IoTSM: An End-to-end Security Model for IoT Ecosystems

Joseph Bugeja, Bahtijar Vogel, Andreas Jacobsson
Internet of Things and People Research Center and Department of Computer Science
Malmö University
Malmö, Sweden
{joseph.bugeja, bahtijar.vogel, andreas.jacobsson}@mau.se

Rimpu Varshney
Department of Security & Enterprise
Sony Mobile Communications
Lund, Sweden
rimpu.varshney@sony.com

Abstract—**The Internet of Things (IoT) market is growing rapidly, allowing continuous evolution of new technologies. Alongside this development, most IoT devices are easy to compromise, as security is often not a prioritized characteristic. This paper proposes a novel IoT Security Model (IoTSM) that can be used by organizations to formulate and implement a strategy for developing end-to-end IoT security. IoTSM is grounded by the Software Assurance Maturity Model (SAMM) framework, however it expands it with new security practices and empirical data gathered from IoT practitioners. Moreover, we generalize the model into a conceptual framework. This approach allows the formal analysis for security in general and evaluates an organization's security practices. Overall, our proposed approach can help researchers, practitioners, and IoT organizations, to discourse about IoT security from an end-to-end perspective.**

Keywords—IoT, end-to-end security, security model, secure development.

I. INTRODUCTION

With surveys estimating that by 2020 there will be over 20 billion Internet of Things (IoT) devices [1] and a projected global market size of about $457B by 2020 [2], IoT products are widely being deployed and enabling the creation of new applications. These applications span from domestic scenarios such as smart homes to industry scenarios such as smart manufacturing processes. To reach such a level of diffuse and influence, and due to the tight coupling with the physical realm, IoT technologies should be secure-by-design [3]. This means that security should be considered as a core system-level property and taken into the account in the actual design of architectures and approaches for IoT solutions [4]. Nonetheless, even though the technology has been widely adopted, a thorough IoT security pattern still has not been properly discussed to ensure further growth in an increasingly sophisticated threat landscape.

In recent years, we have witnessed a surge of attacks ranging from those targeting individual users, e.g., by exploiting video baby monitors inside smart homes, to nation-wide attacks, e.g., those triggered by IoT botnets [5]. While these cyberattacks have contributed to raising IoT risk awareness, insecure devices are still being released to the market leading to privacy violations, monetary costs, and sometimes loss of life. Part of this problem is that manufacturers rush to deliver innovative devices that attract consumers and dominate the market in advance, but lack security as a core functional requirement. Another factor is that security is new to many manufacturers operating in the IoT domain [6]. Indeed, many IoT product developers never had to deal with security, especially cybersecurity, concerns before. This is as their products were mostly physical devices installed with constrained interfaces, e.g., digital control panels on the actual devices, and were mostly not Internet-connected. Thus, manufacturers may lack the expertise and resources required to develop products in a secure manner.

A way to improve IoT product security is to incorporate security into the actual software development lifecycle leading towards a Secure Software Development Life Cycle (SSDLC). SSDLC methodologies could help avoid costly design flaws and increase the long-term viability of software projects. However, implementing SSDLC processes is oftentimes a challenging task as IoT is evolving at a fast pace and companies lack visibility over which processes are used by actual IoT practitioners. Exacerbating this is the fact that existing security practices require changes in order to be applicable for the IoT [7]. Nevertheless, there is a shortage of end-to-end comprehensive standards and reference architectures that can help secure IoT development [8]. With this, different vendors tend to favor their own IoT approaches for incorporating security. This results in the creation of vertical models that apply to the particular company needs but leaving out gaps that can be the target of security attacks. Moreover, security is not only a technical problem, but it should be implemented as a combination of processes, technology, and people [9]. These issues specifically emphasize the human-in-the-loop aspect, an important security characteristic for the IoT field.

Given the above challenges, in this paper we leverage the first-hand experience of different IoT security experts in tandem with existing literature on IoT and secure development to propose a novel IoT Security Model (IoTSM). This model can be used by IoT organizations to formulate and implement a strategy for developing end-to-end IoT security. The presented model is grounded by the SAMM framework, however we expand it with new security practices and empirical data gathered from IoT practitioners. SAMM is a framework designed to help organizations formulate a strategy for software security, and as a self-assessment test to get an overview on IT security processes within an organization [10]. Our proposed IoTSM is generalized into a preliminary conceptual framework that can be used for conducting formal security analysis. Overall, our proposed approach can help researchers, practitioners, and IoT organizations, to discourse about IoT security from an end-to-end perspective.

