Threat Modeling and Attack Simulations of Smart Cities: A Literature Review and Explorative Study

Robert Lagerström, Wenjun Xiong and Mathias Ekstedt
School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden

Keywords: Threat Modeling, Attack Graph, Smart City, Systematic Literature Review, Internet-of-Things, Cloud.

Abstract: Digitization has made enterprises and inter-enterprise organizations (e.g. smart cities) increasingly vulnerable to cyber attacks. Malicious actors compromising computers can have potential damage and disruptions. To mitigate cyber threats, the first thing is to identify vulnerabilities, which is difficult as it requires (i) a detailed understanding of the inter-enterprise architecture, and (ii) significant security expertise. Threat modeling supports (i) by documenting the design of the system architecture, and attack simulation supports (ii) by automating the identification of vulnerabilities. This paper presents a systematic literature review and provides a research outlook for threat modeling and attack simulations of smart cities. The results show that little research has been done in this area, and promising approaches are being developed.

1 INTRODUCTION

Smart cities are completely reliant on information and communication technology (ICT) (Suciu et al., 2013). Technical solutions like the Internet of Things (IoT) and cloud computing are key concepts driving the development (Jin et al., 2014), and a lot of their focus is on functional ICT aspects, i.e. providing new innovative solutions to problems in e.g. energy, mobility, and infrastructure integration. This focus together with the speed of development and implementation causes issues when it comes to non-functional aspects, and specifically security (Elmaghraby and Losavio, 2014). For instance, a bi-partisan group of American senators is sponsoring legislation to secure IoT, and comparing it to weapons of mass destruction [1]. Swedish radio [2] reported that over 7000 Swedish systems were found with security flaws, including more than 1000 systems missing password authentication for controlling e.g. sewage, heat, and fire alarms. Lists of the worst hacks in IoT include large distributed denial-of-service attacks, hackable cardiac devices, baby heart monitors and cars, and spying webcams[3], which are just some examples taken from popular media. Researchers are worried about this phenomenon, and some emphasize the challenges and opportunities (Holm et al., 2015), while others focus more on possible solutions (Ning and Liu, 2012). They all seem to agree that the security challenges for smart cities are massive, and must be handled for all the possible benefits to reach their full potential. Also, the issues are difficult to address, and that there is a need for both detailed solutions for specific attacks and holistic solutions to consider the whole picture. There are significant research and development efforts directed toward specific defenses e.g. cryptography, anti-virus, intrusion prevention, and firewalls, but less targeting holistic approaches.

One such holistic solution is threat modeling and attack simulation of ICT architectures (Ekstedt et al., 2015; Johnson et al., 2016a; Johnson et al., 2016b). However, the methods and tools available today are generally focused on a comparatively small scope, e.g. one connected car (Katsikeas et al., 2019).

In this paper, we conduct a systematic literature review (SLR) for large-scaled ICT in smart cities,

[1]http://denver.cbslocal.com/2017/09/12/internet-of-things-cybersecurity/

[2]http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=6825512

[3]https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

Lagerström, R., Xiong, W. and Ekstedt, M.
Threat Modeling and Attack Simulations of Smart Cities: A Literature Review and Explorative Study.
DOI: 10.5220/0008921903690376
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 369-376
ISBN: 978-989-758-399-5; ISSN: 2184-4356

and the 25 papers studied show that there is no solution so far, where e.g. connected cars and power systems are part of the same systems-of-systems. Instead, our SLR had to focus on the few initiatives, where the core aspects of smart cities e.g. IoT and cloud are addressed.

To further investigate and discuss these issues, we also arrange a workshop with ten participants from a Swedish industry working in IT or IT-security positions. The conclusions from the workshop are that: (i) Since threat modeling is promoted for single organizations to handle the complexity of infrastructure and risks, it should also be a good approach for larger systems-of-systems. (ii) Many threats, attack types, and countermeasures in smart cities are the same as for single organizations but are integrated to form a larger network, where each island is owned by different legal entities. This would most likely mean that every actor creates a detailed threat model of their domain (their island) with outgoing and incoming dependencies to other actors, and a systems-of-systems-wide (e.g. city) actor is responsible for collecting and integrating the models to get the complete picture.

