Automation and Orchestration of IoT Security

Reddy supriya[1], S Mabuni[2], B Srinivasulu[3]
[1]Department of CSE
[2] Assistant Professor, Department of CSE
[3] Head of the Department, Department of CSE
[1, 2, 3]Seshachala institute of technology

Abstract- *The massive boom of Internet of Things (IoT) has led to the explosion of smart IoT devices and the emergence of various applications such as smart cities, smart grids, smart mining, connected health, and more. While the proliferation of IoT systems promises many benefits for different sectors, it also exposes a large attack surface, raising an imperative need to put security in the first place. It is impractical to heavily rely on manual operations to deal with security of massive IoT devices and applications. Hence, there is a strong need for securing IoT systems with minimum human intervention. In light of this situation, in this paper, we envision security automation and orchestration for IoT systems. After conducting a comprehensive evaluation of the literature and having conversations with indus- try partners, we envision a framework integrating key elements towards this goal. For each element, we investigate the existing landscapes, discuss the current challenges, and identify future directions. We hope that this paper will bring the attention of the academic and industrial community towards solving challenges related to security automation and orchestration for IoT systems.*

Keywords: *IoT, security, security automation, security orchestration, configuration.*

I. INTRODUCTION

The Internet of Things (IoT) is experiencing a tremendous boom, with the number of network-connected IoT devices expected to grow to 50 billion in 2020 [1]. With the support of a variety of communication technologies such as Wi- Fi, Bluetooth, 3G/4G networks, satellites, IoT has enabled a very broad range of applications, including smart cities, smart grids, smart mining, smart farming, smart transportation, connected health, and many more. In addition to the terrestrial technologies that can support most IoT applications, there are also satellite networks which allow IoT to be deployed in geographically remote regions where terrestrial networks fall short. For example, hazardous industries (such as mining, oil, and gas) and agriculture are usually located in geographically remote regions, suffering network issues. Satellite networks could be used in such a situation to help IoT systems to monitor conditions remotely and gather data to anticipate and react to potential safety threats. Other examples of the use of satellite networks are transport and logistics applications for IoT. They allow us to track goods and services utilization based on Radio Frequency ID (RFID) tags and an array of sensor devices linked to actuators or complex IT-based logistics software. These applications range from automated haulage, industrial production lines, smart airports to agricultural applications as part of the food supply networks.

However, the proliferation of IoT devices and applications exposes a large attack surface for cyber-attacks. According to the United States Defense Advanced Research Projects Agency (DARPA) [2], the deployment of smart IoT devices has quickly spread across different sectors including industry, government, and military platforms. There is a growing trend of using cheaper programmed IoT components to replace the special purpose, custom-built systems too provide identical functionalities. As programmable configurations and software settings now govern behaviors that were physically hard to achieve in special-purpose hardware, this creates security risks as well as increases system vulnerability [2]. IoT devices have a growing market, that was originally dominated by consumer electronics and is now entering the industrial arena through innovations in Industry 4.0 and Factory of the Future devel- opments. Often, significant price pressures and competition means that good hardware/software design practices have been sacrificed for time-to-market and market-share considerations, thus exposing these devices and the systems they integrate with, to many more vulnerabilities [3].

From a practical perspective, there is a strong demand to accomplish security automation and orchestration for IoT systems, so that the security operations and tasks of IoT systems can be automated and work together with minimum human intervention. Since IoT systems are typically complex, large-scale distributed systems, it is becoming increasingly challenging to detect and prevent various types of potential attacks against them. It is a non-trivial task to update the software running on thousands (or even millions) of heteroge- neous devices when the attackers compromise some of them. This is due to reasons such as the complexity of patching, the requirement of system isolation during patching, and the lack of built-in support in IoT devices for patching.

To manage the scale and complexity of this task, it is de- sirable to design and implement a framework to continuously monitor the security of different components and subsystems and apply necessary patching automatically. This aims to reduce the vulnerabilities and attack surfaces with minimum human intervention, while maintaining the expected function- ality and performance of the system. Accomplishing security automation and orchestration for IoT systems is complicated, because of (i) the number of components involved (both software and hardware), (ii) the variety of components, and (iii) the number of semi-trusted/untrusted parties involved such as subcontractors, resellers, and solution providers.

We have seen an explosion of literature in IoT security including surveys and tutorials in many leading journals (e.g., [4], [5], [6], to list just a few). At the same time, automation and orchestration have gained a lot of momentum in industries, more specifically in Security Operations Centers (SOC). Re- cently, researchers have also started to look at the automation and orchestration of incident response plans [7]. To the best of our knowledge, none of the existing literature has been focused on automation and orchestration for securing IoT systems.

In this paper, we envision security automation and orches- tration for IoT systems. We start by providing the definitions of automation and orchestration, and clarifying the scope covered in this paper. After scanning the academic and industrial literature and conversations with industry partners, we envi- sion a framework integrating the key elements to accomplish security automation and orchestration for IoT systems. These key elements are identified according to the common themes in the surveyed literature (see the search criteria in Section II). They include threat modeling, security and privacy by design, trust management, security configuration, threat monitoring, patching, secure data sharing, and compliance checks. This initial categorization provides a framework for the analysis and design in security automation and orchestration for IoT systems. For each element, we study the current landscape by investigating the existing solutions. Based on our observations, we discuss the key challenges still impeding the fulfillment of each element. We discuss future directions for the devel- opment of each element to improve security automation and orchestration for IoT systems.

Overall, this paper aims to provide researchers and prac- titioners pointers for understanding the challenges and ad- vancements in security automation and orchestration for IoT systems, as well as significant future directions to motivate further academic research and industrial activities.
The rest of this paper is organized as follows. Section II presents the related work. Section III introduces definitions and scope. Section IV presents the definitions of elements, existing landscape, challenges, and future trends in security automation for IoT systems. Section V describes the definitions of security orchestration for IoT systems, existing landscape, challenges, and future directions. Section VI concludes the paper.