The remainder of this paper is organized as follows. Section II delineates the IoT characteristics. Next, in Section III, we summarize the relevant research. Based on that, we introduce the research methodology in Section IV. Then, in Section V, we introduce the IoT security model. In Section VI, we generalize the proposed model into a formal model and apply it in a use-

978-1-5386-9151-9/19/$31.00 ©2019 IEEE

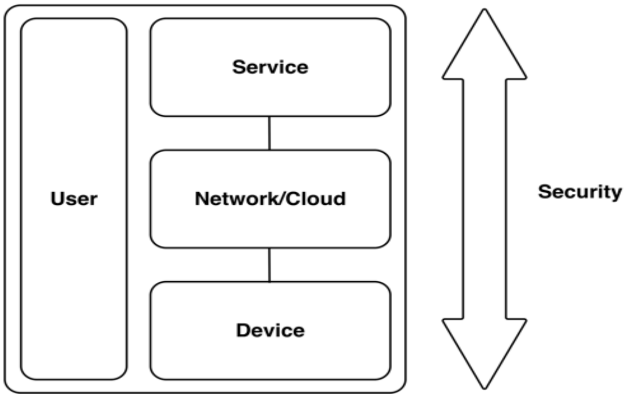

Fig 1. High-level IoT architecture with security representing a cross-sectional aspect.

case in Section VII. Finally, in Section VIII, we reflect on our contributions before concluding the paper and identify avenues for future work in Section IX.

II. IoT Characteristics

The IoT is commonly described as a dynamic global network infrastructure with self-configuring capabilities, based on standard and interoperable communication protocols [11]. IoT ecosystems involve heterogeneous devices and services, constrained resources, deal with highly personal data, and are likely to form a highly dynamic environment, which makes control hard. Furthermore, they may involve artificial intelligence aspects, making smart objects able to autonomously react to different situations, in order to minimize human intervention [3].

Key components comprising such a system include: network, device, service, cloud, and user [12] [13] as depicted in Figure 1. Network represents the communication infrastructure and supporting protocols allowing for the interaction among the devices and users. Devices are hardware entities that provide sensing, actuation, control, and monitoring capabilities. Typically, these devices are Internet-connected, uniquely identifiable, and may have the capability to communicate autonomously over a network, including the Internet. Services represent the software applications that the IoT system provides. Cloud acts as a relay between devices and services, and can also provide storage, data processing, and data analytics capabilities often contributing for the smartness of IoT applications. Users represents the stakeholders of the IoT ecosystem.

In designing IoT ecosystems, security represents an enabling technology that must span across all the mentioned components.

III. Related Work

To improve the security of software applications, several security methodologies and models have been proposed across the years [14] [15] [16]. Some of the most cited ones are identified hereunder.

The Microsoft Security Development Lifecycle (MSSDL) [17] is a software development process designed to reduce software maintenance costs and increase reliability of software concerning security related bugs. This model is used internally by Microsoft, e.g., for Vista project, and it is mostly intended for large organizations especially as it is considered more heavyweight and rigorous [18].

Similar to MSSDL, the Comprehensive, Lightweight Application Security Process (CLASP) [19] defines an extensive set of activities covering a broad spectrum of the development lifecycle with security being at the center stage. Different to MSSDL, CLASP is more lightweight making it more suitable for organizations with less strict security demands [18]. Recently, the CLASP project has been superseded by the SAMM.

The SAMM [10] is an open project designed to help organizations formulate and implement a strategy for application security to the specific business risks. This framework provides a way to assess and quantify the security activities (maturity) of organizations. It is a prescriptive model that is put together by different experts based on their experience and that can be tailored according to the specific risk environment each organization faces. This latest version of the model (version 1.5) has 12 core security practices grouped under four categories: governance, construction, verification, and operations.

Similar to SAMM, the Building Security In Maturity Model (BSIMM) [20] measures which software security activities are included in an organization’s overall SSDLC; and thus also provides a way to assess the maturity of organizations. BSIMM has 12 main activities divided into 4 domains: governance, intelligence, secure software development lifecycle touchpoints, and deployment. Different to SAMM, BSIMM is based on empirical data created by observing and analyzing real-world data from leading technical companies; and it is a descriptive model. The latest version of BSIMM – BSIMMv9 – includes 120 firms with 16 of them being IoT firms.

