# Emerging Trends in Smart Home Security, Privacy, and Digital Forensics

*Full paper*

**Miloslava Plachkinova, Ph.D.**
University of Tampa,
Tampa, FL
mplachkinova@ut.edu

**Au Vo**
Claremont Graduate University,
Claremont, CA
au.vo@cgu.edu

**Ala Alluhaidan**
Claremont Graduate University, Claremont, CA
ala.alluhaidan@cgu.edu

## Abstract

Technology integration is becoming an impetus to everyday lives. This new interconnected world can be found from our most private spaces to the public ones. Smart homes, which is the use of Internet of Things (IoT) within a home, has become the utmost concern in the security and privacy domain. In this paper, we review the current literature from both research and practice and offer five research trends for security and privacy in smart homes: potential for remote security breaches, risks for smart home devices, privacy violations, infrastructure vulnerabilities, and digital forensics challenges. We integrated these five trends in a conceptual model showcasing their roles in the rapidly changing IoT landscape. Combining the trends and smart forensics, we elucidate the bimodal lenses in security and privacy: preventive and investigative. These discussions offer research directions and practitioners' implications for further development of a safe and secured smart home.

**Keywords (Required)**

Internet of Things, IoT, Smart Homes, Security, Privacy, Digital Forensics, Emerging Trends

## Introduction

The Internet of Things (IoT) has empowered the progressiveness of an integrated world and established many new sectors such as smart homes and smart buildings. Collectively, they are known as smart environments. The development of such smart environments has been growing exponentially and the market for smart home appliances alone is projected to reach $26 billion by 2019 (Wilson et al. 2015). The integration and connection of physical 'things' to the Internet means it is now possible to remotely access sensors and devices (along with their data) integrated into homes for monitoring, analytics, and forecasting (Kopetz 2011). However, IoT technology also introduces numerous vulnerabilities. These are the byproduct of remote monitoring and remote controlling the building infrastructure along with the devices connected to them (Wendzel et al. 2014). This situation creates an environment where the security and privacy of both devices and end-user data are at risk (Weber 2010b).

Technology integration is becoming an impetus to everyday lives, especially for individuals in developed countries. This new interconnected world can be found from our most private spaces to the public ones. Technology enabled greater productivity and provided opportunities for cost savings. Such an optimistic view lays the foundation for more technological innovations. However, as technology grows, the associated risks exacerbate. While new developments possess unlimited potential for making our lives better, we need to also beware of any unforeseeable and foreseeable vulnerabilities that arise from them. Thus, the purpose of this research is to create awareness about the dark side of IoT in the most treasured location: our homes.

The inception of the moniker  smart home, which is the use of IoT within a home, has become one of the top IoT trends. Due to the nascent of IoT technology, home security systems are susceptible to a plethora

of new and unexpected vulnerabilities. This would, in turn, create an impediment in technology adoption. Luckily, the innovation also highlights another aspect, digital forensics, which could be used to bring justice into previously impossible-to-solve cases. We feel such discussion is imperative for future development of IoT in smart homes. By bringing digital forensics into light, we envision a wholesome and discussion about the multi-faceted IoT concerns, especially when the war between digital forensics and personal privacy is raging profusely at the District Court[1]. As a result, based on an analysis of 221 manuscripts, we outline five major trends in smart home technology: (1) potential for remote security breaches, (2) risks for smart home devices, (3) privacy violations, (4) infrastructure vulnerabilities, and (5) digital forensics challenges.

In order to keep up with the rapidly changing technological innovations, we looked at academic and practitioner literature to identify some of the most common trends that have the potential to drive IoT development in the future. We argue that is important to understand these IoT aspects in order to provide more security and privacy for users. Our analysis reveals that certain themes appear more frequently in IoT and we suggest that manufacturers and policy makers should focus their attention to these aspects with urgency. Furthermore, we discuss how IoT devices can be improved to support smart forensics and offer approaches to enhance the data collection from such devices. We present the possible data that can be used and outline the challenges and approaches to smart forensics. Preparing digital forensics for the smart age is needed, as they should be able to encompass all the aspects of the emerging IoT technologies.

