A Survey on Risk Assessment and Management in IoT

Abstract: The Internet of Things (IoT) represents a modern approach where boundaries between real and digital domains progressively eliminated by changing over consistently every physical device to smart object. Each of these smart objects play a role in different life domains but at the same time create new challenges. The glue that binds IoT systems and their actors or devices will provide a mechanism for risk propagation and creation of harm, particularly in security and privacy, at physical, social, and economic scales. As such, the IoT actor, if repurposed, might be able to facilitate harms far beyond what is expected. Estimating risk is a complex operation that requires the consideration of a variety of factors. Moreover, the interpretation and estimation of the risk might vary depending on the working domain. This needs to be considered in a new risk assessment approach, as the inability of periodic assessment to respond to dramatic changes in IoT environments. This paper presents a review of different risk assessment techniques.

Keywords: Internet of things, IoT, Risk assessment, Risk management, Risk estimation, Security risk, Privacy.

1. Introduction

The Internet of Things (loT) is a mean of connecting multiple smart objects to the Internet with the intention of data capturing, communicating and providing services. IoT involves smart objects that are increasing day by day and are interconnected to monitor and control environment, thus playing a significant role in improving various aspects of human life. Some of the loTs applications include healthcare, transportation, industrial automation, and emergencies where it is difficult for humans to take decisions (Khan et al., 2016).

The IoT relies heavily on wireless networks and communications to provide connectivity for smart devices (Abouzakhar et al., 2017). Wireless communications are necessary because of their mobility requirements (Abouzakhar et al., 2017). However, their openness makes wireless communications more susceptible to various security threats, eavesdropping and/or different forms of risks (Abouzakhar et al., 2017). The IoT presents some key risks, with so many devices becoming interconnected (Want and Dustdar, 2015). The risks in IoT-based critical systems is becoming more significant, and any interruption or corruption could result in costly damage or, life threatening challenges (Want and Dustdar, 2015).Therefore, the security of and trust that we place in IT systems are a significant concern (Nurse et al., 2017).

The traditional approach to addressing such challenges has been to conduct cyber risk assessments that seek to identify critical assets, the threats they face, the likelihood of a successful attack, and the harms that might result. Only in this way, and after the identified risks have been prioritized, would appropriate approaches be selected to effectively address these risks (Nurse et al., 2017). From a security and trust management perspective, however, the challenge with the IoT is that existing risk assessment methodologies were established prior to its development (Nurse et al., 2017). Simply adopting preexisting risk assessment methods to the IoT could make us blind to new risks arising in this ecosystem (Nurse et al., 2017). In this article, we carefully analyze reasons why current risk assessment approaches are unsuitable for the IoT and highlight the need for new approaches or adaptations to underpin trust in IoT-based systems (Nurse et al., 2017). Only by crafting such methods, in partnership with industry, government, and academia, can we prepare to address the threats facing the IoT (Nurse et al., 2017).

The rest of this paper is structured as follows. Section 2 presents some literature review; Section 3 talks about some backgrounds of this topic; Section 4 describes the research methodology; Section 5 provides a review of risk assessment methods. Finally, The comparison of the reviewed mechanisms and their outcome are presented in Section 6. Also, Section 7 maps out same open issues. Finally, Section 8 concludes the paper.

2.Related Works

Up to now, very few surveys on risk assessment and risk management mechanisms in internet of things and how to control, manage and reduce security risks in many different fields has been carried out. This section will

refer to almost all review papers that discussed about risk assessment mechanisms in IoT and outlines their main advantageous and disadvantageous. Atlam et al. (2017) have presented a review of different risk estimation techniques that are used in existing risk-based access control models. In addition, they have discussed existing risk-based access control models and compared them in terms of the risk estimation technique, risk factors, and the evaluation domain. They have also presented some of the IoT requirements for selecting the appropriate risk estimation technique.