The identified frameworks have a broad focus representing activities that are common across traditional software companies. Nonetheless, we observe that the security practices identified therein tend to incline more towards the development of secure web applications. While most of the practices remain valid as well for IoT ecosystems, we believe it brings additional complexities and challenges into the security processes having in mind that IoT is the most evolving domain. First, an IoT product may range from an embedded device to a web-based user-interface. Second, IoT applications tend to utilize cloud resources more extensively than web applications. Third, IoT technologies often deal with highly personal data to a greater extent than a typical software application.

Similar to the approach followed by BSIMM [21], we leverage SAMM to create a security model by grouping different security practices relevant for IoT. However, different from BSIMM we focus on IoT firms, and utilize both first-hand data gathered from IoT practitioners and scholarly literature.

IV. Research Method

The adopted research method utilized a mixed-method research design leveraging both interview and literature data to yield a comprehensive perspective on IoT security.

A. Literature survey

Study selection involved a search for literature sources and then iteration of screening and filtering. The search was conducted in October 2018 using Google Scholar as a primary database. Here, peer-reviewed articles focusing on IoT security were collected and analyzed. These were retrieved by searching for a combination of keywords such as: "IoT", "CPS", and "security"; and included both scholarly literature and industry technical reports. Excluded results were related to studies predating 2000, non-English texts, and articles specifically focusing on privacy and trust, that are considered out-of-scope for this paper. Kept studies lay the groundwork for the devised IoT security model.

B. Interview process

To investigate the perspectives of IoT practitioners, qualitative one-to-one, in-person, semi-structured interviews took place with six industry experts located in the southern part of Sweden in June 2018. The participants were working at companies that offer IoT solutions such as IoT devices, cloud-based services, and security solutions, occupying roles as per Table I. The interview questions and their answers are detailed in [22]. Main questions covered topics including, but were not limited to, IoT security mechanisms, technical constraints, and operational challenges.

C. Data analysis and synthesis

To analyze the collected data, interviews were transcribed to text and coded. Emerging themes were grouped and developed inspired by the categories and descriptions observed in previous studies (e.g., [20] [23] [24]) identified in the literature survey. Results are summarized in the model presented in Section V.

V. IoT Security Model (IoTSM)

In this section, we describe the IoT Security Model. Motivated by SAMM, we group the security practices under four dimensions: governance, construction, verification, and operations. These dimensions cover the main activities tied to any organization performing software development.

A. Governance

Governance is related to how an organization manages overall the software development activities. Key practices identified here include:

Security education and awareness: The user is the most vulnerable element in IoT security [13]. Even if information system are implemented securely, if a user, is careless in managing security it will not be effective. For example, in a password-based authentication mechanism, if a user makes the password a guessable passphrase, attackers could easily extract the password. Key here, is to educate both the end-user as the consumer of the IoT system but developers as well should be trained on roles related to securing IoT devices and on typical attack patterns for exposed IoT devices. Especially, it was noted by P4 that there is an overall lack of security awareness, example when it comes to specific practices, e.g., threat modeling, and that some organizations, especially IoT startups simply ignore security. The importance of having the right security mindset when designing IoT systems was emphasized by the majority of the respondents.

Regulations and compliance: When dealing with IoT regulatory and compliance challenges are likely to grow in their importance. For instance, some devices may not only track fitness levels but may potentially infer more sensitive data regarding health information. This raises the need for independent security audits to be performed. Concurrently, this adds the importance of regulations e.g., the Health Insurance Portability and Accountability Act[1] when it comes to dealing with patient health data. More generally, compliance with privacy and data security are key. Example, the EU General Data Protection Regulation (GDPR)[2] is important for devices to comply to especially if devices are to be sold/used in the EU. The importance and implication of GDPR were emphasized by P1 especially when sending private data about the user, and as a driver to open the system to new functionality, e.g., the erasure of personal data. At the same time, as noted by P1, the same regulations, could stop IoT product engineers from amending or increasing the functionality of a system.