Based on the five outlined trends and the increasing security and privacy challenges, we offer a novel solution for policy makers to better prepare them for the upcoming technology revolution. Our work is positioned to enhance security and improve forensic endeavors for the smart home age, as these aspects are currently lagging behind the rapid growth of IoT.

## Research Method

The work presented in this paper has been organized as a systematic review and conducted based on recommendations by Kitchenham, et al. (2007). The objective of the systematic review was to identify current research efforts and challenges for security, privacy, and digital forensics in the smart homes domain. The research question that guided the review was: "What are the major trends in smart home security and privacy?" We were specifically interested in this topic as IoT for smart homes is a fast growing field and in order to stay ahead of the curve, it is crucial for researchers and practitioners to be familiar with the main driving forces in it.

We limited our study to literature documenting 'smart home' experiences and practices and only included literature published after 2010 in order to capture the most recent smart home trends. Relevant literature was identified through five different major databases: ACM Digital Library, AIS Electronic Library, IEEE Explorer, ABI/INFORM, and Academic Search Premier. The search terms intended to identify all literature that covered security, privacy, and digital forensics challenges in the smart home domain were: ("smart home" AND "internet of things" AND "security"); ("smart home" AND "internet of things" AND "privacy"); ("smart home" AND "internet of things" AND "digital forensics"). The identified literature was then manually sorted into inclusion or exclusion categories by relevancy in the study by two researchers for ensuring consistency and reliability.

The literature review search was performed in December, 2015 and resulted in 346 papers. These results included research manuscripts, practitioner reports, and whitepapers. 89 duplicated papers were removed from the review list, leaving 257 papers to be reviewed for suitability. The title and abstract of the 257 papers were then analyzed to determine if they were relevant or not and irrelevant papers were discard at this point. After this initial review, 221 publications were analyzed to answer the research question. The process was performed by two independent researchers who then compared their results and the final list was reviewed by a third researcher for confirmation. Software tools such as EndNote X7 and Microsoft Excel 2013 were used to compile and analyze the database.

[1] https://www.justice.gov/usao-cdca/file/825001/download, accessed March 2, 2016

# Results

After analyzing the 221 publications, we identified five major trends related to the security and privacy of smart homes: (1) potential for remote security breaches, (2) risks for smart home devices, (3) privacy violations, (4) infrastructure vulnerabilities, and (5) digital forensics challenges. Furthermore, we created a model to conceptualize these trends. The following subsections are an overview of our findings from the literature review.

## *Potential for Remote Security Breaches*

The Consumer Technology Association projects that U.S. sales of smart-home devices would reach 8.9 million units in 2016, generating $1.2 billion revenue (Clark 2016). Yet in contrast, a recent survey by Accenture LLP (Poeter 2014) reported that 47% of respondents would not adopt smart home technology due to concerns with the security and privacy of such devices. The report by Accenture also stated that those individuals, who were planning to buy smart home gadgets in the next 12 months, were either delaying their purchase for fear that their devices could be hacked by trespassers or used by vendors to collect private data (Poeter 2014). Therefore, the more security is integrated into these devices, the higher the adoption rates would be.

Academics have looked into the problem of remote security breaches in smart homes and have identified some major problems that are unique for the ecosystem. For example, Kim et al. (2010) pointed out the following flaws of smart homes: no dedicated expert administrator, mixed ownership, complexity of home environments, diversity of visiting parties, multiple uncoordinated administrators, differences in administrator preferences, and social context – distrust revelation problem. These were among the main reasons for lack of adequate access right administration for secure home networks. These challenges are unique and different from enterprises regarding creating access control lists due to the lack of clear roles and responsibilities of the smart home's inhabitants and visitors.