IoT sensor devices connected to patients monitor their pressure, temperature, heartbeats etc. and track their activity and behavior. A compromised sensor connected to a patient could lead to a devastating result. Monitoring IoT objects such as patients' sensors can be resource intensive and time consuming. GA offers the advantage of being cost effective and offers visualization tools that can help IoT designers see how patients interact with their healthcare application. Critical IoT systems must keep the operational environment safe, secure and resilient against constantly evolving cyber threats. This implies that critical IoT systems must keep the operational environment safe, secure and resilient against constantly evolving cyber threats. This is to maintain the safety of patients, medical assets as well as the communities they serve. Applying cybersecurity to critical IoT systems such as healthcare systems is becoming a challenging task and crucial business. A brief survey to recent security threats and vulnerabilities to different IoT systems is provided by Abouzakhar et al. (2017).

Kim (2017) has listed the types of IoT security and privacy risks, IOT-security requirements, and has summarized the main trends in IoT security related technology and research. He showed in his paper that, first, there are many security risks in all layers of IoT architectures and many privacy concerns related to the leaking of personal information. Second, IoT-security related research has grown rapidly in the last five years. Third, articles in this area address four distinct technologies: authentication, encryption and key management, protocols, security architecture, and other security schemes. Lastly, what threats are covered by the technologies and what type of issues need to be discussed as future research directions.

Nurse et al. (2017) carefully analyzed the current risk assessment approaches and the reasons why current risk assessment approaches are unsuitable for the IoT. Finally, they highlighted the need for new approaches or adaptations to underpin trust in IoT-based systems and mostly were thinking of a real-time approach for this risk assessment in IoT. In addition, they believed that only by crafting such methods, in partnership with industry, government, and academia, we can prepare to address the threats facing the IoT.

Although these papers have published in 2017 but they have not discussed most of the papers released in published year and some of the old ones. They only explained the brief methods of a few papers. Also, the papers have not been checked based on security and risk parameters in IoT. Briefly, the previous review papers suffer from some weakness as follows:

- The papers do not contain the new proposed mechanisms especially in 2017.
- The papers do not have the systematic structure; therefore, the article selection method is unclear.
- Some papers do not investigate the QoS parameters for reviewing the methods.
- Some papers do not implicate to the risk assessment method.
- Many papers do not provide any logical categorization.

The mentioned reasons motivated us to prepare a survey paper that covers all of these deficiencies.

3. Background

Risk assessment can have various meanings depending on its context of use. Here, we define the term as used in this article. Risk assessment is generally understood as the process of identifying, estimating, and prioritizing risks to organizational assets and operations (Gallagher and Blank, 2012). This is a critical activity in risk management because it provides the foundation for treating the identified risks. Treatment options include risk acceptance for cases in which the risk is at an acceptable level considering the organization's risk appetite; risk mitigation using security controls; risk transfer through the purchase of cyber insurance; or risk avoidance through removing the affected asset. There are several core concepts in risk assessment, such as assets, vulnerabilities, threats, attack likelihood, and impact or cyber harm.

Assets can be defined as any items of value to the organization and can have various properties. Vulnerabilities describe how assets can be exploited and define weaknesses in assets or in the risk controls put in

place to protect them. A threat is the action that could adversely impact an asset and typically involves exploiting a vulnerability. Cyber risk is the combination of these concepts; it considers the likelihood of a successful threat or attack occurring and the harms that could result to assets.

Although, each service in IoT environment has some QoS factors for service evaluating. The mentioned factors will be evaluated in the total possible compounds of IoT environment. Five important factors have been defined as follows:

- Time: Time is the interval from a submitting request and responding to it. Typically, it is measured in milliseconds as a time unit.
- Cost: The payment of a specified sum of money to order the action that it has needed to do.
- Scalability: The capacity to be altered and reformed in various conditions in a IoT environment.
- Optimization: The process of finding the best or most effective service combination by applying the appropriate methods.
- Efficiency: The ratio of the mechanism to the total cost and time taken.

4. Research Methodology

In order to have a clear picture of the energy saving mechanisms in Internet of things (IOT), this section provides a systematic literature review (SLR) of energy saving and energy-aware mechanisms with a specific focus on researches related to computer networks and IT. Previous researchers have argued that using such an approach to review literature can ensure that the systematic error is limited, chance effects are reduced, and the legitimacy of data analysis is enhanced (Buller and McEvoy, 2012, Fraj et al., 2015). All of these benefits lead to more reliable results that form the basis for drawing conclusion (Buller and McEvoy, 2012, Fraj et al., 2015). Article selection process is described in section 4.1.

