International Journal of Academic Research and Development
ISSN: 2455-4197; Impact Factor: RJIF 5.22
Received: 05-10-2020; Accepted: 21-10-2020; Published: 08-11-2020
www.academicjournal.in
Volume 5; Issue 6; 2020; Page No. 42-45

Privacy and security in the internet of things (Iot)

Khan Muhammad Wafa[1], Sebghatullah Aslamzai[2]
[1] Dean of Computer Science Faculty and Lecturer, Bost University, Helmand Province, Afghanistan
[2] Assistant Professor, IT Department, Computer Science Faculty, Kabul University, Afghanistan

Abstract
The Internet of Things (IoT) provides opportunities for intelligent wearable devices, home appliances, and software/middleware to communicate and share information on the Internet. In this research, I begin with general information security background of IoT and continue on with information security related challenges that IoT will have experienced. I will also point out research directions that could be the future work for the solutions to the security challenges that IoT encounters. With the aim and target at proposing a methodological approach for secure IoT application development, I investigated what are security challenges in the sense of IoT development. I reviewed literature and investigated two industry cases. The preliminary finding results in a list of few security challenges with regards to organizational, technical and methodological perspectives. Cross case comparison provides initial explanation about the less focus on organizational and methodological security concerns in my cases. My approach was initially exemplified in a smart home setting and consists of three main tiers namely: cloud storage, overlay, and smart home but I delve deeper and outlined the various core components and functions of the smart generous tier. Each smart place is equipped with an always high resource device, online, known as miner that is responsible for handling all communication within and external to the internal system. The miner also preserves a private and secure Block Chain, used for controlling and auditing communications. I show that our proposed block chain base smart places framework is secure by thoroughly analyzing its security with respect to the fundamental security goals of integrity, confidentiality and availability. Finally, I present solutions and results to highlight that the overheads in terms of traffic, processing time and energy consumption introduced by this approach are insignificant relative to its security and privacy gains.

Keywords: network security and privacy

1. Introduction
The Internet of Things (IoT) was originally coined as a phrase by Kevin Ashton in 1990 (Ashton, K.2009) [3]. in terms of tangible items to become identifiable electronically so they used Radio Frequency Identification Device (RFID) chips and therefore intractable with the Internet. With the availability of considerably cheap processors and System on Chip (SoC) based devices, the definition has expanded to include wireless, Internet attached sensors and actuators including (smart meters, home smart automation systems, Internet attached set top boxes, smartphones, connected cars, and other systems that connect the physical world to the Internet either by measuring it or affecting it.

1.1 Objectives of the Research
1. To ensure security of personal data on public databases.
2. To maximize IoT Access control.
3. To maximize security awareness of IoT.

2. Methodology
The list of challenge was initiated by looking at IoT security literature. I identified a set of security challenges that have been experienced and projected in industrial projects all around the world. I have visited few of the organizations in Kabul Afghanistan. Thoroughly I haven't found any kind of IoT security inside Afghanistan. Smart homes are not available, smart cars, Smart medical facilities. With little knowledge on the topic, I have conducted two exploratory case studies with startups as a unit of analysis.

A Software Engineering Perspective
The cases were selected because 1) they developed software solution based on connected devices, and 2) my close contact with the CEOs, which enabled insight from the cases. The data was collected via interviews with CEOs of the startups.
Case1: French Medical Institute for Children Kabul Afghanistan, referred to as Case1 from here on in, is a medical institute in Kabul that has quickly grown to be one of the leading suppliers of performance tracking and monitoring systems for high quality Medical Procedures. Because of the success of their systems, they are expanding into the area of IoT. They are currently in the planning phase of the development of a Wireless Body Area Network known as WBAN that will be connected to a cloud storage system. The system will enable multiple users with access to a mobile application or a computer desktop application or web browser to monitor the performance, health and movement information of patients in real time through the cloud storage system.
Case2: Bright Water Manufacturing Kabul, referred to as Case2 from here on in, is a Trondheim based startup available in Kabul in aquaculture. The company is developing a water environment monitoring and peer to peer consultancy application for Asian market. The company was selected as top 20 IoT startups in Ningrhar Afghanistan startup contests and funded under government of South Koria incubator program. The company is initializing a Minimum Viable Product (MVP) for fund raising by March

2018. The current teams included three software engineers, one electronic engineer and a UX designer (foreigners).

In the first case of Medical Institute, I was able to have multiple insights as the author of this thesis, the second and the third stage I am working as a security researcher.