Another study pointed out that cyber-physical system security demands additional security requirements and both information security and system-theory-based security were essential to securing cyber–physical systems (Mo et al. 2012). Combining both methods is important in order to improve the current state of smart home security and privacy and we recommend policy makers and manufacturers to consider a more integrative approach to this problem of growing concern.

In addition to academicians, practitioners have also looked into the problem of securing smart homes. Remote Access Tools presented yet another concern; people have been spied upon when webcams being remote-controlled. The same is true with smart TVs with built-in cameras and microphones. If this device was compromised, then, in theory, it would be used to monitor the users' TVs and the surrounding environment. This vulnerability has already been demonstrated as a potential risk in currently available systems (Grattafiori and Yavor 2013). A compromised smart TV could potentially be used to attack other systems on the same home network, or to form part of a botnet. One security company found evidence of smart devices (including a refrigerator) already being exploited by malware (Sutherland et al. 2014). Some smart TVs contained speech recognition, which could be used to extract a user's biometric data (Lee et al. 2011; Mehrabani et al. 2015).

## *Risks for Smart Home Devices*

A second trend outlined in literature is the risks for smart home devices. As Swatsky (2015) pointed out, there has been a pressing need for regulation and certification to ensure that smart home devices comply with the minimum level of security data and protection. Currently, no such governing authority exists, resulting in a growing number of mobile malware and malvertising (injecting malicious advertisements into legitimate online advertising networks). Furthermore, the author explained that these problems have resulted in hackers switching from desktop to mobile devices, as the latter offered more opportunities for security breaches.

Such projections are not made without reason. Now that smart phones are integrated into people's lives and they have become so reliable on them for everyday activities, these devices have logically become an important aspect of smart homes as well. In essence, smart phones are typically used as remote access points for smart homes. However, the relatively low security on smart phones and the lack of control over

uploading applications have made smart phones an easy target and are thus a weak link for smart home security.

Utilizing smart phones for managing appliances in the home becomes more pervasive. Ahmad et al. (2015) explored the concept of nested systems. They believed that a new ecosystem within an existing smart phone ecosystem will be a "suitable platform for distribution of apps for smart home and IoT devices". The authors expressed their concern that ecosystems built in Android had limitations that can be exploited by malicious apps that would leak sensitive data unintendedly. For instance, Android did not control which servers the app talked to or what data it shared with other apps. Thus, sub-ecosystems that enforced additional fine-grained tailored policies on top of existing ones in smartphone ecosystems were necessary within IoT platforms. Ahmad et al. (2015) presented a tool that enforces additional policies on inter-app interactions and permissions of Android app. They suggested that such a tool should:

• Restrict an app to a limited whitelist of permissions or no permissions at all.

• Restrict an app to a limited whitelist of other apps with whom they can interact explicitly.

• Enable an app to access privileged resources, if required, only through APIs provided by home automation ecosystem framework.

These ideas only demonstrate the importance of looking further into securing smart phones, as they may turn out to be the weak link in a smart home ecosystem. Smart phone manufacturers need to improve the review process of submitting apps to their app stores in order to avoid any potential flaws that may lead to security breaches into the smart homes of their customers.

### *Privacy Violations*

IoT devices typically collect data that is sent using Wi-Fi internet connections. This approach poses certain risks for the individual's privacy, since it is unclear how the data is being stored, who has access to it, and what are the data retention policies among devices. In addition, many IoT devices are connected to the primary Wi-Fi network in the home, which makes it easier for hackers to access. Problems can arise if the home's wireless network is not encrypted properly. All of these issues can lead to privacy breaches, identity thefts, and financial losses. Thus, there have been calls for new models of consent and privacy to protect the individual in fundamental ways (Friedland 2015), as well as for proposing frameworks for managing such new security threats (ISACA 2015; Maras 2015).

