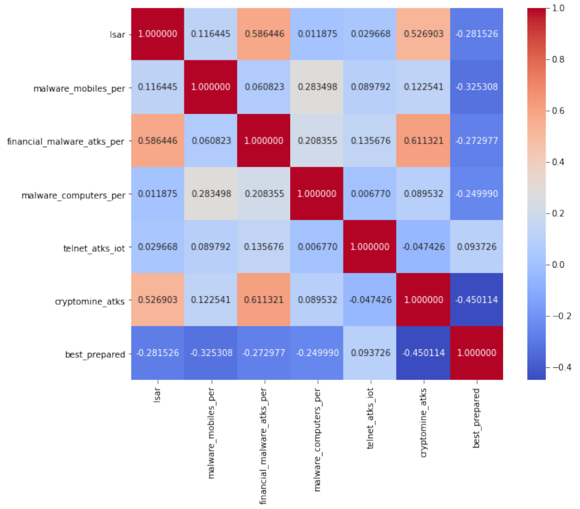

Figure 2: Pearson correlation coefficient

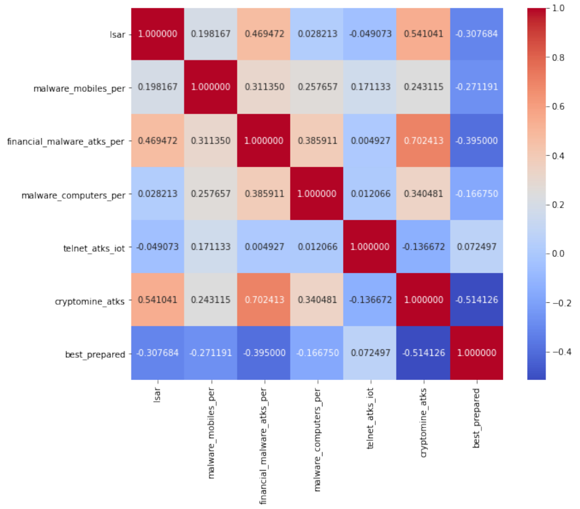

Figure 3: Spearman correlation coefficient

LSAR and the best-prepared metric of the Comparitech survey have a moderate downhill relationship (-0.28,-0.30 correlation coefficients), which is expected. This further validates our findings rendering LSAR as a metric to check the security posture of a sum of devices, in this case a country. The coefficients are not very high, which could be explained from the specificity of the use case of the Shodan findings (external attacks) compared to the best-prepared feature which is derived from the Global Cybersecurity Index scores [25]. The GCI score performs a general security evaluation on a country's cybersecurity including factors such as cyber crime legislations and information extracted from questionnaires, hence the index is not fully consistent with our case.

LSAR has a weak uphill relationship with mobiles infected with malware. Additionally, there is a non-significant relationship of LSAR with computer malware which could be explained from the fact that most of it deviates from attacks like phishing, downloaded malware disguised as a useful program or infected drives. The case of the Shodan findings is the vulnerability to external cyberattacks so a huge proportion of the variability that could be explained is missed, thus the insignificant correlation with mobile and computer malware. Telnet attacks and LSAR also have insignificant correlation which is explained from the fact that they are bruteforcing attacks, not CVE-specific exploits.

Summarizing, we can see that even the omission of a simple activity such as consistent updating of software to secure versions can compromise the security of a device, and collectively widen the attack surface of the device's environment. The LSAR is a metric that can be used to assess the security posture of a large group of internet connected devices, owned and handled by different individuals or organizations by checking the exposure to potential common vulnerabilities (CVEs). Apart from countries, large groups of machines/devices could also be considered to be Wide Area Networks (WAN), geographical regions such as cities, or even large data centers were the VM could take the place of devices, and in those cases LSAR can provide a general view of the awareness of security as well as the density of vulnerable points inside the group.