II. RELATED WORK

To identify the survey papers related to our vision paper, we first conduct a search of several popular scientific databases including IEEE Xplore, ACM Digital Library, and Google Scholar. In particular, we are looking for survey papers that match the following criterion: papers focusing on IoT security, IoT privacy, security automation, or security orchestration. Through a comprehensive search, we manage to divide the existing related survey papers into the following categories: (i) works on surveying general security, privacy, and trust issues in IoT (e.g., [8], [9]), (ii) works on surveying automation of information security management (e.g., [10], [11]), and (iii) works on surveying security orchestration in organizations and enterprises [7].

The first category focuses on identifying and analyzing the general challenges and solutions regarding security, privacy, and trust in IoT. In [8], Sicari et al. examine the issues in IoT regarding authentication, confidentiality, access control, privacy, trust, and secure middleware. In [9], Yang et al. inves- tigate the main limitations of IoT devices and corresponding solutions, present a classification of IoT attacks, and survey approaches to authentication and access control.

The second category focuses on examining the potential for security automation in information management systems. In [10], Montesino et al. discuss some common information security standards (like ISO/IEC 27001 and NIST SP800- 53) and analyze several security tools that have the poten- tial to automate the security controls of those standards. In [11], Kampanakis focuses on automated security-related information sharing among organizations and analyzes some popular information sharing models (e.g., the Security Content Automation Protocol developed by the NIST).

The third category, where little work has been done, focuses on surveying security orchestration platforms and solutions for deployment in organizations' IT infrastructure. Very recently, in [7], Islam et al. take the first step in exploring the challenges and opportunities for the evolution of security orchestration in organization environments, and analyze the characteristics, strengths, and weaknesses of existing technologies.

Through our comprehensive evaluation, we identify that none of the existing literature focuses on exploring security automation and orchestration for IoT systems. The paper aims to fill this gap.

III. DEFINITIONS AND SCOPE

A. Definitions

Many researchers and companies are using the terms secu- rity “automation” and “orchestration”. However, according to [12], orchestration often gets confused or lumped with security automation.

Automation is typically used for automating a manual task or process. Take an example of antivirus, firewall or incident response; they all have a common mission, which is to perform an automated action when any particular risk is raised based on a list of potentially known threats.

Orchestration is “the planning or coordination of the elements of a situation to produce a desired effect, especially surreptitiously”, as defined in the Oxford dictionary. In the computer security context, one of the widely accepted definitions has been presented by [13]: “Security orchestration represents the union of people, process and technology. It’s computer automation where it works and human coordination where that’s necessary”. In other words, automation is a step inside orchestration along with many others such as planning, integration and coordination.

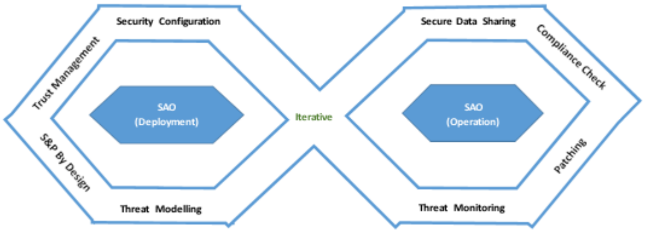

Fig. 1. The envisioned SAO framework: Security Automation and Orchestration for IoT systems. The elements on the left are related to the deployment of IoT systems, and on the right are related to the operation of IoT systems. The elements are across both IoT devices and data in IoT systems.

B. Scope

We envision a framework integrating the essential elements of Security Automation and Orchestration (SAO) for IoT sys- tems, as shown in Fig. 1. The SAO framework is specifically aimed at catering for complex and large-scale distributed IoT systems with resource-limited IoT devices (such as Arduino Due, Zolertial Re-Mote, IoT-LABM3, and Atmel SAM R21 [14]). It covers the key elements regarding both the deploy- ment and operation of IoT systems. In particular, regarding the deployment of IoT systems, we have identified the following elements: threat modeling (Section IV-A), security and privacy by design (Section IV-B), trust management (Section IV-C), and security configuration (Section IV-D). These elements together correspond to the workflow of modeling the poten- tial threats, designing adequate built-in security and privacy mechanisms, assessing the trustworthiness of IoT devices in specific deployed contexts, and configuring the IoT devices. Regarding the operation of IoT systems, we have identified the following elements: threat monitoring (Section IV-E), patching (Section IV-E), compliance check (Section IV-F), and secure data sharing (Section IV-G). These elements together correspond to the workflow of monitoring the threats and security issues, patching the discovered vulnerabilities, making alignment with security policies, regulations and legislation, and sharing generated data securely. Note that these elements run in an iterative process since the security status of IoT systems needs to be continuously monitored and maintained to ensure up-to-date security in practice. We are aware that IoT security is broad and our framework concentrates on the aspects regarding the security of networked IoT devices and IoT data. Other aspects like authentication, password security, network service security, and ecosystem interface security [15] are out of the scope.

IV. ELEMENTS, CHALLENGES AND FUTURE DIRECTIONS

In this section, we present the definition, existing landscape, challenges, and future directions of each element of the envisioned SAO framework in turn.

A. Automate Threat Modeling

Definition: Threat modeling refers to the process which proactively identifies potential security issues and vulnerabilities to IoT systems so that defense and mitigation mechanisms can be prioritized. Since IoT is an ecosystem rather than just embedded devices, threat modeling is a necessary process to understand all potential risks and analyze all possible security vulnerabilities across both data and physically controlled systems.