Some of the privacy concerns outlined in prior literature focused also on selling personal data to third parties. For example, Southerland (2015) pointed out that smart home devices had a lot of disadvantages when it came to privacy. For example, they sent all of user's personal data to corporate servers, where it was stored with third party. Companies, individuals, and the device owners had no control over this process. Another privacy concern is related to collecting information about browsing or viewing behavior and later used to tailor online advertising. However, with IoT, only information related to device and network performance should be collected. Privacy of local Wi-Fi networks is a sensitive area for any user. After its Street View mapping cars inadvertently captured personal data including emails from unsecured networks in 30 countries between 2008 and 2010, Google faced a huge challenge for securing data while providing adequate information (Bradshaw 2015).

The protection of IoT devices is a multidimensional, multifaceted, and complex process. The limited control and choice over the collection, retention, and distribution of data reduce user control and threaten their privacy. A new approach in legislation is required to address existing risks of inadequate legal frameworks. To effectively address existing IoT vulnerabilities, it is recommended that a continuous thorough analysis of the existing legal frameworks is conducted. New elements should also be developed to tackle the risks related to IoT deployment (Maras, 2015).

### *Infrastructure Vulnerabilities*

IoT for smart homes provides numerous opportunities, features, and capabilities. Although technical functionalities have been growing rapidly, the security issues arising from these new devices are alarmingly high. Our review points out a number of vulnerabilities in the technologies that are now being built in more and more homes. For example, the ZigBee protocol offers a wide variety of

intercommunication. It enables vendors to pre-install security keys so devices recognize each other. Rubenking (2015) explained that non-critical devices like smart lightbulbs can connect using the main, shared network key, while important devices like door locks could instead use a unique link key to communicate with the master automation device. But at the lowest level of security, there should be a fallback case that involves establishing the initial connection using a fixed default key. Yet, Zillner and Strobl (2015) demonstrated at the Black Hat Conference in 2015 that only the fallback default key system was implemented in a set of Zigbee devices. Unfortunately, this allowed the system to be connected and accessed remotely to read data, send commands, and eventually owned by a third party.

The small size of IoT devices and the fact that some of them run on low power along with limited computational capacity made adding encryption and other security measures difficult. Peppet (2014) emphasized the issue by discussing the November 2013 attack that took control of over 100,000 IoT web cameras, appliances, and other devices. A single attack affecting a myriad of machines points out the need of significantly improving the technical features and capabilities of the IoT devices, especially those in smart homes, where users are supposed to feel the most private and protected.

There have been sparse attempts to integrate more security features through security devices. However, those devices were not warmly welcomed by the general public, as security inhibits the customers' catered experience and prevents users from having an easy access to the IoT devices. Lynn (2014) discussed the problems associated with implementing Wi-Fi Protected Setup (WPS). "The idea behind WPS was to make it easier to connect devices to a wireless network while maintaining network security. Unfortunately, the WPS methods have not gained popularity since the process is not designed with mobile or smart home products in mind" (Lynn 2014). The demonstrated user resistance pointed out the need to integrate security in a more seamless manner when designing and developing IoT devices, especially for smart homes.

In addition to providing WPS capabilities, it is important to consider securely shielding the memory of the device to prevent attackers from reading the certificate and credentials from the memory. This is an important issue, as many of the IoT devices store sensitive data, so both data transmission and storage are crucial. Certificates add another layer of protection and the use of a chip-based authentication method is recommended to "carry the identity; a number, passwords and one or more cryptographic keys" (OECD 2012). Customizing chips for each organization is also highly recommended. This issue is only one of the numerous technical challenges associated with the mass deployment of IoT devices in smart homes and further research is needed to improve the current state of security and privacy, especially with regards to offering better technical capabilities.