2 RELATED WORK

Popular threat modeling tools and methods for application development include the Microsoft Threat Modeling Tool[4] with the related STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege) and DREAD (**D**amage, **R**eproducibility, **E**xploitability, **A**ffected users, **D**iscoverability) models.

When it comes to holistic threat modeling in a more system-wide perspective, one of the most well-known initiatives would be UMLsec, an extension of UML for secure systems development (Jürjens, 2002).

Modeling and doing security analysis in many threat modeling approaches requires security expertise. Also, the analysis is often complex and time-consuming. To deal with these issues, attack trees were proposed (Schneier, 1999).

In an attack graph, nodes represent attacks and countermeasures, and edges represent how these relate to each other. Depending on your interests, the values and algorithm implemented can analyze different aspects, such as **T**ime-**T**o-**C**ompromise (TTC), attack success likelihood, loss of money, business impact, CIA (**C**onfidentiality, **I**ntegrity, **A**vailability), etc.

To decrease the manual efforts of creating attack graphs and analyzing threat models, there are initiatives combining the two. The **Cy**ber **Se**curity **Mo**deling **L**anguage (CySeMoL) is a modeling language for enterprise-level system architectures coupled to a probabilistic inference engine (Holm et al., 2015). pwnPr3d is an attacker-centric threat modeling approach that allows for automated threat identification and quantification based on a model of the network under analysis, by combining a network architecture modeling language and a probabilistic inference engine. It allows probability distributions over the **T**ime-**T**o-**C**ompromise (TTC) for attack steps by quantifying the attack step (conditional) dependencies (Johnson et al., 2016a). There are a few commercial tools for attack simulation threat modeling e.g. securiCAD by foreseeti[5] (Ekstedt et al., 2015). Recently, the **M**eta **A**ttack **L**anguage (MAL) was proposed for the design of domain-specific attack languages (Johnson et al., 2018), e.g. vehicleLang (Katsikeas et al., 2019).

We have only found one systematic literature review on threat modeling, which focused on threat modeling in general (Xiong and Lagerström, 2019). However, so far there is no systematic literature review on threat modeling for smart cities.

3 REVIEW METHODOLOGY AND RESULTS

Following the guidelines of Booth et al. (2012), we did a literature search on October 2nd and 3rd, 2018. Google Scholar was used as the search engine for academic work with titles on the chosen topic. Only texts in English, and only articles in computer science, software engineering or related fields were collected. Keywords “smart city” and “viable city”, combined with “threat modeling”, “attack graph”, “attack tree”, and “attack simulation” gave a result of 1 paper. Since the core of the smart city concept includes the Internet of Things (IoT) and cloud, we extended our search with these keywords, which gave us an additional 27 papers, three of which were manually discarded since these were versions of a paper already present in the collected set (e.g.,

[4] https://www.microsoft.com/en-us/download/details.aspx?id=49168

[5] www.foreseeti.com

Aydin and Jacob, 2016). Thus, the final number of included papers is 25. The search process used in this work can be seen in Figure 1.

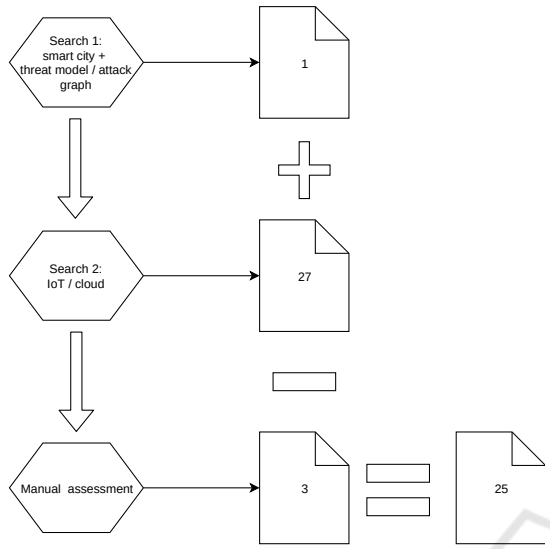

Figure 1: Search process for the systematic literature review.