In the second case of Water Company, I was a part of the management board, which enables the understanding on product prototyping and development. We faced the challenges those were placed into categories. The categories emerged from the data and were constructed 'a posterior'. They were then placed in a table to enable a cross case comparison of the challenges.

The approach followed is common in search of qualitative data. The list was also renewed based on input from workers from the two case companies and other security researchers at Universities of Science and Technology and Regulated Software Research Centre around the world, as well as practitioners.

3. Results

In reviewing both the security and privacy challenges of the wide range of Internet of Things and a detailed review of more than fifty middleware platforms, of which many are mentioned, key categories that can be applied across these areas have been identified.

The first set is that did not address security the majority of the identified systems, left it for future work, or did not describe the security approach in any meaningful detail were identified.

There were other systems such as UBIWARE and NAPS, theoretical models are offered by them but did not describe any real world implementation or solid approach. The next set is clear category, those middleware's that apply the SOAP or Web Services model of security. This includes the mentioned SOCRADES, SIRENA, and non-discussed Hydra or Link smart.

As I have discussed in the previous sections there are significant challenges in memory footprint, performance, processor power and usability of these approaches when used with the IoT.

To the XMPP standards two of the approaches delegate the model: 1. VIRTUS and 2, XMPP. XMPP also has the complexity of XML, but avoids the major performance overheads by using Transport Layer Security instead of XML Security and XML Encryption.

In addition, recent work on XMPP using EXI makes this approach more effective for IoT. This finally leaves a few unique approaches; each of them brings their own unique benefits.

The system that is to provide Multi level security is DREMS based on the concept of security clearances.

As this model is attractive to government and military circles because of the classification systems used in those circles, it has be argued that it fails in many regards for IoT so I didn't discuss it in my research. Actually there are no personal controls, no policy based access controls and no concept of federated identity in this model.

The one that I have discussed in my documentation is SMEPP which offers a model based on shared session keys and public key infrastructures.

It can be quarrel that this approach has a number of challenges in terms to the requirements of the IoT. Firstly, there are clear cut issues in key revocation and key distribution. Secondly, a new form of perimeter based on the concept of a shared session key is created by this model. This means that if one device is being compromised, the control and data of all the devices in that group will also compromise.

The concept of stream processing in the cloud is only supported by DIOPTASE, which is a very serious requirement for the IoT. The requirement is to be able to process, filter and summarize streams of data from devices to support reduction of data leakage and anonymization.

In the replacement fiware has an extensible and powerful model for access control and authentication, including support for federated identity and policy-based access control.

The most advanced approach that is proposed by Webinos identified. Webinos utilizes some main technologies to provide a privacy and security model. Firstly, this utilizes policy-based access control (XACML). Though, the model does not support user guided access control mechanisms such as OAuth2.

Webinos does support the use of federated identity tokens (Open-ID), but only from users to the cloud, as disputed to devices on the cloud.

I and others (authors of the papers) have proposed the model of using federated identity tokens from the device to the cloud in this discussion.

The contribution of the Webinos work with the biggest hidden impact is the concept of Personal Zone Hub (PZH) as discussed in chapters, which is a cloud service dedicated to a single user to handle the privacy and security requirements of that user.

However, there is further research around this area: the PZH model from Webinos does not look into many of the challenges of how to implement the PZH in real life. For example, cloud hosting, user registration and many other aspects need to be defined in more detail before the Webinos PZH model is attainable for real world projects. Furthermore, there are challenges using the PZH model with smaller devices as well, because of the requirement to use the PZP.

Finally I summarized that the all the mentioned have some of the draw backs and with the growth of the new era technology block chain security is filling up the gaps. Where-as, block chain technology has secured bitcoin, other same technologies as well, so the future of IoT also implementing the same technology.