Another aspect of the technical vulnerabilities in smart homes is setting access controls. Authorization frameworks like role-based access control (RBAC) and attribute-based access control (ABAC) do not provide scalable, manageable, effective, and efficient mechanisms to support distributed systems with many interacting services. In addition, the controls are not able to effectively support the dynamicity and scaling needs of IoT contexts that envisage a potentially unbound number of sensors, actuators and related resources, services and subjects, as well as a more relevance of short-lived, unplanned and dynamic interaction patterns (Gusmeroli et al. 2013). Although these frameworks are widely accepted by practitioners, they do not directly address the emerging challenges of IoT devices. Thus, we recommend that new and improved access control systems are utilized for managing the growing number of IoT devices in smart homes.

To address these concerns, (Gusmeroli et al. 2013) proposed a capability-based access control (CBAC) system that enterprises or individuals may use to manage their access control practices. The proposed capability supports rights delegation and an added sophisticated access control customization. We argue that such a solution be considered by manufacturers, policy makers, and even users who set up their smart home infrastructures. CBAC addresses many shortcomings of existing frameworks and can add more security to IoT devices in the home. While the proposed frameworks may be too complex for the general population, large corporations and governments would be the direct benefactors when making a decision on IoT infrastructure developments.

### *Digital Forensics Challenges*

The last trend focuses on digital forensics which are constantly evolving, especially in smart homes. The need for a forensic analysis could arise from either the activity or misuse of the owner, or as a result of a network compromise by a malicious entity, the same as a laptop or desktop computing platform. However, digital forensic investigations of smart homes pose a number of challenges, particularly with the collection of evidence for investigative purposes.

However, there is a concern surrounding the reliability of the data that is stored on these devices when a security incident or privacy breach occurs (Sutherland et al. 2014). Furthermore, specific tools could be required for individual smart home devices and there is the possibility that these may currently be unavailable to a forensic investigator (Sutherland et al. 2014). Forensic investigations in smart homes would also need to take into consideration that smart home owners could be more involved in the investigation process when compared to traditional forensic investigations (Oriwoh and Sant 2013).

Hegarty, et al. (2014) argued that the presence of IoT systems in smart homes posed challenges related to the identification of a particular user's data. There were particular concerns related to the 'search and seizure' of smart home devices, as in such environments it might not be clear where data being investigated was currently stored (Hegarty et al. 2014). The data from one smart home device may be transferred and consumed by another device or a local ad-hoc network of things. The end result was that creating and maintaining a chain of custody for this data could become a difficult task. The preservation of digital evidence in smart home investigations could also be an issue in such investigations (Hegarty et al. 2014).

Smart home forensic investigations would complicate data preservation because data could be either overwritten or lost if smart devices that interacted with cloud service providers were suddenly removed from the cloud (Grispos et al. 2012; Hegarty et al. 2014). The interaction between smart home devices and cloud computing also meant that smart home investigations were likely to include investigations of cloud environments (Osborne and Slay 2011), which has been well discussed in the literature (Dykstra and Sherman 2011; Grispos et al. 2012; Ruan et al. 2011).

Till now, there is no widely accepted protocol or standard for IoT. Vendors are using their proprietary protocols for IoT communication. The wide varieties of structure of the data generated by the IoT devices make the examination and analysis phase challenging. Organizing logs collected from different sources (such as multiple IoT devices) remain ambiguous, as there are no standard formats for logs across different systems. Some of the logs may not even provide crucial information for forensic purpose, e.g., who, when, where, and why. However, log organization might impede personal privacy and security as hackers could make use of the data mischievously.

## Discussion

The current research builds upon prior studies on IoT in general (Medaglia and Serbanati 2010; Weber 2010a) but also highlights a new aspect of IoT security and privacy by incorporating digital forensics for smart homes. We are able to confirm that some of the trends discovered in the past are still relevant and pertinent to smart homes, which demonstrates their importance to the field. Our conceptual model (Figure 1) touches upon the concerns researchers have had in the past, such as identity and storage management, communication threats, embedded security, and physical threats among others (Babar et al. 2010). However, our focus is on smart homes and we investigate the specifics of that particular context, as it presents some unique challenges related to the perception of personal space and privacy. These are different from other applications of IoT, for instance, in smart cities or smart grids.