5 CONCLUSIONS

In this paper, we established a structured methodology towards assessing the security posture of an Internet of Things ecosystem and reinforcing it. This is achieved through a divide and conquer approach where we decompose the ecosystem into the assets that compile it, inspecting each asset's attack surface, defining security requirements, and proposing mitigations or good practices. This work aspires to become a handy guide for developers, researchers, engineers or managers working on the IoT domain, and contribute to the vast research towards secure IoT deployments and products. Potential future work includes a practical application of the defined methodology into a real IoT ecosystem focused on a specific use-case, such as a power-grid or a vehicular Ad-hoc network. Such an approach could validate the methodology's applicability and usability as well as yield potential insecure factors that this work has not yet taken consideration of.

ACKNOWLEDGMENTS

Charilaos Akasiadis acknowledges partial support of this work by the project SYNTELESIS "Innovative Technologies and Applications based on the Internet of Things (IoT) and the Cloud Computing" (MIS 5002521), which is implemented under the "Action for the Strategic Development on the Research and Technological Sector", funded by the Operational Programme "Competitiveness, Entrepreneurship and Innovation" (NSRF 2014-2020), and co-financed by Greece and the European Union (European Regional Development Fund).

REFERENCES

[1] 2017. *Baseline Security Recommendations for IoT: in the context of critical infrastructures.* Technical Report. ENISA: European Union Agency for Cybersecurity.

[2] 2019. *Good Practices for Security of IoT: Secure Software Development Lifecycle.* Technical Report. ENISA: European Union Agency for Cybersecurity.

[3] 2019. *Guidelines: Internet of Things (IoT) Cybersecurity Guide.* Technical Report. Infocomm Media Development Authority.

[4] C. Adaros Boye, P. Kearney, and M. Josephs. 2018. Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment. In *Information Security*. Springer Int. Publishing, 502–519.

[5] T. Ahanger. 2018. Defense Scheme to Protect IoT from Cyber Attacks using AI Principles. *Int. Journal of Computers Communications & Control* 13 (11 2018), 915–926. https://doi.org/10.15837/ijccc.2018.6.3356

[6] A. A. Akinyelu and A. O. Adewumi. 2014. Classification of Phishing Email Using Random Forest Machine Learning Technique. *Journal of Applied Mathematics* 2014 (03 Apr 2014), 425731. https://doi.org/10.1155/2014/425731

[7] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. 2019. SoK: Security Evaluation of Home-Based IoT Deployments. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA. https://doi.org/10.1109/SP.2019.00013

[8] J. Ambrose, R. Ragel, D. Jayasinghe, T. Li, and S. Parameswaran. 2015. Side channel attacks in embedded systems: A tale of hostilities and deterrence. 2015 (04 2015), 452–459. https://doi.org/10.1109/ISQED.2015.7085468

[9] M. Ammar, G. Russello, and B. Crispo. 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications* 38 (2018), 8–27. https://doi.org/10.1016/j.jisa.2017.11.002 cited By 144.

[10] B. Arunkumar and K. Govardhanan. 2018. Analysis of AES-GCM Cipher Suites in TLS. 102–111. https://doi.org/10.1007/978-3-319-68385-0_9

[11] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. 2010. Quark: A Lightweight Hash. *Journal of Cryptology* 26, 1–15. https://doi.org/10.1007/978-3-642-15031-9_1

[12] J.-P. Aumasson, S. Neves, Z. Wilcox-O'Hearn, and C. Winnerlein. 2013. BLAKE2: Simpler, Smaller, Fast as MD5. In *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 119–135.

[13] Paul Bischoff. 2020. Which countries have the worst (and best) cybersecurity? https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

[14] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys Tutorials* 21, 3 (2019), 2671–2701.

[15] A.B. Chebudie, R. Minerva, and D. Rotondi. 2015. *Towards a definition of the Internet of Things (IoT)*. Ph.D. Dissertation.

[16] M. Dabbagh and A. Rayes. 2017. *Internet of Things Security and Privacy*. 195–223. https://doi.org/10.1007/978-3-319-44860-2_8

[17] M. Dikmen and C. Burns. 2017. Trust in autonomous vehicles: The case of Tesla Autopilot and Summon. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 1093–1098.

[18] X. Du and X. Chang. 2014. Performance of AI algorithms for mining meaningful roles. *Proceedings of the 2014 IEEE Congress on Evolutionary Computation, CEC 2014*, 2070–2076. https://doi.org/10.1109/CEC.2014.6900321

[19] E. Dubrova. 2018. *Anti-tamper techniques*. Technical Report. KTH Royal Institute of Technology, Sweden.