4.1. Article selection process

The process of choosing the articles in this paper for a systematic literature review is conducted in four steps, including:

1) Automated search based on keywords and papers language;
2) Article filtering by selecting Non-review articles based on publication year, quality of the publisher, reputation and validity of the journals;
3) Selecting related articles based on the title of papers and abstract;
4) Final evaluation based on analyzing the full text of selected papers from previous steps;

Figure 1: Process steps of choosing the articles in a SLR

4.1.1. Step 1: Automated search

The search process is conducted via electronic searching on online scientific databases. Therefore, first, we identify electronic databases to find an article for which the following famous databases were used:

- Google scholar (https://scholar.google.com/)
- Springer (http://link.springer.com/)
- IEEE explorer (http://ieeexplore.ieee.org/)
- Science Direct (http://www.sciencedirect.com/)
- Sage (http://online.sagepub.com/)
- Taylor (http://www.tandfonline.com/)
- ACM (http://www.acm.org/)
- Scientific (http://www.scientific.net/)
- Emerald (http://www.emeraldinsight.com/)

Keywords selected and searched to find relevant articles in this step are “Internet”, “Things”, “IoT”, “Risk”. In addition, to make sure of finding all papers about this subject, all synonyms and alternative spellings of the main elements have been added, hence, the following search string was defined:

- “Risk” OR “Risks” "Internet" "Thing" OR "Things"
- “Risk” OR “Risks” "IoT"

The result of the search without having language filter was 101 articles from journals, conference papers, books, chapters, thesis, notes and any articles in which a part of these keywords were mentioned. After applying English language filter, the number decreased to 94.

4.1.2. Step 2: Article filtering

We found 94 articles at searching articles in Step 1. This step begins with the selection of certain practical screening criteria to ensure that just high-quality publications and articles are included in the review (Reim et al., 2015). The search string was limited by searching at most for journal and conference articles as they obtain validated empirical results. Therefore, all other types of studies were excluded in the initial search. During the first search, working paper, revolution editorial note commentaries and book review articles were excluded, the main aim to be a focus on quality publications (Seuring and Müller, 2008).

Figure 2: Percentage of published article in any publication

By means of this strategy, we have found 82 articles in step 2 which are shown in Figure 2. Where 1% of the articles are related to Emerald, 1% of the articles are related to Scientific, 3% of the articles are related to Science Direct, 4% are related to Taylor & Francis, 5% are related to Springer, 6% are related to ACM, 28% are related to IEEE, and 52% are related to other publications. In addition, Figure 3 illustrates the number of published articles between 2010 and 2017. A serious attraction to risk topic in IoT is shown from year 2015.

Figure 3: Total number of articles released in every year

4.1.3. Step 3: Topic relation

44 conference articles, book sections and thesis, 3 review articles, and 5 articles which were published before 2013 were removed. At the end, the proposed method in each article has been investigated and 29 articles were selected that their method is directly related to the risk assessment in IoT. **Error! Reference source not found.**, shows details of the selected articles such as publication year, journal, and authors.

Table 1: Details of the selected articles

4.1.4. Step 4: Final evaluation

In this step, the full body of the selected papers from the previous step are examined for finding the appropriate papers for review. We select the paper that:

1.Explained proposed method obviously and clearly,
2.determined the research goals and risk assessment parameters,
3.Provided and explained the dataset clearly.

The reason for selecting these criteria is that reviewing the well-written articles can help and boost the researchers to do the future works mindfully. This step results in selection 11 article where are indicated in the last column of **Error! Reference source not found.**.

5. Review of the selected risk-based mechanisms in IoT

In this section, 11 selected articles will be reviewed. In addition, their techniques, basic properties as well as their diff erences, advantageous and disadvantageous will be discussed and described. The approaches in the literature can be divided into 3 distinct categories including risk-based assessment and management, Framework and models. Classification of methods and its definition are illustrated in Fig. 4. In Sections 5.1 to 5.3, these methods and their examples are provided.