Existing Landscape: In general, existing works for automation of threat modeling for IoT systems can be divided into (i) non-adaptive threat modeling and (ii) adaptive threat modeling. Works in the first category [16], [17] mainly rely on theoretical methods like game theory and graph theory to model the potential threats and vulnerabilities regarding communication, computation, and control among IoT devices. Works in the second category [18], [19] focus on designing frameworks which can continuously evaluate the security using various security metrics, learn and adapt to dynamical environments in IoT systems, and identify and respond to unknown threats.

Challenges: Real-life IoT systems usually have large-scale deployment and operate in dynamic (devices may appear and disappear without any synchronization) and heterogeneous (in terms of hardware, software, functions, communication models, etc.) environments [20]. The resulting high uncertainty makes it quite challenging to do threat modeling directly on the deployed IoT system in such a situation.

Future Direction: One possible direction to overcome these challenges is to explore the possibility of creating a virtual simulation environment [21] that mimics the real deployment and operations of IoT systems, where threat modeling is then performed on the simulated IoT systems. Such a virtual simulation environment could enable IoT system designers to enumerate and test potential threats as well as efficiently investigate mitigation mechanisms against new emerging threats. There are some emerging platforms for simulating IoT systems with certain operating system-empowered IoT devices, e.g., the Cooja simulator [22] allows the networks of Contiki (a popular operating system tailored for IoT devices) motes to be simulated. It would be valuable to explore how to do threat modeling on these platforms, and how to properly build on them to do simulation and threat modeling on IoT systems comprised of large-scale smart devices with heterogeneous operating systems.

B. Security and Privacy by Design

Definition: Security and privacy should not be an afterthought. They should be built into the IoT systems. A system should be designed to be secure, rather than be modified in response to security attacks. In other words, as system designers, we have to be proactive, rather than reactive. One of the important principles is that the default behaviour of the system should be secure and private. There is always a trade-off between usability and security in the context of security, as well as privacy and utility in the context of privacy. The research challenge is to build IoT systems with usable security. This may need a human-centric approach in designing IoT systems. The IoT data should be managed and analysed in such a way that it preserves the privacy without having much impact on utility.

Existing Landscape: The book by Cavoukian and Chanliau [23] discusses at length about Privacy and Security by Design. Cavoukian [24] explains the 7 fundamental principles of Privacy by Design: user-centric, preventive (not remedial), privacy as the default setting, privacy embedded into the design, positive-sum (not zero-sum), full life cycle protection, and visibility and transparency. One of the most popular frameworks used to achieve privacy is five safes: safe projects, safe people, safe data, safe settings and safe outputs [25]. With regard to security, Microsoft Security Development Life-cycle (SDL) introduces security and privacy considerations throughout all phases of the development process, helping developers build highly secure software, address security compliance requirements, and reduce development costs. Open Web Application Security Project also proposes security by design principles which include principles of least privilege, secure defaults, minimize attack surface area, separation of duties, etc.

Challenges: The challenges in building a system with security and privacy by design is the complexity, unsafe behavior of users and unknown threats. Some of the principles defined for enterprise systems discussed above might not be directly applicable to IoT systems. What are the core security and privacy by design principles for IoT systems? How do we apply the five safes framework to IoT? Furthermore, security and privacy are inherently ephemeral in nature, as it is difficult to anticipate all types of future attacks. Hence, one would not be able to design a system to protect against all such unknown threats. We expect to have privacy and security drift in default settings as new threats emerge. The drift will create privacy and security debt in the IoT systems. Default security and privacy settings are not sufficient to secure future attacks.

Future Directions: The possible future directions include (i) design a new set of security and privacy by design princi- ples for IoT systems, (ii) develop a new mechanism to address security and privacy debt in an operational environment, and (iii) develop a new security and privacy framework for IoT Systems. One of the potential areas of research to address security and privacy debt is to develop an iterative and orchestrated approach to security and privacy by design, where the default security and privacy settings will be continuously monitored against emerging threats with a human in the loop.

C. Automate Trust Management

Definition: Trust management assesses the trustworthiness of data and services in IoT systems. In practice, due to various factors such as device faults, noises, interference, and cyber security attacks, the data and services from IoT applications could be prone to errors or even be false and misleading. Therefore, an automatic assessment of the trustworthiness is critical.

Existing Landscape: In the literature, researchers have made some attempts to deal with the data and service trustworthiness problem in IoT. Most of the existing solutions mainly rely on trust management mechanisms, which build trust models to estimate the trust level of smart objects engaging in the life cycle of data in IoT systems. The trust manage- ment mechanisms that have been proposed by researchers can be divided into five categories: recommendation-based techniques, prediction-based techniques, policy-based techniques, reputation-based techniques, and machine learning-based techniques.

1) Recommendation-based Techniques: These techniques require the existence of trusted parties and rely on their recommendations to evaluate the trustworthiness [26], [27]. These techniques can detect the misbehaving objects to make decisions on a safe routing path in the case that the objects do not have interactions before.

2) Prediction-based Techniques: These techniques run trustworthiness evaluation between the objects [28]. That is, each object evaluates the trustworthiness of other objects, to identify misbehaving objects. The prediction- based techniques are especially suited for the scenarios where new objects are introduced into an IoT system, so minimal knowledge about the new objects is available for use in trustworthiness evaluation. So, these tech- niques usually tend to rely on measuring the similarity of objects in terms of capabilities.

3) Policy-based Techniques: These techniques leverage pre-defined policies using mathematical modeling or natural language as constraints on the behavior of smart objects in the IoT systems [29], [30]. In particular, a set of rules is established (e.g., specifying trust thresholds for system access request and authorization), so as to give automatic responses to various events taking place in the IoT systems.