3.1 General Information

According to the review results, sixteen of the collected papers focus on threat modeling and nine on attack graphs (or attack trees). Only one has smart cities as its domain. Three papers focus on IoT, the plurality of papers (21 papers) focus on cloud computing or cloud storage. In Figure 2, we visualize the relationship between the approaches, i.e. threat modeling (TM) or attack graphs (AG), and the application domain, i.e. smart city (SC), IoT, or Cloud.

The plurality (18 out of 25) of the papers are published in conference proceedings and 7 in journals. None of the papers are published in the same outlet. The conferences range from general IT conferences, e.g. *Americas Conference on Information Systems (AMCIS)* and *IEEE International Conference on Computer & Communications*, to cloud or IoT specific ones e.g. *IEEE 4th World Forum on Internet of Things (WF-IoT) and IEEE International Conference on Cloud Engineering (IC2E)*. Also, general security conferences e.g. *International Symposium on Foundations & Practice of Security*, and most importantly security conferences for smart cities (cloud and IoT) e.g. *International Conference on Cyber Security of Smart cities, Industrial Control System & Communications (SSIC)* and *International Conference on Cloud Security Management* are on the list of outlets for this type of work. For the journal publications, the papers found are mostly published in general outlets such as *Journal of Applied Sciences, International Journal of Intelligent Computing Research (IJICR)*, and *IOSR Journal of Computer Engineering (IOSR-JCE)*. Only one is published in a security journal, which is *International Journal of Network Security & Its Applications (IJNSA)*.

Two people have authored more than one paper and both are co-authors of the same two papers, where (Gholami et al., 2016) is an extension of (Gholami and Laure, 2016).

The top five cited papers (8-30 citations) are all published in conference proceedings by first authors with North American or European affiliations (see in Table 1 for more information).

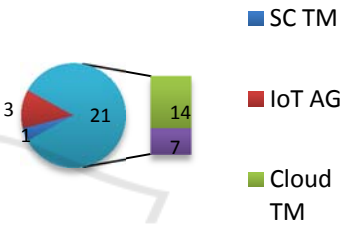

Figure 2: Among the 25 studied papers, 21 are focused on work related to the cloud, with 14 on threat modeling (TM) and seven on attack graphs (AG). One paper is focused on TM for smart cities, and three on AGs and IoT.

Table 1: Top five cited papers.

Author, Title, Outlet, Year.	Citations
Ingalsbe, J. et al., "Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise," *Americas Conference on Information Systems (AMCIS)*, 2011	30
Wang, P. et al., "Data security and threat modeling for smart city infrastructure," *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015.	17
Alhebaishi, N. et al., "Threat modeling for cloud data center infrastructures," *International Symposium on Foundations and Practice of Security*, 2016.	11
Kammüller, F. et al., "Attack tree analysis for insider threats on the IoT using Isabelle," *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2016.	10
Schilling, A. and Werners, B., "A quantitative threat modeling approach to maximize the return on security investment in cloud computing," *International Conference on Cloud Security Management*, 2013.	8

Ten countries on four continents are represented (counting the first author affiliation): eleven from

Asia, nine in Europe, four from North America, and one in Africa.

A few papers are fairly short (perhaps by some defined as short papers), to be more specific, fourteen papers have no more than 7 pages.

The oldest paper is from 2011 and each year until 2018, one to four papers were published, except for 2016 that nine papers were published.

3.2 Detailed Information

Among the found 25 papers, eleven presented studies use an existing threat modeling (TM) or attack graph (AG) - based method (cf. Table 2), and 14 propose a new (or improved) TM or AG to the based method (cf. Table 3).

Table 2: Papers employing an existing threat modeling or attack graph-based method.

Ref.	Employ existing TM or AG method
Alhebaishi et al. (2016)	Employs threat modeling of cloud data center design.
De et al. (2016)	Proposes re-classification of attacks on P2P networks using goal-based threat modeling.
de Souza and Tomlinson (2014)	Investigates the no hypervisor architecture using a threat model.
Ingalsbe et al. (2011)	Uses the Enterprise Threat Modeling (ETM) methodology to identify, assess, and mitigate risk in cloud computing, mobile toting, and consumerized enterprises.
Wen (2014)	Employs an attack graph on a university cloud infrastructure.
Nagaraju and Parthiban (2015)	Analyzes configurations of authentication access points in cloud using attack graphs.
Sahay et al. (2018)	Uses attack graphs for vulnerability assessment of IoT.
Sharma (2017)	Uses a threat model to recognize the most insecure threats of security in cloud computing.
Subasinghe et al. (2014)	Analyzes social media network data using attack trees.
Torkura et al. (2018)	Uses a threat modeling approach for measuring security threats in cloud storage brokers.
Zimba et al. (2016)	Employs attack trees to analyze man in the cloud attacks.