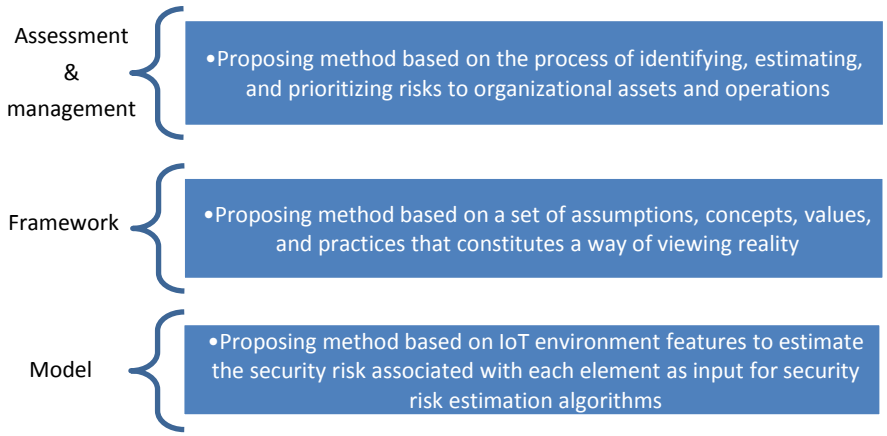

Figure 4: Classification of risk-based methods in IoT.

On the other hand, according to the goal of the mechanism, many parameters were determined. We investigate on of article simulation results and comparing them with mechanism goals to identify which parameters are improved and which one is attenuated. "+" and "-" are used to show the parameters (time, cost, efficiency, optimization, scalability) improvement, weakening and "??" to say that it's not mentioned in the article. These parameters were explained clearly in Section 3.

5.1. Risk-based assessment and management

In this section, first the IoT risk assessment or management mechanisms and their basic properties are described in Section 5.1.1. Then 4 IoT risk assessment or management mechanisms are discussed in Section 5.1.2. Finally, their diff erences, advantageous and disadvantageous are discussed and compared in Section 5.1.3.

5.1.1. Overview of the risk-based assessment and management

IoT risk assessment or management mechanisms are needed to identify, estimate, and prioritize risks to organizational assets and operations. There are several core concepts in risk assessment, such as assets, vulnerabilities, threats, attack likelihood, and impact or cyber harm.. In Section 5.1.2, some risk-based assessment will be shown.

5.1.2. Overview of the selected risk-based assessment and management

Kotenko et al. (2015), proposed the methods of fuzzy inference and fuzzy clustering, classification and ranking intended for security risk management in IoT. The considered approach allows keeping the main target functions of the network and application layers of IoT for security risk management. Further directions of research are associated with automatic parameter setting of the developed algorithms depending on the analyzed features.

Ziegler et al. (2016), presented some views on IoT, crowdsourcing and systemic risk management with a focus on smart cities. First, they clarified the notion of risk and risk management from ISO 31000 perspective and presenting the IoT Lab European research project on crowdsourcing and Internet of Things (IoT), with an overview of its architecture and approach. Then, they explored more specifically the potential use of IoT and crowdsourcing by reducing the level of uncertainty and potential deviation, to systematically reduce risks for smart cities.

Xi and Ling (2016), studied the causes of privacy security risks, and put forward some relevant IoT risk prevention methods. They could not have any simulation experiment research for each specific type of those risks

because of the limitation of some data acquisition about IOT. These research results have some certain practicalities, which would provide an important theoretical reference.

Yan et al. (2017), discussed the risks of the agricultural supply chain under IoT. They classified and summarized the risks of the current agricultural supply chain through qualitative analysis. Also, measured the size of the risk factors from a quantitative perspective based on a mathematical model. In addition, according to the calculations of the model, several measures of risk management and control are proposed for the agricultural supply chain under IoT.

5.1.3. Summary of risk-based assessment and management

risk-based assessment and management in IoT is one of crucial topics for improving network efficiency and prolonging network lifetime. Scope, Goal and Approach of the authors are shown in table 5 and side-by-side comparison of the opted techniques as well as their main advantage and weakness are shown in Table 3.