[20] B. Farahani, F. Firouzi, and K. Chakrabarty. 2020. *Healthcare IoT*. 515–545. https://doi.org/10.1007/978-3-030-30367-9_11

[21] T. Gopal, M. Meerolla, G. Jyostna, L. Eswari, and E. Magesh. 2018. Mitigating Mirai Malware Spreading in IoT Environment. 2226–2230. https://doi.org/10.1109/ICACCI.2018.8554643

[22] S. Goswami, N. Hoque, Dhruba K Bhattacharyya, and Jugal Kalita. 2017. An unsupervised method for detection of XSS attack. *International Journal of Network Security* 19 (09 2017), 761–775. https://doi.org/10.6633/IJNS.201709.19(5).14

[23] J. Guo, T. Peyrin, and A. Poschmann. 2011. The PHOTON Family of Lightweight Hash Functions. In *Advances in Cryptology – CRYPTO 2011*. Springer BH, 222–239.

[24] A. Hameed and A. Alomary. 2019. Security Issues in IoT: A Survey. 1–5. https://doi.org/10.1109/3ICT.2019.8910320

[25] International. 2020. Global Cybersecurity Index. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

[26] G. Kaur and M. Sohal. 2018. IOT Survey: The Phase Changer in Healthcare Industry. *Int. Journal of Scientific Research in Network Security and Communication* 6 (04 2018), 34–39. https://doi.org/10.26438/ijsrnsc/v6i2.3439

[27] J. King and A. I. Awad. 2016. A distributed security mechanism for Resource-Constrained IoT Devices. 40 (01 2016), 133–143.

[28] Y. Lee, J. Lim, Y. Jeon, and J. Kim. 2015. Technology trends of access control in IoT and requirements analysis. 1031–1033. https://doi.org/10.1109/ICTC.2015.7354730

[29] S. Liu. 2020. Internet of Things - Statistics & Facts. https://www.statista.com/topics/2637/internet-of-things/.

[30] K. L. Lueth. 2020. IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year. https://iot-analytics.com/iot-2019-in-review/.

[31] A. Makiou, Y. Begriche, and A. Serhrouchni. 2014. Improving Web Application Firewalls to detect advanced SQL injection attacks. *2014 10th Int. Conf. on Inf. Assurance and Security* (11 2014). https://doi.org/10.1109/ISIAS.2014.7064617

[32] M. S. Mekala and V. Perumal. 2017. A Survey: Smart agriculture IoT with cloud computing. 1–7. https://doi.org/10.1109/ICMDCS.2017.8211551

[33] Romanosky S. Mell P, Scarfone K. 2007. *CVSS: a complete guide to the common vulnerability scoring system version 2.0*. Technical Report. FIRST: forum of incident response and security teams.

[34] S. Mohanty. 2016. Everything You Wanted to Know About Smart Cities. *IEEE Cons. Electronics Mag.* 5 (2016), 60–70. https://doi.org/10.1109/MCE.2016.2556879

[35] S. Mukkamala, G. Janoski, and A. Sung. 2002. Intrusion detection using neural networks and support vector machines. *Proc. of the Int. Joint Conf. on Neural Networks* 2, 1702 – 1707. https://doi.org/10.1109/IJCNN.2002.1007774

[36] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. 2019. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys Tutorials* 21, 3 (2019), 2702–2733.

[37] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, and D.-H. Nguyen. 2020. A survey of IoT malware and detection methods based on static features. *ICT Express* (2020). https://doi.org/10.1016/j.icte.2020.04.005

[38] S. O'Dea. 2020. Data volume of IoT connected devices worldwide 2018 and 2025. https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/.

[39] M. Patel. 2017. *QRadar UBA App Adds Machine Learning and Peer Group Analyses to Detect Anomalies in Users' Activities*. Technical Report. SecurityIntelligence.com.