Looking at what types of data and validation methods the papers are based on we find that among the 14 papers proposing a new or improved method, five of them have no data or unclear data for validating or testing their proposed approach, and the other nine papers report data use - a case study (Kazim and Evans, 2016), examples (Kammüller et al., 2016; Schilling and Werners, 2013), and experimental implementations (cloud environments, virtual machines) (Gholami et al., 2016; Kamongi et al., 2014; Ngenzi et al., 2016), with some also including vulnerability data (Manzoor et al., 2018; Mjihil et al., 2017; Wang et al., 2018).

Table 3: Papers making a methodology contribution to threat modeling or attack graphs.

Ref.	Proposing a new or improved TM or AG method
Amini et al. (2015)	Proposes a dynamic threat modeling method.
Aydin and Jacob (2016)	Presents extensibility features to the threat modeling tool Cloud-COVER.
Cheng et al. (2012)	Proposes an approach of security evaluation based on attack graphs in a cloud computing environment.
Gholami and Laure (2016)	Describes an extension of the Cloud Privacy Threat Modeling (CPTM) methodology.
Gholami et al. (2016)	Describes an extension of the Cloud Privacy Threat Modeling (CPTM) methodology (and tests it in a case study).
Kammüller et al. (2016)	Presents an approach to characterizing malicious and unintentional insider threats on the IoT by attack vectors.
Kamongi et al. (2014)	Proposes a novel automated architecture for threat modeling and risk assessment for cloud computing called NEMESIS.
Kazim and Evans (2016)	Presents a threat modeling approach to determine the threats for cloud services.
Manzoor et al. (2018)	Proposes a threat modeling approach for cloud ecosystems based on Petri nets and Design Structure Matrices.
Mjihil et al. (2017)	Proposes a framework for improving attack graph scalability for the cloud.
Ngenzi et al. (2016)	Proposes a threat modeling approach that prevents attacks that may affect the virtual machines on the cloud.
Schilling and Werners (2013)	Proposes a quantitative threat modeling approach to evaluate and increase the security of cloud-based systems.
Wang et al. (2018)	Presents a vulnerability assessment framework based on attack graphs.
Wang et al. (2015)	Proposes an approach to analyze threats and to improve data security of smart city systems.

Among the 25 analyzed papers, some interesting future work are outlined - extend the scale and scope of existing efforts (Alhebaishi et al., 2016), deploy a novel model to define new threats which are more critical (Amini et al., 2015), build a prototype (Gholami et al., 2016), graphically represent the risk identified in threat models (Ingalsbe et al., 2011), integrate with quantitative analysis (Kammüller et al., 2016), dynamically assess any given cloud environment and be able to detect and prevent new zero-day type of weaknesses (Kamongi et al., 2014), identify simulated attacks in multiple systems on the cloud (Ngenzi et al., 2016), representation of uncertainty (Schilling and Werners, 2013), develop a fully automated risk management framework (Subasinghe et al., 2014), implement automatic

security configuration methods (Torkura et al., 2018), and improve the threat library to shorten the threat assessment life cycle (Wang et al., 2015). Noticeably, eight papers do not outline any future work and six papers focus their future work entirely on specifics of their approach.

4 WORKSHOP

To further investigate and discuss these issues in large-scaled ICT in smart cities, a cyber security workshop was arranged on November 20th, 2018 with the topic of security beyond enterprise architecture (systems-of-systems in smart cities). The workshop lasted for one hour and fifteen minutes and was a part of a National executive course in cyber security hosted by the University. The ten participants have roles such as IT architect, head of system management & IT, senior adviser IT, IT responsible, chief of operative IT security, and CEO. They come from organizations such *as the National Energy Agency*, *National Defense*, *National department of traffic*, a smaller power utility company, and an investment management company.

During the workshop, the participants first discussed the risks and threats in smart cities, then continued the discussion with what types of attacks can be exploited for such threats, followed by what countermeasures one can implement to prevent such attacks.