5.2. Risk-based frameworks

In this section, we first describe the risk-based frameworks proposed in IoT and their basic properties in Section 5.2.1. Second, we discuss the 4 selected risk-based frameworks in Section 5.2.2. Finally, their differences, advantages, and disadvantages are discussed and compared in Section 5.2.3.

5.2.1. Overview of the risk-based frameworks

The framework-based mechanisms are based on a set of assumptions, concepts, values, and practices that constitute and form a way of viewing reality. The framework-based mechanisms are utilized in order to Analyze, organize and manage risks by completely novel approaches. In Section 5.1.2 some framework-based mechanisms will be shown.

5.2.2. Overview of the selected risk-based frameworks

Mohsin et al. (2017), presented IoTRiskAnalyzer, which was a novel framework for automated verification and probabilistic quantification of attack likelihoods against generic IoT system configurations. The reports delivered by IoTRiskAnalyzer can help IoT engineers to select the best possible system and policy configurations from a security standpoint. The framework can also assist in analyzing the impact of component-level vulnerabilities over system-level threats.

Saint and Garba (2017), presented an insurance model for the Internet of Things. At first, they argued that an IoT insurance system would distribute IoT risk more equitably, improve security, provide funding for addressing large scale incidents, and build trust in IoT systems for users. Secondly, they presented IoT insurance models and argued that IoT insurance should be offered by companies beyond traditional insurers, such as internet service providers (ISPs), telephone companies, and cloud service providers since they have experience assessing and managing security technology and Internet users. Third, they discussed regulations and argue that regulation would help establish what is currently an immature market in a mature industry, and encourage standardization in products and procedures similar to the way insurance in more traditional markets is regulated.

A dynamic occupational safety and health (OSH) risk management within the smart working environments (SWE) was developed by Podgórski et al. (2017). The framework was based on continuous assessment of risks in a real-time manner, and the capacity to assess and monitor the risk level of each worker individually. The SWE was viewed as being composed of two partly overlapping spheres: the Manufacturing Sphere and the Worker Sphere. Networks of integrated smart objects that should act collectively to fulfil two equal and complementary objectives cover these spheres: firstly, to ensure workers' safety and comfort secondly to maintain the highest possible productivity and quality of manufacturing processes. Their goal was to attain a level of embodiment of electronic and computing devices into various smart objects of the SWE, at which they become indistinguishable from these objects, and are able to efficiently perform safety functions in a user-friendly manner with respect to the requirements of the users and the society.

Blinowski (2017), proposed a risk-based decision-making framework for the perception layer of IoT systems. Its major feature was that local decision-making (done by the sensor node) was based on risk estimates pre-

calculated at the cloud level. This approach was suitable for large-scale perception layer systems, since it keeps the trust-based "fine-grained" decision purely local. On the other hand, the risk information used to measure the feasibility of transactions in a given global context is provided by the cloud level.

5.2.3. Summary of risk-based frameworks

The framework-based mechanisms are utilized in order to Analyze, organize and manage risks via applicable approaches. Scope, Goal and Approach of the authors are shown in table 5 and side-by-side comparison of the opted techniques as well as their main advantage and weakness are shown in Table 3.

5.3. Risk-based models

In this section, we first describe the risk-based models proposed in IoT and their basic properties in Section 5.3.1. Second, we discuss the 2 selected risk-based models in Section 5.3.2. Finally, their differences, advantages, and disadvantages are discussed and compared in Section 5.3.3.

5.3.1. Overview of the risk-based models

At its highest level risk-based modeling is a discipline in its own right that requires various factors to be statistically analyzed in order to quantify the risk(s). The risk-based models which is based on the analysis of assets, vulnerabilities, risks and etc. has a view to assessing their impacts on the system as a whole. In Section 5.2.2, the selected risk-based models and their anatomy are discussed.