4) Reputation-based Techniques. These techniques leverage past observations and experiences to build trust [31], [32]. They produce a reputation score for each IoT object by allowing the IoT objects to rate the reputation of each other through the collection of feedback for each object and aggregation of the collected information in either a centralized or distributed manner.

5) Machine Learning-based Techniques: To effectively mine valuable insights from typically large-scale dis- tributed data in IoT applications, machine learning techniques are emerging and could be more advantageous compared with other previous trust management tech- niques. Existing solutions [33], [34] based on machine learning techniques generally formulate the trust eval- uation problem as a multi-class classification problem where the class labels include trustworthy, neutrally trusted, and untrustworthy. They collect multiple distinct factors from the IoT system, called trust features [34], and combine the trust features in different ways to predict the trust level of the IoT objects.

Challenges: IoT systems could operate in different environmental contexts with regard to time, location, activity, devices types, operational mode, etc. Some IoT objects trusted to perform a particular function in some context might become untrusted in other different contexts. Meanwhile, IoT systems could also work with varying user contexts. A general question here is: how the operation of an IoT device in the context of current user activity could affect the user's privacy? This is a general question arising from, e.g., smart-meters where work/living habits can be inferred. Therefore, the contextual information could have a crucial effect on data trustworthiness. It is especially challenging to conduct context-aware trust man- agement for distributed IoT applications where multiple trust domains exist and a centralized trust manager is not available. Besides, the behaviors of IoT objects are not immutable over time and their trust levels should be dynamically assessed and kept up to date to reflect the state of the IoT system.

Future Directions: Concerning context-aware trust management, the main task is an efficient context comparison. Namely, one would need to consider how to efficiently perform trust evaluation based on trustworthiness under similar context, and how to efficiently compare the trustworthiness under different contexts [35]. For dynamic trust management in IoT systems, an emerging trend is to devise trust decay functions, and use the dynamic weighting of trust features to perform trust updates on an event-driven basis [36].

D. Automate Security Configuration

Definition: IoT security configuration refers to setting the security-related functionalities of an IoT device based on a defined threat model, or making changes on the settings in response to identified security incidents (e.g., identification of misbehaving IoT devices in the network). Automating that means these functionalities can be configured remotely without human intervention.

Existing Landscape: Vendors of IoT devices have shifted towards producing flexible and general-purpose products to maximise their potential revenue. This results in including a broad range of possible configurations to match all deployment scenarios. This behaviour goes beyond hardware to widely affect software solutions as well. However, this flexibility puts a significant burden on enterprise IT administrators who must manually configure all these IoT devices to reduce the risk coming from the unwanted functionalities. Currently, these functionalities are configured before the device operating system image is compiled [37]. It is then transferred to the IoT device. This must be repeated every time security functionalities have to be updated. In turn, it makes managing the rapidly changing security requirements and configurations both expensive and complicated.

The threats of hacking those components are severe. They may result in stealing confidential information, data poisoning, Distributed Denial of Service attacks (DDoS) against enter- prise solutions, and many other attacks [9]. There are far more activities in the industry than the academic literature. Many commercial products are already introduced in the market to achieve automating the security configuration task. Examples include Puppet, Chef, Ansible and SaltStack. They automate the deployment process into various servers and computers [38]. However, they focus on enterprise and more powerful devices. In the IoT context, Azure IoT Hub [39] and Amazon IoT Device Management [40] recently introduced products to automate configuration deployment to IoT devices. Most of these products are one-way solutions which mean automating general configuration deployment but not designed for automating the security configuration based on agile threat model. Also, they are only a logistic bridge to components (hardware/software), and you still have to write manually what should be deployed.

Recently, many researchers are trying to solve automating the IoT security configuration problem by employing the Security Content Automation Protocol (SCAP) developed by NIST [41]. The focus of these efforts is automated security configurations for Routers or smartphones [42]. Most of the existing works are not in the IoT context and face the challenge of how far they could automate. An evaluation study in [10] demonstrated that as per NIST SP 800-53 protocol, 198 security features are recommended to be managed. Only 62 features can be automated without human intervention in most of these studies. How these features can be automated without human interference is still an unsolved problem. Chung et al.[37] proposed a promising technique for on-demand security configuration of IoT devices. It allows changing the security functionalities without recreating device images, but it has to be done manually. Recently, Yokogi et al. [43] have introduced a model to automate authentication of deployed IoT devices. Challenges: Due to the cost and time required to do a comprehensive field testing against various threat models, IoT devices are very likely to be deployed before they are thor- oughly configured and tested. In addition, owner organisations do not reconfigure these devices regularly, because of the vast number of components, the manual process that has to be fol- lowed, and their presence at unmanned sites. As a result, these devices are far more prone to vulnerabilities. The challenges for researchers is to come up with techniques that can not only automate the security configurations of heterogeneous devices, but also monitor and reconfigured against the past, present and future threats.

Future Directions: In the IoT context, device image recompilation and manual deployment hinder the frequent reconfiguration. Chung et al. [37] present a way to reuse the device image without recreation to update security functionalities.

This study can be expanded on heterogeneous IoT devices. Also, researchers may explore the automation mechanisms to deploy a similar model.

E. Automate Threat Monitoring and Patching

Note that the two elements have been combined together in this section.

Definition: IoT threat monitoring and patching are the processes of examining the IoT devices against various identified vulnerabilities and updating their images with up-to date patches. Automation requires that these two processes should be achieved automatically with minimum human intervention. Existing Landscape: A deployment of IoT system may contain hundreds of or much more IoT devices. Checking the health of all these devices in composite systems manually against possible threats or untrusted software’s is costly, time-consuming and very disruptive. Therefore, many organizations are obliged to be reactive rather than proactive in many hacking disasters such as Mirai [44] and IRCTelnet [45]. In other words, they only take actions after something wrong has happened. This is no longer acceptable in the era where those edge devices are fully integrated into enterprise systems with privileged access to a wide range of existing services.