Finally, the participants discussed the differences between a single organization (enterprise architecture) and an ecosystem of organizations (incl. individuals) such as a smart city, and also how these differences could affect threat modeling approaches.

4.1 Threats, Attacks, and Countermeasures in Smart Cities

Smart city threats that were discussed include lacking personal integrity, disrupting societal functions such as healthcare, energy, water, and waste, manipulating data creating economic damage, as well as terror attacks e.g. using vehicles, etc.

Typical attacks discussed regarding the mentioned threats were denial-of-service, man-in-the-middle, zero-day vulnerabilities, and known vulnerabilities (due to not patched or none hardened IoT products), etc.

According to the participants of the workshop, countermeasures could be the usual suspects such as hardening, patching, network segmentation and isolation, SIEM, IDS, IPS systems, and active monitoring using AI, etc.

4.2 Differences between Single Organizations and the Smart City Ecosystem

During the workshop discussions, the participants talked a lot about the differences between one single organization and the network of organizations and technology as a part of a smart city and how this influences approaches such as threat modeling and attack simulations. Some findings are presented below:

(i) For one organization, it is usually clear who owns technology and data, as well as who is responsible for the security and potential flaws. For a smart city, there are plenty of scenarios where ownership and responsibility are unclear.

(ii) The attack surface is already large and complex in an organization but will become much larger and more complex within smart cities, opening up new avenues of potential attacks.

(iii) There are also large areas of unclear juridical issues especially with having national state-owned organizations in the ecosystem.

(iv) Simple bugs or vulnerabilities in peripheral small IoT devices might have a huge impact on completely different parts of the system, especially since patching and hardening these might be difficult.

(v) Trust between different parties in a smart city is needed to share data and infrastructure. For instance, with threat modeling, you might need to share sensitive information about technology and vulnerabilities with others.

4.3 Threat Modeling and Attack Simulations for Smart Cities

Since threat modeling is promoted for single organizations to handle the complexity of infrastructure and risks, one could assume that it would also be a good approach for larger systems-of-systems. Looking at the threats, attack types, and countermeasures discussed for smart cities, many are the same as for single organizations, but are further integrated to form a larger network, where each island is owned by different legal entities.

Using threat modeling and attack simulation approaches in systems-of-systems owned and managed by different actors, would most likely mean that, every actor creates a detailed threat

model of their domain (their island) with outgoing and incoming dependencies to other actors, and a systems-of-systems-wide (e.g. city) actor is responsible for collecting and integrating the models to get the complete picture.

5 DISCUSSION

In this section, the results are discussed, and the limitations of the work are addressed.

5.1 Results Discussion

It was a surprise to us to find that, only one paper focuses on threat modeling or attack graphs for smart cities. Both of them are up and coming fields that can benefit greatly if combined. Security should be a priority if the smart city dream is to come true, and especially the use of proactive methods for designing a secure smart city infrastructure from the beginning.

21 out of the 25 papers found are focused on securing cloud infrastructure. This is an indication that cloud work is more mature when it comes to proactive security, while IoT is still focused more on functionality. This is also what we can see in the media, where IoT products are being hacked all the time. While the cloud providers have been fairly spared, it is our true belief that we need to put more focus on designing secure IoT products and that threat modeling can be of great assistance here.

None of the papers in the SLR have been published in the same outlet, and the majority have been published in conferences (and according to our expertise in the area, not the most prestigious ones). This is another indicator that the field of threat modeling is still fairly immature and has not found its place in the academic community (there is no Journal or Conference of Threat Modeling yet). The lack of data used for validation makes it difficult for new approaches to be published in high impact journals.

The participants of the workshop concluded that, for smart cities, it is expected that it will be the same type of attacks and countermeasures as in single organizations today, just on a larger scale, and with some added issues regarding ownership and responsibilities. Threat modeling will be of assistance with some of these issues, but the same problem of modeling responsibility and data ownership (liability) will be present for these approaches as well.