5.3.2. Overview of the selected risk-based models

Johny et al. (2014), presented and discussed various approaches used in data discovery and integration. They extended the discussion to include social search engines, ranking techniques as well as social graph as approaches that use social network to discover important online resources. The authors articulated the drawbacks of the various approaches with the aim to provide evidence showing the limitations that motivated the proposal of a social graph modeling approach.

Developing a dynamic and adaptive risk-based access control model for the IoT was proposed by Atlam et al. (2017). This model can adapt to IoT changing conditions and can be realized by estimating the security risk using IoT real-time features at the time of the access request to make the access decision. The model used user context, resource sensitivity, action severity and risk history as inputs to estimate the overall risk value associated with each access request. They prevented any misuses from authorized users using smart contracts and provided adaptive features to monitor user behavior.

Gebrie and Abie (2017), proposed a novel risk-based adaptive authentication model for IoT in Smart Home eHealth to identify the activities of the user and to verify the validity of the sensor nodes. The model used a naïve Bayes machine learning algorithm to classify the channel characteristics variation between sensor nodes and their gateway. According to the observed variation of channel characteristics, the model assess the risk to determine the probability of the device in question being compromised, based on the risk score obtained from the assessment the model selects an authentication decision suitable for the particular risk score.

5.3.3. Summary of risk-based models

The selected risk-based models are discussed in the previous section. The important factor that has increased with all of the risk-based models is optimization. Scope, Goal and Approach of the authors are shown in table 5 and Side-by-side comparison, advantages, and disadvantages of the discussed methods are showed in Table 6.

6. Results and comparison

7. Open issues

Methods of fuzzy inference and fuzzy clustering, classification and ranking intended for security risk management in IoT are optimized sufficiently but further directions of research are needed to have an automatic parameter setting of the developed algorithms depending on the analyzed features. The IoT privacy security risks can be characterized in political, economic, and personal fields, each of these forms would bring many privacy security risks and deserves great attention in the future researches. Developing or optimizing current frameworks, towards budget-constrained security planning of IoT systems is one of the issues that needs to pay more attention. Creating such a framework will assist non-expert IoT designers to plan, verify and optimize the security of their configurations, within the affordable budget, after putting minimal technical efforts. Developing a Future Internet based framework by incorporating a social graph modeling approach with key requirements for discovering risks in IoT. Choosing the most appropriate risk estimation technique for a specific IoT context is one of the highest priorities to proceed to implement security models as well as creating different IoT access control case studies with data to evaluate the model.

However, because of the limitation of some data acquisition about IOT, it is so difficult to have simulation experiment research for each specific type of those risks. Hope we can obtain a large scaled data in the future, so that we can combine with the risk simulation models for the specific risks in the further studies. In addition, some of the issues involved in risk assessment and management in IoT that needs more investigations in the future are as follows:

- Investigating the potential security risks associated with cryptocurrency use in IoT deployments
- Capturing the risks of machine-to-machine payments and unconventional technologies for frictionless payments, such as implantable devices
- Incorporating unique financial interactions with multiple actors, such as group payments and peer-to-peer lending
- Modernizing the agricultural supply chain to reduce the risks involved in this job for investors, farmers etc.
- Calculating the channel characteristics before making any decision about authentication, access control and privacy

8. Conclusion

In this paper, we have systematically surveyed the past and risk-based mechanisms in IoT environments. First, we overviewed the risk assessment and then risk-based mechanisms in IoT and the problem of risk assessment and management in IoT were discussed. Then, we explained research methodology and investigated risk assessment techniques in three main categories including risk assessment and management, frameworks and models. For each of which, we reviewed and compared several past and risk-based techniques. We also discussed the advantages and disadvantages of the important methods of each category. The challenges of these methods are addressed so that more efficient risk assessment techniques can be developed in future. The framework-based mechanisms are used for organizing and managing risk assesment by novel approaches. The model-based mechanisms are methods based on a component of approach that has been managing risks such as authentication, privacy or user requests. The most important factor that has been focused is optimization of processes, assessments and scalability of the involved systems. The overall data collected in this study help to acquaint the researchers with the risk-based mechanisms in IoT area. We sincerely hope that the outcomes of this work could lead researchers to develop more effective risk-based mechanisms in IoT.