Security-by-design processes and standards: Companies should embed security into their devices at the outset, rather than as an afterthought. As part of the security-by-design process, companies should example consider: conducting a privacy or security risk assessment; minimizing the data they collect and retain; and testing their security measures before launching their products [25]. Nonetheless, standards that can help in doing so when it comes to IoT are not mature, leaving the market open to competing platforms and resulting in increased complexity which can introduce vulnerabilities. Here, respondents agreed on the need to follow standardized approaches however they observed how the existing market is fragmented, with P6 saying that "there are more than 600 different protocols in IoT" and that adds to the difficulty when it comes to developing security.

B. Construction

Construction deals with how an organization defines its goals and develops software. Core practices identified here include:

Continuous and automated risk assessment: Risk assessment is generally understood as the process of identifying, estimating, and prioritizing risks to an organization's resources. This is a critical activity in risk management since it provides the foundation for mitigating the identified risks. Examples of well-regarded approaches include: NIST SP800-30, ISO/IEC 27001, and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [26]. When it comes to the IoT, given the dynamic and evolving nature of stakeholders and technologies, it is ideal if it is performed continuously and in an

TABLE I. Participant roles and their corresponding organization function.

ID	Participant role	Organization function
P1	Security architect	Mobile communications
P2	Senior IoT architect	IoT solutions
P3	Technology leader	Industry automation
P4	Technology expert	Home security
P5	Security coach	Home surveillance
P6	Security expert	Data security

[1] https://www.hhs.gov/hipaa/index.html [accessed January 11, 2019].

[2] https://eugdpr.org [accessed January 11, 2019].

automated manner [26]. P5 emphasis the benefit of risk assessment in particular for prioritizing IoT security work and henceforth as a method for allocating resources effectively.

Data and application threat modeling*:* Threat modeling is a structured approach for analyzing the security of an application [27]. Threat modeling approaches are broadly divided into two approaches: attack tree-based approaches and stochastic model-based approaches, with the former representing possible attacks in a system in a tree structure, while the latter commonly converting system models to Markov chains and analyzing them using state transition matrices [27]. Threat modeling, including its application to data, is important as a method to systematically identify and categorize security-related threats that are most likely to affect the system under consideration. P5 and P6 both emphasize the importance of threat modeling as an approach to better understand the risks and to facilitate risk assessment.

Security requirements and architecture: Security requirements and architecture involve the specifications and the adoption of principles for the creation of secure functionality. Some of the IoT high-level requirements are derived by [6] [12] [13] [28] and were identified by different respondents are:

- *Physical/device security:* Ensuring that the hardware provides the required security features, e.g., encryption of firmware updates, and possibly anti-tamper and tamper detection features.
- *Network/cloud security:* Provide the appropriate level of identification, privacy preservability, and integrity to network communication. This also involves trust management, especially as IoT devices may communicate autonomously over the network.
- *Service security:* Selecting and implementing suitable technological platforms and supporting technologies that provide a robust and layered environment upon which to build the solutions easily and quickly.
- *Data security*: Identifying and managing data and its lifecycle are core especially for safeguarding end-user privacy. Especially, fine-grained and context-based access control mechanisms, authentication, and end-to-end data protection are key to ensure that only authorized individuals can access the data of a customer.
- *Logging and auditability:* Robust logging and auditing information from low-level and high-level software components which facilitate investigation of misuse. This is especially important in order to investigate attacks in an effective manner. Furthermore, providing a complete audit log of transformations made to data helps in implementing data provenance which is useful to provide data integrity.
- *Resilience:* IoT systems need to display resilience against failures and robustness against attacks and thus sustaining availability under desired levels as well.

C. Verification

Verification is focused on the activities related to how an organization tests its artifacts likes source code and design documentation. Central practices identified here include:

Artifact review: Security focused design and code reviews assist in the early vulnerability discovery and related mitigation activities. Reviews could be based on lightweight checklists and for efficiency could be performed on the most sensitive or security impacting segments [10]. These can include for instance, the boot process, security enforcement, mitigations, and similar, especially for logic issues that are difficult to detect with software tools. P5 emphasized the need for code reviews alongside with architecture reviews as a means to build secure software and to embed quality into development.