The context of smart cities (and other inter-organizational scoped digital infrastructures) also poses new demands for threat modeling, which has largely grown from a single system development perspective as discussed in the workshop. The progression to meet this demand includes the development of efficient methods for automatic support for threat modeling, as well as the development of ontologies and domain-specific languages appropriate for the scope of the target system environment. Such work is also ongoing. Another, perhaps newer need, is to be able to share threat models and results from analyzing them. This topic is close to the domain of cyber threat intelligence and its need for information sharing. A natural evolution for threat modeling would be to move into standardization and develop something like the Structured Threat Information Expression (STIX) and its accompanying communication protocol the Trusted Automated Exchange of Intelligence Information (TAXII)[6]. Combing the topics of threat modeling and threat intelligence is largely a natural evolution that would be beneficial to both domains. Maybe we will see a future version of STIX/TAXII covering also threat models and a specific smart city STIX language.

5.2 Limitations

There are some limitations of our systematic literature review. We tried to go broad by using Google Scholar rather than a set of individual databases, which is a more common way of doing it. This would have given us a much smaller number of papers to work with since many of the journals and conferences are not indexed in the high-quality databases. We chose quantity over quality this time.

Threat modeling and attack graphs might not be the only approaches to do similar types of proactive security work (using graphical models for security analysis). Thus, we might have missed some work, but it is still unclear to us what that would be.

Although plenty of sources list IoT and cloud infrastructure as the main technologies for smart city development there could be other technologies we have not looked at.

The participants of the workshop were chosen in a higher learning course in security and not based on their skills and expertise for this purpose. However, we still believe that they know necessary for the

[6]The OASIS Cyber Threat Intelligence Technical Committee, https://oasis-open.github.io/cti-documentation/

types of discussions we had. We have to keep in mind that their views on the issue represent a narrow set and are most likely not statistically significant.

6 CONCLUSIONS

One can conclude from the systematic literature review that, few of the approaches used or proposed have taken the whole systems-of-systems into account in their work, instead, most focus on securing one single IoT device or the internals of a specific cloud solution. How to deal with the complexities of a smart city, and where there are many different types of technologies, huge amounts of assets (e.g. all the IoT devices are spread out)? The technology, data, et cetera developed, implemented, used, owned, and maintained by different organizations have not been considered yet in any found materials, which was also the main point discussed in the workshop, and suggested to be needed.

Future work includes proposing a smart city threat modeling and attack simulation method based on the Meta Attack Language (MAL) (Johnson et al., 2018), and validate it with test cases that are similar to (Xiong et al., 2019) and real-world case studies (similar to Lagerström et al., 2010).

ACKNOWLEDGEMENTS

This work has received funding from the Swedish Energy Agency in the Viable Cities program.

REFERENCES

Alhebaishi, N., Wang, L., Jajodia, S., and Singhal, A. (2016). Threat modeling for cloud data center infrastructures. International Symposium on Foundations and Practice of Security. Springer.

Amini, A., A.R., N. Jamil., and Z`aba, M.R. (2015). Threat modeling approaches for securing cloud computing. Journal of Applied Sciences, 15(7).

Aydin, M., and Jacob, J. (2016). Providing Extensibility to Threat Modelling in Cloud-COVER's Underlying Analysis Model. 2016 European Intelligence and Security Informatics Conference (EISIC), pages 45-51.

Booth, A. A., Papaioannou, D., and Sutton, A. (2012). Systematic approaches to a successful literature review. Los Angeles: SAGE.

Cheng, Y., Du, Y., Xu, J., Yuan, C., and Xue, Z. (2012). Research on security evaluation of cloud computing based on attack graph. Cloud Computing and Intelligent Systems (CCIS), IEEE 2nd International Conference on Cloud Computing and Intelligence Systems (CCIS). IEEE.

De, S., Barik, M. S., and Banerjee, I. (2016). Goal Based Threat Modeling for Peer-to-Peer Cloud. Procedia Computer Science, 89: 64-72.

de Souza, W. A. R., and Tomlinson, A. (2014). A Threat Model for a Cloud Infrastructure with no Hypervisor. International Journal of Intelligent Computing Research (IJICR), 5(1): 391-397.

Ekstedt, M., Johnson, P., Lagerström, R., Gorton, D., Nydrén, J., and Shahzad, K. (2015). Securi cad by foreseeti: A cad tool for enterprise cyber security management. In 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, pages 152-155. IEEE.

Elmaghraby, A. S., and Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research, 5(4): 491-497.