The top 10 vulnerabilities for IoT devices are defined by the Open Web Application Security Project (OWASP) [15] in 2018. They include insecure network services, lack of secure update and patching mechanism, and lack of remote device management. This is due to several reasons such as limited computational power of IoT devices. Poorly implemented encryption in IoT devices, insecure third-party components, lack of secure patch delivery, and weak default settings. Many commercial products are trying to overcome these challenges such as PubNub [46] for IoT status tracking. They vary in their capability and coverage in terms of what they can check and do. However, they (i) mostly look for IoT devices status and transmitted packets rather than checking vulnerabilities and automate secure patching, and (ii) lack of flexible mecha- nisms that give enterprises more control over what should be considered abnormal or unhealthy based on their threat model. Existing literature has proposed mechanisms to identify some potential threats that exist in the contemporary IoT systems. These models can be divided into three broad categories as follows: 1) default password detection, 2) privacy disclosure analysis, and 3) anomaly detection [47], [48]. Despite the effectiveness of these models, they (i) only detect the threat but still do not solve the issue, and (ii) are narrow-focused rather than general models that consider the automation aspect in a large-scale setting. Recently, Princeton University researchers demonstrated a promising way that allows us to look at the above 3 threats together and solve them [49]. They run their algorithm on a Raspberry Pi in a smart home setting.

Challenges: The IoT security threats are far more than three discussed above as per the OWASP list. Many challenges remain to be addressed. There is a lack of IoT device management and system monitoring in production mode. There is also a lack of mechanism for secure delivery of patching and anti-rollback mechanisms. Since there are no physical hardening measures as highlighted by OWASP, this allows attackers to gain control, which renders IoT devices vulnerable to attacks. Future Directions: The automation of monitoring IoT systems against threats and patching them in native operat- ing environments is a critical step. There are a few works introduced to check only specific threats, but they have failed to consider the examination of IoT system under composite threats. Jonsdottir et al. [49] demonstrated a promising path that examines three risks and solves them. More research should be done to generalise such an approach to cover at least the top 10 threats identified by OWASP and address them by introducing automation in dynamic patching.

F. Automate Compliance Check

Definition: Compliance check refers to the status of the IoT systems and how far they are in alignment with the policies, regulations and legislation.

Existing Landscape: According to a recent survey by Bain.com [50], the most crucial barrier to IoT adoption is the lack of targeted security and privacy policies that ensure the compliance of IoT systems to standard regulations and legislation. Examples include compliance to password complexity, installed libraries, open ports, the way they collect data, and the types of data they are allowed to accumulate. There have been various IoT security guidelines proposed by different organisations as baselines. However, there are no global standards for which guidelines are suitable for which scenario. Also, there is no coordination between these guidelines. Recently, there are only a few commercial products such as Firmalazer [51] that try to address these gaps by introducing joint guidance. They automate the compliance process checking against a joint list in IoT systems. However, they are vendor dependent.

Challenges: The main problems that face automating the compliance checking are the lack of guidelines that checks the compliance of IoT systems against public policies such as HIPAA and GDPR. Also, the IoT space lacks standard regularisation entities which ensure allowing only certified IoT devices to be available in the market.

Future Directions: To have fully automated compliance checker, one would consider developing clear guidelines that should be followed to be in alignment with established policies such as GDPR. Besides, introducing standard entities that help in regulating the IoT devices would be a reasonable direction to enforce compliance. Another research direction is to code the policies, regulations and legislations in executable and verifiable forms so that the computer can automatically check them. Regulation Technologies (RegTech) have made some progress in this direction, but further research is needed in the context of IoT systems.

G. Automate Secure Data Sharing

Definition: Secure IoT data sharing refers to access control on encrypted IoT data so that only authorized entities are allowed to recover the original data. As IoT data are typically stored on the cloud, this means the enforcement of access control mechanisms over the encrypted IoT data on the cloud. Existing Landscape: In the literature, there are two key techniques that can support the sharing of encrypted data, including proxy re-encryption and attribute-based encryption.

1) Proxy Re-encryption. Proxy re-encryption (PRE) is a public key-based encryption technique [52] enabling a data owner to encrypt data to be shared under its own public key. The encrypted data can be later transformed by a semi-trusted third party, i.e., the cloud in the IoT

data sharing scenario, so that intended authorized data users can decrypt the encrypted data after transformation. Under the basic working paradigm of PRE, a lot of schemes have been proposed for secure data sharing, with focus on various aspects such as the multi-use feature where the transformed ciphertext can be further re-encrypted, the unidirectional feature where the intermediate proxy can only transform the data owner's decryption rights to data user's decryption rights on the same ciphertext but not vice versa, and the collusion-resistant feature where the proxy colludes with some data users cannot recover the data owner's private keys, user revocation [53], [54], [55], [56].

2) Attribute-based Encryption. In comparison with PRE, attribute-based encryption enables much more fine-grained access control through the use of attributes [57], [58]. The concept of ABE was originally proposed by Sahai and Waters [59]. In the initial ABE system, the keys and ciphertexts of a party are labeled with sets of attributes. The private key of a party can decrypt a ciphertext when there is a match of at least a pre-defined number of attributes between the key and the ciphertext. Later, two highly expressive and variants of ABE are proposed for more flexible access control, which are called Key-Policy ABE (ABE) [60] and Ciphertext-Policy ABE (CP-ABE) [61]. In KP-ABE, a data user is assigned with an access policy (usually defined as an access tree), while a data item is assigned a set of attributes. Each attribute in the system is associated with a public key component. To encrypt a data item, the data owner performs encryption using the corresponding public key components. The data user's private key is defined following the access policy so that the data user can decrypt a ciphertext if and only if the attributes of the ciphertext satisfies its access policy. For CP-ABE, the case is just reversed, where a ciphertext is associated with an access policy while a data user is assigned a set of attributes.