Through our analysis, we looked at a number of published manuscripts in both scientific and practitioner outlets. Our work was driven by the question: "What are the major trends in IoT security and privacy?" The trends we identified are summarized in the conceptual model below (Figure 1):

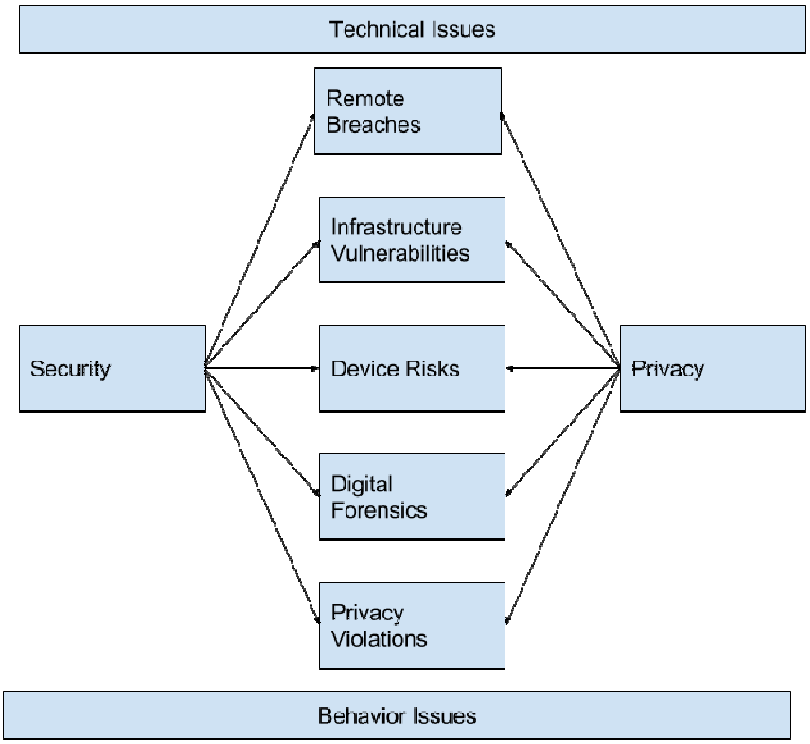


**Figure 1. Conceptual Model**

We suggest that these five trends be taken into serious consideration by manufacturers, policy makers, and even end-users, as all of them are involved in shaping security and privacy policy. Manufacturers can assist in upholding our collective security and privacy by adding more layers of security and addressing potential software and hardware flaws. Policy makers can propose legislation changes that can be more adequate to the current state of IoT and provide more privacy for individuals who have such devices in their homes. In order for them to fully enjoy the privacy of their homes, users should demand to know how their data is being collected, who has access to it, what the retention policies are, and whether the data is sold to third parties or not. If all involved parties start working together in this direction, then the IoT for smart homes will gain more trust and the market will grow at a much faster pace.

Through our analysis we also found out that although digital forensics has advanced at a great pace in the past, it is not fully ready for smart homes technology. Within IoT, there are some unique risks related to the security and privacy of individuals in their homes and it is imperative to address these shortcomings as we are prepared to curb more and more smart home attacks in the future. The five trends we pointed out are all possible attack vectors and it is critical for experts to consider how they can enhance the capabilities of forensics and move to the smart forensics age.

And finally, we provided two aspects of smart homes security: preventive and investigative. In the lens of preventive issue, researchers should focus on a discussion of the bimodal view of privacy and security. Using the five trends discussed above, researchers could establish an in-depth investigation of a smart home security and privacy vulnerabilities. On the other hand, researchers uses investigative lens to determine ways that would aid officials in their investigation endeavor. Protecting smart homes needs to be an effort of preventing undesirable events from happening and punishing the entity who is responsible for malicious attacks.