Security testing: Security testing is focused on inspecting the software in order to discover vulnerabilities. Here, penetration testing and high-level functional test cases could be used, e.g., to detect test interfaces and weak configurations that could lead to compromise. A combination of computerized scripts and penetration tools were used by Vijay et al. [29] to assess the safety and security performance of diverse IoT devices ranging from cameras, motion sensors, medical devices, and so on. P1 further hinted on the need for security penetration testing before purchasing an IoT product and P5 especially identified the need for automated testing for improving the quality and security of IoT systems.

D. Operations

Operations involves processes that are related to how an organization releases products to end-users, including operating in the actual (runtime) environment. Key practices identified here include:

Secure operation and maintenance: The IoT system should be kept updated for new vulnerabilities and in order to operate securely. Especially, an updating mechanism and process, preferably an automatic one, should be in place, freeing users from having to manually update systems. Furthermore, such updates should be delivered over a secure channel and verified (e.g., through code signing) to avoid malicious updates. Furthermore, P1 and P6, add the need to have such patches in an IoT system delivered timely to avoid exposing the consumer to extra risks.

Secure configuration and (de-)installation: The IoT should be configured and installed securely. Especially, the interfaces should be segregated and isolated properly. Example, administrative interfaces should be separate from those of non-privileged users. Likewise, there should be proper segregation and protection of communications channels to reduce the attack surface and enforce the principle of least privilege. It is also important to configure the system in such a way to cater for the digital divide that exists among the users, especially for those that are not well-versed with security [30]. Furthermore, the IoT system should provide for the secure deletion and revocation of data stored and processed by devices including associated cloud services [28]. Likewise, decommissioning IoT devices is just as important in order to protect sensitive data from getting into the wrong hands.

Continuous monitoring and auditing: Companies should monitor their products throughout the entire lifecycle. This can be done through technologies such as Intrusion Detection Systems, but also through products that test the entire infrastructure of the IoT applications against attacks and vulnerabilities [31].

TABLE II – COMPARISON OF THE IMPLEMENTATION OF THE DEVISED IOT SECURITY PRACTICES IN DIFFERENT SECURITY FRAMEWORKS.

Security practice	IoTSM	SAMM	BSIMM	CLASP	MSSDL
Security education and awareness	●	●	●	●	●
Regulations and compliance	●	●	●	–	–
Security-by-design processes and standards	●	●	●	●	●
Continuous and automated risk assessment	●	–	–	–	–
Data and application threat modeling	●	◗	◗	◗	◗
Security requirements and architecture	●	◗	◗	◗	◗
Artifact review	●	●	●	●	●
Security testing	●	●	●	●	●
Secure operation and maintenance	●	●	●	◗	◗
Secure configuration and (de-)installation	●	◗	◗	–	◗
Continuous monitoring and auditing	●	–	–	–	–

In conjunction with continuous monitoring, regular audits and analysis of log and event data can help to detect intrusions or attack attempts within the IoT environment. The key control to focus on here is logging at all layers within and surrounding the IoT ecosystem. P3 identified the importance of security audits especially given the financial penalties associated with data-breaches; and P6 stressed the need for a "continuous process" especially with regards to vulnerability patching.

VI. TOWARDS A FORMAL IOT SECURITY MATURITY MODEL

In this section, we generalize the proposed model described in Section V into an IoT security maturity model. An IoT security maturity model M is a tuple (b,C,p,f_p). The components of M are:

- b: finite set of utilized business functions. The set of possible business functions is represented by *B={governance, construction, verification, operations}*
- C: finite set of IoT components. This is represented as *C={service, network, cloud, device, user}*
- p: finite set of adopted security practices (e.g., security testing). Each practice, has a corresponding maturity score, m, where $m \geqslant 0$, indicating the level of expertise the organization has in implementing it, and a set of target IoT components, c, where $c \subseteq C$
- f_p: The organization security posture. This is represented as a function $f_p : p \times b \rightarrow s$

Using the above we can derive a new property – *end-to-end IoT security (e2e)* – representing the overall maturity of an IoT company. A company has *e2e*, if $|s| > 0$, $B - b = ø$, and there exists a p with $m > 0$, for each $c \in C$.

If we assume a common scheme for m, e.g., with m ranging from a value of 1 representing the lowest expertise to a value of 3 representing the highest, then we can qualify the above metric. For instance, we can have the metrics: high-, medium-, and low-e2e, if the ceiling of the overall average of m, i.e., $\lceil m \rceil$, is 3, 2, and 1, respectively.