Challenges: Despite the feasibility provided by the above cryptographic techniques to enable secure sharing of IoT data through the cloud, challenges still remain. The first challenge is efficiency. Most of the existing solutions require expensive cryptographic operations like bilinear pairing operations or modular exponentiation operations, which might not be practically affordable on lightweight IoT devices. It is essential to develop lightweight cryptography that can be deployed on resource-constrained IoT devices to support secure data sharing. The second challenge is functionality. Most of the existing solutions only support access control on encrypted data, and no computation is allowed over the ciphertexts. However, in IoT applications, analytics usually have to be applied over the massive amounts of raw data so as to extract valuable information, like the use of machine learning algorithms. It would be much more desirable if computation could be allowed on the encrypted IoT data stored in the cloud while access control is enforced.

Future Directions: For the efficiency challenge, one might consider devising secure mechanisms for outsourcing the heavy cryptographic operations. There exist some works inves- tigating computation outsourcing for efficiency improvement [62], yet they mostly focus on the outsourcing of ABE's decryption operation for data users. This is not directly ap- plicable for IoT devices as they need to do encryption instead of decryption. It would be valuable to explore how to devise outsourcing mechanisms applicable for use on IoT devices, as well as suitable for not only ABE but also PRE. For enriching the functionality, one might consider having a co- design of access control mechanisms and secure computation techniques. For example, one could combine ABE with searchable encryption [63], [64] to support search over ABE-encrypted data [65]. There exist various techniques like secret sharing, homomorphic encryption, and garbled circuits [66], [67], [68]. They have different trade-offs in terms of bandwidth consumption, communication rounds, and computation. It is worthwhile to explore how to properly combine them with secure data sharing techniques to enrich the functionalities.

V. TOWARDS ORCHESTRATION OF THE SECURITY AUTOMATION ELEMENTS FOR IOT SYSTEMS

Definition: Security orchestration for IoT systems refers to the methodology and techniques that seamlessly connect and coordinate the security automation elements and security experts to establish a defense layer in depth for IoT systems. It could minimize the efforts from human experts, and enable cost-effective and fast decision making and responses. Besides, it could potentially streamline more menial tasks usually carried out by stretched and sometimes under-skilled teams.

Existing landscape: Most of the existing works on security orchestration are aimed at the traditional IT infrastructure of enterprises [7]. Security orchestration for IoT systems is more complicated than traditional IT systems due to a couple of factors. First, it is easier for attackers to identify exploitable vulnerabilities of IoT devices since they are often low cost and easily obtainable. Second, IoT devices are often deployed in unsupervised locations or even geographically remote regions (e.g., in satellite-based smart farming and smart mining applications), making it more difficult to have timely detection of the security incidents. Third, IoT systems could involve large-scale devices with limited battery and low bandwidth, making it more difficult to deploy security updates in a timely fashion. In the book [69], Sabella et al. study security orchestration for IoT. They focus on understanding the security in IoT networks, introducing the emerging network function virtualization (NFV) and software-defined networking (SDN) architectures. They also describe how to properly leverage these emerging network architectures to orchestrate the generic security services like identity, authentication, authorization, and virtualized network functions.

Challenges: Security orchestration for IoT systems need to integrate different security automation elements that are dispersed over heterogeneous components — low end IoT devices, fog devices, cloud, and human experts. These components are deployed in different environments and may face different kinds of threats and attacks. It is not easy to develop a single security orchestration solution that can simultaneously handle various types of threats and attacks across them.

Future Directions: One promising direction would be to consider the integration of security orchestration for enterprise environments with orchestration architecture designed for IoT applications. Some researches [70], [71] propose the concept of fog orchestrator which provides the centralized arrangement of the resource pool, maps applications with specific requests, and provides an automated workflow to physical resources. It would be interesting to explore the characteristics of such orchestration architecture design for IoT systems and consider adapting the security orchestration solutions originally designed for enterprise systems to make them work for IoT systems. In addition, one could explore the proper use of the power of advanced artificial intelligence (AI) technologies to investigate threats and guide response processes, so as to further reduce as much human intervention as possible, saving precious time of human experts. Other key areas of research include human-AI interactions in the context of IoT systems, IoT device discovery and composition.

VI. CONCLUSION

In this paper, we have envisioned the SAO framework which integrates the key elements for security automation and orches- tration for IoT systems, including threat modeling, security and privacy by design, trust management, security configuration, threat monitoring, patching, compliance check, and secure data sharing. For each element of the SAO framework, we identified the existing research challenges and major contributions that seek to address them, as well as highlighted the remaining challenges and opportunities for future research.

For future work, it would be valuable to explore more elements to be integrated into the SAO framework as well as investigate the development in other related areas like service-oriented computing with the orchestration of services to get inspirations for further advancing the SAO framework.

REFERENCES

[1] The Internet & Television Association (NCTA), “Behind The Num- bers: Growth in the Internet of Things,” https://www.ncta.com/whats- new/behind-the-numbers-growth-in-the-internet-of-things, [Online; ac- cessed 15-Nov-2019].

[2] DARPA, “Configuration security program to make network- connected systems less vulnerable,” https://www.darpa.mil/news-events/ 2018-01-09, 2018, [Online; accessed 10-Nov-2019].

[3] digitialjournal.com, “Beware: Security risks from cheap iot devices,” http://www.digitaljournal.com/tech-and-science/technology/ beware-security-risks-from-cheap-iot-devices/article/542373, 2019, [Online; accessed 10-Nov-2019].