## Limitations and Future Work

Our work touches upon a new and emerging topic as IoT in smart homes and there are limitations related to it. The paper discusses a number of problems and offers recommendations to manufacturers, policy makers, and end users to solve this problem. We would like to further expand our work by examining in

more detail various smart home devices and analyze their vulnerabilities. As technology grows, the trends might expand and/or change. This first-hand experience will provide us with more insights and knowledge on how to better protect IoT users. Our work is preliminary in essence, as we are now laying the foundations of an entire new branch of digital forensics – smart forensics. Our next step will be to focus on collecting more evidence to support this concept. In addition, our future work would include adding quantitative results to present the number of IoT papers published in each discipline as well as rank ordering the manuscripts based on their number of citations for instance.

## Conclusion

The current study contributes to literature, as it presents an investigation of the emerging trends related to the security and privacy of IoT. Based on our analysis of 221 manuscripts, we were able to identify five growing trends. Due to the rapid development of new technologies, policy makers have been experiencing a difficulty conceptualizing IoT issues and proposing viable solutions for improving user security and privacy but without harming user experience and satisfaction.

Thus, another major contribution of the study is to introduce the current state of digital forensics readiness to solve smart home security problems. We discussed a number of challenges and concerns that currently exist in the field in order to focus the attention of experts and raise awareness of this problem. We explored the challenges and opportunities associated with this endeavor and outline the possible forensic data that can be collected from a smart device in the home. With the growing number of security breaches and the lagging solutions for IoT, this study identifies several important aspects that can be addressed to provide safer use of IoT devices in smart homes.

Finally, our work will not only impact academicians, but also practitioners who are designing new IoT devices every day. This study raises awareness of the important aspects of the design and development of such technologies by presenting some of the most pressing issues they need to focus on. Hence, we strive to bridge the gap between theory and practice and foster a successful collaboration that can provide better outcomes.

## Acknowledgement

We would like to thank Dr. George Grispos for his infinite support and guidance throughout the development of this project. We highly appreciate his opinion and efforts to strengthen the quality of our work. His work during the process is highly valued and greatly appreciated.

## REFERENCES

Ahmad, W., Sunshine, J., Kaestner, C., and Wynne, A. 2015. "Enforcing Fine-Grained Security and Privacy Policies in an Ecosystem within an Ecosystem," *Proceedings of the 3rd International Workshop on Mobile Development Lifecycle*: ACM, pp. 28-34.

Babar, S., Mahalle, P., Stango, A., Prasad, N., and Prasad, R. 2010. "Proposed Security Model and Threat Taxonomy for the Internet of Things (Iot)," in *Recent Trends in Network Security and Applications*. Springer, pp. 420-429.

Bradshaw, T. 2015. "Google in Home Hub Challenge to Cable," in: *Financial Times*. London (UK): p. 15.

Clark, D. 2016. "Smart-Home Gadgets Still a Hard Sell," in: *Wall Street Journal (Online)*. New York, N.Y.

Dykstra, J., and Sherman, A. T. 2011. "Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies," *Proceedings of the Conference on Digital Forensics, Security and Law*.

Friedland, S. I. 2015. "I Spy: The New Self-Cybersurveillance," *Washington and Lee Law Review* (72:3), pp. 1459-1501.

Grattafiori, A., and Yavor, J. 2013. "The Outer Limits: Hacking the Samsung Smart Tv," *Black Hat Briefings*).

Grispos, G., Storer, T., and Glisson, W. B. 2012. "Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics," *International Journal of Digital Crime and Forensics* (4:2), pp. 28-48.

Gusmeroli, S., Piccione, S., and Rotondi, D. 2013. "A Capability-Based Security Approach to Manage Access Control in the Internet of Things," *Mathematical & Computer Modelling* (58:5/6), pp. 1189-1205.

Hegarty, R., Lamb, D., and Attwood., A. 2014. "Digital Evidence Challenges in the Internet of Things," *Proceedings of the Tenth International Network Conference (INC 2014)*.