[40] G. C. C. F. Pereira, R. C. A. Alves, F. L. da Silva, R. M. Azevedo, B. C. Albertini, and C. B. Margi. 2017. Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems. *Security and Communication Networks* (2017), 1–16. https://doi.org/10.1155/2017/2046735

[41] H. Qiu, X. Wang, and F. Xie. 2017. A Survey on Smart Wearables in the Application of Fitness. 303–307. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.64

[42] S. Ragupathy and M. Thirugnanam. 2017. *Review on Communication Security Issues in IoT Medical Devices*. 189.

[43] S. Rawal, B. Rawal, A. Shaheen, and S. Malik. 2017. Phishing Detection in E-mails using Machine Learning. *Int. Journal of Applied Information Systems* 12 (10 2017), 21–24. https://doi.org/10.5120/ijais2017451713

[44] E. Rescorla. 2008. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246. RFC Editor. https://www.rfc-editor.org/rfc/rfc5246.txt

[45] E. Rescorla. 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. RFC Editor. https://www.rfc-editor.org/rfc/rfc8446.txt

[46] S. Rizvi, RJ Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi. 2020. Identifying the attack surface for IoT network. *Internet of Things* 9 (2020), 100162. https://doi.org/10.1016/j.iot.2020.100162

[47] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, and N. Kefalakis. 2019. Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems. 1–6. https://doi.org/10.1109/GIOTS.2019.8766407

[48] R.Rishi and R. Saluja. 2019. Future of IoT. http://ficci.in/spdocument/23092/Future-of-IoT.pdf.

[49] J. Ruan, H. Jiang, C. Zhu, X. Hu, Y. Shi, T. Liu, W. Rao, and F Chan. 2019. Agriculture IoT: Emerging Trends, Cooperation Networks, and Outlook. *IEEE Wireless Communications* 26 (12 2019), 56–63. https://doi.org/10.1109/MWC.001.1900096

[50] D. Sahoo, C. Liu, and S. Hoi. 2017. Malicious URL Detection using Machine Learning: A Survey. (01 2017).

[51] D. Serpanos and M. Wolf. 2017. Security and Safety. In *Internet-of-Things (IoT) Systems*. Springer Int. Pub., 55–76. https://doi.org/10.1007/978-3-319-69715-4_6

[52] A. Sharma and A. Thakral. 2020. Malicious URL Classification Using Machine Learning Algorithms and Comparative Analysis. In *Proc. of the 3rd Int. Conf. on Computational Intelligence and Informatics*, K. S. Raju, A. Govardhan, B. P. Rani, R. Sridevi, and M. R. Murty (Eds.). Springer Singapore, Singapore, 791–799.

[53] J. Shetty. 2017. A State-of-Art Review of Docker Container Security Issues and Solutions. *American International Journal of Research in Science, Technology, Engineering & Mathematics* (01 2017).

[54] A. Ukil, J. Sen, and S. Koilakonda. 2011. Embedded Security for Internet of Things. 1 – 6. https://doi.org/10.1109/NCETACS.2011.5751382

[55] E. Vasserman and N. Hopper. 2013. Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *Mobile Computing, IEEE Trans. on* 12 (02 2013), 318–332. https://doi.org/10.1109/TMC.2011.274

[56] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu. 2018. IoT Security Techniques Based on Machine Learning. (01 2018).

[57] H. Xu, W. Yu, D. Griffith, and N. Golmie. 2018. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access* 6 (2018), 78238–78259. https://doi.org/10.1109/ACCESS.2018.2884906

[58] L. Xu, W. He, and S. Li. 2014. Internet of Things in Industries: A Survey. *IEEE Trans. on Industrial Informatics* 10 (11 2014), 2233–2243. https://doi.org/10.1109/TII.2014.2300753

[59] W. Yang, S. Wang, J. Hu, Z. Guanglou, and C. Valli. 2019. Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry* 11 (01 2019), 141. https://doi.org/10.3390/sym11020141

[60] O. Yavanoglu and M. Aydos. 2017. A Review on Cyber Security Datasets for Machine Learning Algorithms. https://doi.org/10.1109/BigData.2017.8258167

[61] M. Zamani and M. Movahedi. 2013. Machine learning techniques for intrusion detection. *arXiv preprint arXiv:1312.2177* (2013).