[4] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, “Au- thentication protocols for internet of things: a comprehensive survey,” Security and Communication Networks, vol. 2017, pp. 6 562 953:1– 6 562 953:41, 2017.

[5] L. Maglaras, L. Shu, A. Maglaras, J. Jiang, H. Janicke, D. Katsaros, and T. J. Cruz, “Industrial internet of things (i2ot),” Mobile Networks and Applications, vol. 23, no. 4, pp. 806–808, 2018.

[6] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain technologies for the internet of things: Research issues and challenges,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2018.

[7] C. Islam, M. A. Babar, and S. Nepal, “A multi-vocal review of security orchestration,” ACM Computing Surveys, vol. 52, no. 2, pp. 37:1–37:45, 2019.

[8] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

[9] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in internet-of-things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[10] R. Montesino and S. Fenz, “Information security automation: how far can we go?” in Proc. of International Conference on Availability, Reliability and Security, 2011.

[11] P. Kampanakis, “Security automation and threat information-sharing options,” IEEE Security & Privacy, vol. 12, no. 5, pp. 42–51, 2014.

[12] Phantom Inc., “The shift to incident response au- tomation and orchestration,” https://go.phantom.us/ the-shift-to-incident-response-automation-and orchestration, 2019, [Online; accessed 10-Nov-2019].

[13] B. Schneier, “Security orchestration for an uncertain world security intelligence,” https://securityintelligence.com/ security-orchestration-for-an-uncertain-world/, March, 2017, [Online; accessed 10-Nov-2019].

[14] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, “A survey on resource management in iot operating systems,” IEEE Access, vol. 6, pp. 8459–8482, 2018.

[15] OWASP, “Owasp internet of things project,” https://www.owasp.org/ index.php/OWASP Internet of Things Project, 2018, [Online; accessed 10-Nov-2019].

[16] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, “A framework for automating security analysis of the internet of things,” J. Network and Computer Applications, vol. 83, pp. 12–27, 2017.

[17] G. George and S. M. Thampi, “A graph-based security framework for securing industrial iot networks from vulnerability exploitations,” IEEE Access, vol. 6, pp. 43 586–43 601, 2018.

[18] H. Abie and I. Balasingham, “Risk-based adaptive security for smart iot in ehealth,” in Proc. of International Conference on Body Area Networks, 2012.

[19] K. Habib and W. Leister, “Threats identification for the smart internet of things in ehealth and adaptive security countermeasures,” in Proc. of International Conference on New Technologies, Mobility and Security, 2015.

[20] U. Ozeer, X. Etchevers, L. Letondeur, F. Ottogalli, G. Salau¨n, and J. Vincent, “Resilience of stateful iot applications in a dynamic fog environment,” in Proc. of MobiQuitous, 2018.

[21] A. Huebner, C. Facchi, and H. Janicke, “Rifidi toolkit: Virtuality for testing rfid systems,” in Proc. of International Conference on Systems and Networks Communications, 2012.

[22] Opensourceforu.com, “Programming internet of things using contiki and cooja,” https://opensourceforu.com/2017/06/ programming-internet-things-using-contiki-cooja/, 2017, [Online; accessed 10-Nov-2019].

[23] O. O. of the Information, P. Commissioner, A. Cavoukian, and M. Chan- liau, Privacy and security by design: a convergence of paradigms. Information and Privacy Commissioner, Ontario, 2013.

[24] A. Cavoukian et al., “Privacy by design: The 7 foundational principles,” Information and Privacy Commissioner of Ontario, Canada, vol. 5, 2009.

[25] T. Desai, F. Ritchie, and R. Welpton, “Five safes: designing data access for research,” University of the West of England Economics Working Paper Series 1601, Bristol, Tech. Rep., 2016.

[26] I. Chen, F. Bao, and J. Guo, “Trust-based service management for social internet of things systems,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 6, pp. 684–696, 2016.

[27] J. Li, Y. Bai, N. Zaman, and V. C. M. Leung, “A decentralized trustworthy context and qos-aware service discovery framework for the internet of things,” IEEE Access, vol. 5, pp. 19 154–19 166, 2017.

[28] O. B. Abderrahim, M. H. Elhdhili, and L. Sa¨ıdane, “Tmcoi-siot: A trust management system based on communities of interest for the social internet of things,” in Proc. of International Wireless Communications and Mobile Computing Conference, 2017.

[29] H. Al-Hamadi and I. Chen, “Trust-based decision making for health iot systems,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1408–1419, 2017.

[30] W. Li, H. Song, and F. Zeng, “Policy-based secure and trustworthy sensing for internet of things in smart cities,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 716–723, 2018.

[31] H. Xiao, N. Sidhu, and B. Christianson, “Guarantor and reputation based trust model for social internet of things,” in Proc. of International Wireless Communications and Mobile Computing Conference, 2015, pp. 600–605.

[32] B. Bordel, R. Alcarria, D. M. de Andre´s, and I. You, “Securing internet- of-things systems through implicit and explicit reputation models,” IEEE Access, vol. 6, pp. 47 472–47 488, 2018.

[33] U. Jayasinghe, G. M. Lee, T. Um, and Q. Shi, “Machine learning based trust computational model for iot services,” IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 39–52, 2019.

[34] P. Abeysekara, H. Dong, and A. K. Qin, “Machine learning-driven trust prediction for mec-based iot services,” in Proc. of IEEE ICWS, 2019.

[35] N. Li, V. Varadharajan, and S. Nepal, “Context-aware trust management system for iot applications with multiple domains,” in Proc. of IEEE ICDCS, 2019, pp. 1138–1148.