ISACA. 2015. " Isaca Identifies Five Cyber Risk Trends for 2016 " Retrieved February 12, 2016, from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx

Kim, T. H.-J., Bauer, L., Newsome, J., Perrig, A., and Walker, J. 2010. "Challenges in Access Right Assignment for Secure Home Networks," *HotSec*.

Kitchenham, B., Charters, S., Budgen, D., and Brereton, P. 2007. "Guidelines for Performing Systematic Literature Reviews in Software Engineering," EBSE Technical Report.

Kopetz, H. 2011. "Internet of Things," in *Real-Time Systems*. Springer, pp. 307-323.

Lee, K.-A., Larcher, A., Thai, H., Ma, B., and Li, H. 2011. "Joint Application of Speech and Speaker Recognition for Automation and Security in Smart Home," *INTERSPEECH*, pp. 3317-3318.

Lynn, S. 2014. "Wps with Nfc Is Exciting, but Is It Safe?," *PCmag.com*).

Maras, M.-H. 2015. "Internet of Things: Security and Privacy Implications," *International Data Privacy Law* (5:2), pp. 99-104.

Medaglia, C. M., and Serbanati, A. 2010. "An Overview of Privacy and Security Issues in the Internet of Things," in *The Internet of Things*. Springer, pp. 389-395.

Mehrabani, M., Bangalore, S., and Stern, B. 2015. "Personalized Speech Recognition for Internet of Things," *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, pp. 369-374.

Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., and Sinopoli, B. 2012. "Cyber–Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE* (100:1), pp. 195-209.

OECD. 2012. "Machine-to-Machine Communications: Connecting Billions of Devices," Organisation for Economic Cooperation and Development (OECD), Paris, pp. 0_1,2,5-44.

Oriwoh, E., and Sant, P. 2013. "The Forensics Edge Management System: A Concept and Design," *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, pp. 544-550.

Osborne, G., and Slay, J. 2011. "Digital Forensics Infovis: An Implementation of a Process for Visualisation of Digital Evidence," *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*: IEEE, pp. 196-201.

Peppet, S. R. 2014. "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent," *Texas Law Review* (93:1), pp. 85-176.

Poeter, D. 2014. "Survey: Iot, Wearables Market Set for Explosive Growth," *PCmag.com*).

Ruan, K., Carthy, J., Kechadi, T., and Crosbie, M. (eds.). 2011. *Cloud Forensics*. Springer.

Rubenking, N. J. 2015. "Your Connected Home Is Wide Open to Attack," *PCmag.com*).

Southerland, R. 2015. "Smart Home Security Risks with Internet of Things (Iot)." Retrieved February 12, 2016, from http://us.sourcesecurity.com/news/articles/18159.html

Sutherland, I., Read, H., and Xynos, K. 2014. "Forensic Analysis of Smart Tv: A Current Issue and Call to Arms," *Digital Investigation* (11:3), pp. 175-178.

Swatsky, M. 2015. "Connecting Your Customers with the Connected Home," *Dealerscope* (57:14), p. 10.

Weber, R. H. 2010a. "Internet of Things–New Security and Privacy Challenges," *Computer Law & Security Review* (26:1), pp. 23-30.

Weber, R. H. 2010b. "Internet of Things – New Security and Privacy Challenges," *Computer Law and Security Review* (26:1), pp. 23-30.

Wendzel, S., Zwanger, V., Meier, M., and Szlosarczyk, S. 2014. "Envisioning Smart Building Botnets," in: *Sicherheit*.

Wilson, C., Hargreaves, T., and Hauxwell-Baldwin, R. 2015. "Smart Homes and Their Users: A Systematic Analysis and Key Challenges," *Personal and Ubiquitous Computing* (19:2), pp. 463-476.

Zillner, T., and Strobl, S. 2015. "Zigbee Exploited - the Good, the Bad, and the Ugly," in: *Black Hat*. Las Vegas.