Overall gaps in the security of middleware

When the requirements for privacy and security of the Internet of Things are examined there are some gaps that are not provided by any of the reviewed middleware systems.

- Only two of the middleware systems explicitly applied the concept of Policy Based Development (PBD), which is practical IoT security, in designing a middleware directly to support privacy, although Webinos did exhibit many of the characteristics of a system that used this approach.
- Only two of the systems applied any concepts of context based security or reputation to IoT devices, not over all security, so they are exposed.
- User consent was only supported in three of the systems.
- Anonymous identities or attestation are not supported by any of the system.
- None of the systems satisfied all the requirements identified.

Table 1

Input	Reason
The Vulnerability Area of IoT has Increased	More increase in the open networks. Increase of Cloud based system, Internet expanstion, and increase in USB devices, Bluetooth, ZigBee Devices.
Dwindling Support For Legacy Systems.	Software updates, patches for security where vendor support is dwindling. Thus they become a soft target for malware attacks.
Non Identifiable unauthorized services have increased.	Unique Identification Schemes must be devised for millions of devices
Remote access Facilities accessed unauthorized	Remote access can open doors for interception and tampering

4. Discussion

It is obvious that for the required IoT outcomes security plays an important role. There are many technical challenges for IOT security in the application layer of TCP/IP reference mode, perception layer, network layer and physical layer (Kumar *et al*., 2016). Many types of studies interrogate these technical challenges in order to secure IoT (Hui *et al*, 2012; Dhillon and Torkzadeh, 2006). On the other hand, these studies do address the socio technical perspective of IoT is rare and existing studies in IoT security mostly consider technical perspective deeply. It is obvious that in human behavior complexity and expectations and the role that people play in IoT requires further interrogations. In addition, according to plenty of research works (Hitchings, 1998; Armstrong, 1999; Dhillon, 2001; Karyda *et al*, 2003) for achieving success in security management even focusing on technical issues is not enough and addressing human issues is definitely important for successful security. For securing IoT the same gape exists in the literature. Most of the studies investigate security of IoT do not consider the social and behavioral perspective for securing IoT but it's too much important. Though, many of the behavioral concerns emerged in this study, including ethics and trust. One of the additional and fundamental objectives that turn up from this study is promoting the ethical use of IoT. In particular, clients highlight the need for organizations to promote IoT usage of ethics and to encourage the authoritative use of IoT. Organizations must invest significant amount of resources in IoT security, education, training and awareness (SETA) campaigns to achieve this objective. Future research is needed to identity unique approaches that will effectively train users on IoT security. In precise, SETA initiatives and studies around the ethical challenges associated with IoT accessibility, accuracy, property and private use will be a combined part of the emerging IoT security research stream.

In addition to ethics and ethical behavior, trust of IoT security also emerged as a significant means of objective. Tested clients emphasized the need for organizations to increase users trust in IoT usage and ensure trust in IoT products as well. Trust has been explored massively in multiple disciplines. The information systems community is loaded with studies on trust in an environment that is online. However, given the procreation of IoT, additional research is needed on the role of trust in the specified domain. The results of this study indicate the need for future research to explore ways to increase the use of trust, securing internet of things with value focused thinking approach (Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, Dublin, Ireland, December 13, 2016), building technologies, design formal security mechanisms for IoT solutions and enhance IoT governance for security. The qualitative study presented in this research has two limitations. First, the process of identifying values from the interview data was largely subjective and interpretive, also have mentioned this issue as one limitation of research of this kind. Second, my research may have had difficulty in considering manager/subordinate or gender values.

In the literature review a two phase approach to reviewing the available literature around the security and privacy of IoT devices has been taken. In the first part a model of security challenges was created that has been applied the existing CIA+ model to three different areas: device, network and cloud. This new model forms a clean and clear contribution to the literature. In each of the cells of the model were identified threats, challenges and approaches, aggravated by the IoT, or unchanged. Further, Spiekerman and Cranor's three-layer privacy model was used to analyze the privacy requirements of IoT. This overall analysis was used to identify several major requirements.