[36] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A´ . MacDermott, and X. Wang, “CTRUST: A dynamic trust model for collaborative applications in the internet of things,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5432–5445, 2019.

[37] B. Chung, J. Kim, and Y. Jeon, “On-demand security configuration for iot devices,” in Proc. of International Conference on Information and Communication Technology Convergence, 2016.

[38] Marco Bravo, “Top 5 configuration management tools,” https:// opensource.com/article/18/12/configuration-management-tools, [Online; accessed 10-Nov-2019].

[39] Microsoft Azure, “Iot hub,” https://azure.microsoft.com/en-us/services/ iot-hub/, [Online; accessed 10-Nov-2019].

[40] Amazon, “Iot device management,” https://aws.amazon.com/ iot-device-management/, [Online; accessed 10-Nov-2019].

[41] S. Radack and R. Kuhn, “Managing security: The security content automation protocol,” IT professional, vol. 13, no. 1, pp. 9–11, 2011.

[42] C.-L. Kuo and C.-H. Yang, “Security design for configuration manage- ment of android devices,” in Proc. of IEEE COMPSAC, 2015.

[43] K. Yokogi, N. Kitagawa, and N. Yamai, “Access control model for iot environment including automated configuration,” in Proc. of IEEE COMPSAC, 2018.

[44] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis et al., “Understanding the mirai botnet,” in Proc. of USENIX Security Symposium, 2017.

[45] S. Khandelwal, “New iot botnet malware discovered; infect- ing more devices worldwide,” https://thehackernews.com/2016/10/ linux-irc-iot-botnet.html, 2016, [Online; accessed 10-Nov-2019].

[46] PubNub, “Iot device control,” https://https://www.pubnub.com/solutions/ iot/, [Online; accessed 10-Nov-2019].

[47] N. Apthorpe, D. Reisman, and N. Feamster, “A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic,” arXiv preprint arXiv:1705.06805, 2017.

[48] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breiten- bacher, and Y. Elovici, “N-baiot—network-based detection of iot botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.

[49] G. Jonsdottir, D. Wood, and R. Doshi, “Iot network monitor,” in Proc. of IEEE MIT Undergraduate Research Technology Conference, 2017.

[50] Bain.com, “Unlocking opportunities in the in- ternet of things,” https://www.bain.com/insights/ unlocking-opportunities-in-the-internet-of-things/, 2018, [Online; accessed 10-Nov-2019].

[51] firmalyzer.com, “Iot device security compliance check,” https://firmalyzer.com/services/, 2019, [Online; accessed 10-Nov-2019].

[52] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.

[53] J. Shao and Z. Cao, “Multi-use unidirectional identity-based proxy re- encryption from hierarchical identity-based encryption,” Inf. Sci., vol. 206, pp. 83–95, 2012.

[54] Y. Cai and X. Liu, “A multi-use cca-secure proxy re-encryption scheme,” in Proc. of IEEE International Conference on Dependable, Autonomic and Secure Computing, 2014.

[55] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, “An efficient cloud- based revocable identity-based proxy re-encryption scheme for public clouds data sharing,” in Proc. of ESORICS, 2014.

[56] J. Lai, Z. Huang, M. H. Au, and X. Mao, “Constant-size cca-secure multi-hop unidirectional proxy re-encryption from indistinguishability obfuscation,” in Proc. of ACISP, 2018.

[57] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. of IEEE INFOCOM, 2010.

[58] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure shar- ing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[59] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. of EUROCRYPT, 2005.

[60] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryp- tion for fine-grained access control of encrypted data,” in Proc. of ACM CCS, 2006, pp. 89–98.

[61] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute- based encryption,” in Proc. of IEEE S&P, 2007.

[62] Z. Liu, Z. L. Jiang, X. Wang, and S. Yiu, “Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating,” J. Network and Computer Applications, vol. 108, pp. 112– 123, 2018.

[63] J. Zhu, Q. Li, C. Wang, X. Yuan, Q. Wang, and K. Ren, “Enabling generic, verifiable, and secure data search in cloud services,” IEEE Trans. Parallel Distrib. Syst., vol. 29, no. 8, pp. 1721–1735, 2018.

[64] X. Yuan, X. Wang, C. Wang, A. C. Squicciarini, and K. Ren, “Towards privacy-preserving and practical image-centric social discovery,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 868–882, 2018.

[65] J. Li, X. Lin, Y. Zhang, and J. Han, “KSF-OABE: outsourced attribute- based encryption with keyword search function for cloud storage,” IEEE Trans. Services Computing, vol. 10, no. 5, pp. 715–725, 2017.

[66] Z. Shan, K. Ren, M. Blanton, and C. Wang, “Practical secure compu- tation outsourcing: A survey,” ACM Computing Surveys, vol. 51, no. 2, pp. 31:1–31:40, 2018.

[67] Y. Zheng, H. Duan, and C. Wang, “Learning the truth privately and con- fidently: Encrypted confidence-aware truth discovery in mobile crowd- sensing,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2475–2489, 2018.

[68] Y. Zheng, H. Duan, X. Yuan, and C. Wang, “Privacy-aware and effi- cient mobile crowdsensing with truth discovery,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 1, pp. 121–133, 2020.

[69] A. Sabella, R. Irons-Mclean, and M. Yannuzzi, in Orchestrating and Automating Security for the Internet of Things. Pearson Higher Ed USA, 2018.

[70] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, “Fog orchestration for internet of things services,” IEEE Internet Computing, vol. 21, no. 2, pp. 16–24, 2017.

[71] A. Viejo and D. Sa´nchez, “Secure and privacy-preserving orchestration and delivery of fog-enabled iot services,” Ad Hoc Networks, vol. 82, pp. 113–125, 2019.