VII. SMART HOME VENDOR USE-CASE

To apply the proposed formal model, let us assume a simple use-case consisting of two smart home vendors, v_1 and v_2. Both vendors cover the entire IoT ecosystem, i.e., services, users, network, cloud, and devices, with security practices and meeting the e2e requirements.

For simplicity, let us assume that v_1 offers advanced security education (e.g., sending monthly awareness emails) and advanced password management features (e.g., supporting two-factor authentication). These security practices are denoted as p_1 and p_2, respectively. In terms of v_2, we assume it offers low security education to its staff (denoted as p_3) but offers advanced password management controls (denoted as p_4).

Given the above, we can represent the security practices of v_1 as $p=\{p_1,p_2\}$ and that of v_2 as $p=\{p_3,p_4\}$. If we assume that both p_1 and p_2 have a corresponding maturity score of 3, then v_1 has a high-e2e. On the other hand, if p_3 has a maturity score of 1, but p_4 with a maturity score of 3, then v_2 has a medium-e2e. This means that more maturity; a possible indicator of vendor trustworthiness; may be put in v_1 than in v_2.

Additionally, we can compare the coverage of the individual security practices by inspecting the IoT components being targeted by each. For instance, if p_2 has *c={cloud,user}* whereas p_4 includes *c={cloud,user,device}*, then we can argue that v_2 password security controls offer a broader coverage than that of v_1. This may indicate that the vendor prioritizes the importance of good password management.

VIII. DISCUSSION

To substantiate the novelty of our proposed IoTSM, we compare it to the frameworks identified in Section III. The results are summarized in Table II. Here, our identified security practices are represented as (full (●), partly (◗), or none (–)) indicating the extent to which the specified measure has been implemented in the given framework.

We observe that the security practice of "continuous and automated risk assessment" and "continuous monitoring and auditing" have not been incorporated in the reviewed frameworks in comparing to our proposed IoTSM. Possibly, this is as such practices were not as important for traditional software applications and as more research effort is needed in implementing them. Moreover, we note that some practices have only been partially implemented in reviewed frameworks. In particular, the application of threat modeling in relation to data. Possibly, because this practice is mostly related to privacy-preservation and not explicitly security. Another aspect is connected to security requirements. Although all frameworks identify this practice, they miss specific IoT aspects, e.g., the requirements for resilience, cloud security, and data security. Such requirements make us reflect on the complexity and new challenges involved to effectively secure IoT applications with our proposed IoTSM from an end-to-end perspective.

A limitation of our model is the number of subjects interviewed (*n=6*) and that these only included companies that are located in the south of Sweden. A side-effect of this is that it is difficult to generalize our findings and to validate example if the business functions completely cover all necessary aspects. However, this is being controlled as the proposed security model draws in tandem with interview data also from established literature sources to establish its foundation. Another limitation concerns the security metrics proposed to measure end-to-end security. Instead of arithmetic average, other complementary measures could be adopted and evaluated to include a more balanced view of maturity. For instance, using a weighted average as indicated in [32] or a harmonic mean.

IX. Conclusions and Future Work

The IoT technologies are advancing rapidly allowing for the introduction of new applications ranging from domestic to industrial scenarios. Concurrently, various IoT vendors lack insights into what is required to develop an end-to-end secure product.

In this paper, we proposed a novel IoT Security Model (IoTSM) that can be used by organizations to plan a strategy and discourse about IoT security from an end-to-end perspective. The model was devised using scholarly literature alongside with empirical data gathered from IoT practitioners. Additionally, we proposed a conceptual framework that can be used to formally analyze, describe, and measure the overall security posture and level of expertise of an IoT organization.

For future work, it would be beneficial to conduct further interviews with a broader sample of IoT practitioners. This will help better assess and validate the proposed model. Another avenue for future work, is to evolve the proposed security practices into concrete guidelines suited for IoT developers. Finally, it would be beneficial to introduce additional security metrics and have their effectiveness evaluated against IoT companies.

Acknowledgment

This work has been carried out within the research profile "Internet of Things and People", funded by the Knowledge Foundation and Malmö University in collaboration with 10 industrial partners.

References

[1] Gartner Inc., "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," 2018. [Online]. Available: https://www.gartner.com/newsroom/id/3598917.