In the other part of thesis, a structured search approach was used to identify specific IoT middleware frameworks and then the security models of each of those was analyzed. The requirements from the first phase were used to validate the capabilities of each system. While there are existing surveys of IoT middleware, none of them focused on a detailed analysis of the security of the systems and therefore this has a clear contribution to the specified literature. There are very clear gaps in the literature and practice has identified. Over half the surveyed systems mentioned in the thesis had either no security or no substantive discussion of security. Out of all of the above-mentioned systems very few address a significant proportion of the major challenges that are identified in the first section. Some aspects have not been addressed by any of the surveyed systems.

This created an opportunity for my research that is the basis of the rest of this thesis:

- First, to define a model and architecture for IoT middleware that is designed from the start to enable privacy and security privacy by Design.
- Secondly, to bring together the best practice into a single middleware that includes, federated identity for users and devices, policy-based access control, user managed access to data, filtering, summarization, and other requirements.
- Thirdly, there is extensive work to be done to define a better model around the implementation challenges for the concept of a personal cloud service in terms of IoT security. This includes the hosting model, bootstrapping, discovery and usage for smaller devices.
- The main perspective that security of IoT is moving towards block chain technology and been grooved inside the security stability of anywhere any time access securely.

5. Conclusion

Two primary investigations into the use of Federated Identity and Access Management (FIAM) for IoT are presented. The first investigation, Federation of IoT (FIOT), was initially published as mentioned above in the thesis.

Later on the research work based, there have been done work on several middleware to enhance the security of IoT. This thesis utilizes the value focused thinking approach to provide objectives for securing IoT. According to Keeney (1999), "values to consciousness, allow you to uncover hidden objectives, the objectives you didn't realize you had". In some studies (Dhillon and Torkzadeh, 2006) have utilized Keeney's value focused methodology for understanding objectives and their relationships based on people values. For example, May *et al* (name), define value based objectives in order to assess ERP systems planning. The value focused thinking approach has not been utilized to define security objectives of IoT from the user perspective. Extracting IoT objectives from user's values can help managers and practitioners maximize IoT security based on comprehensive list of objectives.

This study contributes to extent literature, by introducing fundamental objectives and means objectives for securing IoT. This study investigates the relatively unexplored area of IoT security. We conduct a qualitative investigation using value-focused thinking that helped to extract 17 objectives, grouped into four fundamental and 13 means objectives, essential for securing IoT from user perspective. The objectives developed in this study employ a sociotechnical perspective and provide a way forward for developing IoT security measures. The findings of this research show that confidentiality, integrity and availability should be considered within the broader scheme of things in IoT security

6. References

1. Rahat SM. A review on elliptic curve cryptography for embedded systems. Int. J. Comput. Sci. Inf. Techno, 2011, 84-103.
2. Andrew Simmonds PS. An ontology for network security attacks. In: Applied Computing. New York, NY, USA: Springer, 2004, 317-323.
3. Ashton K. The Internet of Things. RFID Journal, 2009, 97-114.
4. Aziz PF. OAuthing: privacy-enhancing federation for the Internet of Things. Proceedings of the 2nd International Conference IEEE, 2016, 7.
5. Communication IW. IEEE EXPLORE. Retrieved from ieee, 2010. explore: https://ieeexplore.ieee.org:https://Ieeexplore.ieee.org/abstract/document/5416350/.
6. Daniele Miorandi SS. Internet of things: Vision, applications and research challenges. ELSEVIER, CREATE-NET, via Alla Cascata 56/D, IT-38123 Povo, Trento, Italy, 2012, 20.
7. Evans D. The internet of things. How the next evolution of Internet is changing everything, 2011, 5.
8. Gemalto. IoT Security. Retrieved from Internet of things, 2016, 7(4) Security: https://safenet.gemalto.Com/iot-2018/iot-security/.
9. Heslin PJ. Wikipedia. Retrieved from The Transvestite Achilles: Gender and Genre in Statius, 2019, 4(4). https://en.wikipedia.org/wiki/Achilles%27_heel.
10. Imperva. Internet of Things (IOT) security. Retrieved from imperva, 2018, 5(5). https://www.imperva.com/learn/application-security/iot-internet-of-things-security/.