[2] L. Columbus, "2017 Roundup Of Internet Of Things Forecasts," 2017 [Online]. Available: https://goo.gl/MCKCNa.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things - Vision, applications and research challenges.," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[4] B. Vogel and R. Varshney, "Towards designing open and secure IoT systems," In *8th International Conference on the Internet of Things*, pp. 1–6, 2018.

[5] J. Bugeja, D. Jonsson, and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras," In *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 537–542, 2018.

[6] Cloud Security Alliance, "Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products,". 2016.

[7] I. Berrouyne *et al.*, Towards Model-Based Communication Control for the Internet of Things. In *Federation of International Conferences on Software Technologies: Applications and Foundations*, pp. 644–655, 2018.

[8] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1, pp. 1–13, 2018.

[9] K. Dempsey *et al.*, "Information Security Continuous Monitoring (ISCM) for federal information systems and organizations," National Institute of Standards and Technology Special Publication 800-137, 2012.

[10] OWASP, "Software Assurance Maturity Model," OWASP, 2018. [Online]. Available: https://goo.gl/9cCA4h.

[11] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University - Computer and Information Sciences*, 30(3), pp. 291–319, 2018.

[12] Z. Ling *et al.*, "IoT Security: An End-to-End View and Case Study," *arXiv preprint arXiv:1805.05853.*

[13] S.-R. Oh and Y.-G. Kim, "Security Requirements Analysis for the IoT," In *IEEE 2017 International Conference on Platform Technology and Service (PlatCon),* 2017, pp. 1–6.

[14] I. A. Tøndel, M. G. Jaatun, and P. H. Meland, "Security Requirements for the Rest of Us - A Survey.," *IEEE Software*, vol. 25, no. 1, pp. 20–27, 2008.

[15] N. Teodoro and C. Serrao, "Web application security: Improving critical web-based applications quality through in-depth security analysis," In *IEEE International Conference on Information Society (i-Society)*, 2011, pp. 457–462.

[16] G. Trifonov, "Reducing the number of security vulnerabilities in web applications by improving software quality," In *2009 5th International Symposium on Applied Computational Intelligence and Informatics*, 2009, pp. 51–54.

[17] M. Howard and S. Lipner, "The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software," *Microsoft Press*, vol. 8, 2006.

[18] J. Grégoire *et al.*,, "On the Secure Software Development Process - CLASP and SDL Compared.," In *IEEE Computer Society Proceedings of the Third International Workshop on Software Engineering for Secure Systems*, pp. 1–7, 2007.

[19] D. Graham, "Introduction to the CLASP Process," 2006. [Online]. Available: https://goo.gl/wducjb.

[20] Gary McGraw, S. Migues, and J. West, "Building Security In Maturity Model (BSIMM)," 2018. [Online]. Available: https://goo.gl/JUAtbF.

[21] P. Chandra, "What's up with the other model?," 2009. [Online]. Available: https://goo.gl/zhBWm6.

[22] R. Varshney, "Towards Designing Open Secure IoT System - Insights for practitioners," pp. 1–147, 2018.

[23] A. Singh and K. Chatterjee, "Cloud security issues and challenges: a survey," *Journal of Network and Computer Applications*, vol. 79, pp. 1–34, 2016.

[24] P. El-Khoury, P. Busnel, S. Giroux, and K. Li, "Enforcing Security in Smart Homes using Security Patterns," *IJSH*, vol. 3, no. 2, 2009.

[25] Federal Trade Commission, "Internet of Things: Privacy & Security in a Connected World," pp. 1–71, 2015.

[26] J. R. C. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IEEE IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[27] G. Martins *et al.*, "Towards a systematic threat modeling approach for cyber-physical systems," In *IEEE 2015 Resilience Week*, 2015, pp. 1–6.

[28] B. Ismael, "Privacy and Trust Relations in Internet of Things from the User Point of View," In *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1–5.

[29] V. Sivaraman *et al.*, "Smart IoT Devices in the Home: Security and Privacy Implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, 2018.

[30] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: A Model-based Security Toolkit for the Internet of Things," *Computers & Security*, vol. 54, pp. 60–76, 2015.

[31] C. Sandescu *et al.*, "Why IoT security is failing. The Need of a Test Driven Security Approach," In *2018 IEEE 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–6, 2018.

[32] M. G. Jaatun *et al.*, "Software Security Maturity in Public Organisations," In *International Information Security Conference*, pp. 120–138, 2015.