Gholami, A., and Laure, E. (2016). Advanced cloud privacy threat modeling. In proc. of the sixth International conference on Computer Science and Information Technology (CCSIT).

Gholami, A., Lind, A., Reichel, J., Litton, J., Edlund, A., and Laure, E. (2016). Design and implementation of the advanced cloud privacy threat modeling. International Journal of Network Security and Its Applications (IJNSA), 8(2): 103-122.

Holm, H., Shahzad, K., Buschle, M., and Ekstedt, M. (2015). P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language. IEEE Transactions on Dependable and Secure Computing, 12(6): 626-639.

Hwang, Y. H. (2015). Iot security and privacy: threats and challenges. In Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, page 1. ACM.

Ingalsbe, J. A., Shoemaker, D., and Mead, N. R. (2011). Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise - an overview of considerations. Americas Conference on Information Systems (AMCIS), page 359.

Jin, J., Gubbi, J., Marusic, S., and Palaniswami, M. (2014). An information framework for creating a smart city through internet of things. IEEE Internet of Things journal, 1(2): 112-121.

Johnson, P., Vernotte, A., Ekstedt, M., and Lagerström, R. (2016a). pwnpr3d: an attack-graph-driven probabilistic threat-modeling approach. In 2016 11th International Conference on Availability, Reliability and Security (ARES), pages 278-283. IEEE.

Johnson, P., Vernotte, A., Gorton, D., Ekstedt, M., and Lagerström, R. (2016b). Quantitative information security risk estimation using probabilistic attack graphs. In International Workshop on Risk Assessment and Risk-driven Testing, pages 37-52. Springer.

Johnson, P., Lagerström, R., and Ekstedt, M. (2018). A Meta Language for Threat Modeling and Attack Simulations. In Proceedings of the 13th International

Conference on Availability, Reliability and Security, page 38. ACM.

Jürjens, J. (2002). UMLsec: Extending UML for secure systems development. In International Conference on The Unified Modeling Language, pages 412-425. Springer, Berlin, Heidelberg.

Kammüller, F. R., Nurse, J. W., and Probst, C. (2016). Attack tree analysis for insider threats on the iot using isabelle. International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer.

Kamongi, P., Gomathisankaran, M., and Kavi, K.M. (2014). Nemesi: Automated Architecture for Threat Modeling and Risk Assessment for Cloud Computing. In Proceedings of the 6th ASE International Conference on Privacy, Security, Risk and Trust (PASSAT).

Katsikeas, S., Johnson, P., Hacks, S., and Lagerström, R. (2019). Probabilistic Modeling and Simulation of Vehicular Cyber Attacks: An Application of the Meta Attack Language. In Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP).

Kazim, M. and Evans, D. (2016). Threat Modeling for Services in Cloud. 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), pages 66-72.

Lagerström, R., Johnson, P., and Ekstedt, M. (2010). Architecture analysis of enterprise systems modifiability: a metamodel for software change cost estimation. Software quality journal, 18(4): 437-468.

Manzoor, S., Zhang, H., and Suri, N. (2018). Threat Modeling and Analysis for the Cloud Ecosystem. 2018 IEEE International Conference on Cloud Engineering (IC2E), pages 278-281.

Mjihil, O., Haqiq, A., and Huang, D. (2017). Improving attack graph scalability for the cloud through SDN-based decomposition and parallel processing. International Symposium on Ubiquitous Networking. Springer.

Nagaraju, S., and Parthiban, L. (2015). Analyzing configurations of authentication access points in cloud using attack graph. 2015 IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS), pages 72-76.

Ngenzi, A., Selvarani, R. and Suchithra. R. (2016). Threat Modeling Based on Randomized Seeding Attacks in Cloud Virtual Machines. IOSR Journal of Computer Engineering (IOSR-JCE), 18(3): 53-60.

Ning, H., and Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. Advances in Internet of Things, 2(1): 1.

Sahay, R., Geethakumari, G., and Modugu, K. (2018). Attack graph - Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pages 308-313.

Schilling, A., and Werners, B. (2013). A quantitative threat modeling approach to maximize the return on security investment in cloud computing. Proceedings of the 1st International Conference on Cloud Security Management, pages 68-77.

Schneier, B. (1999). Attack trees. Dr. Dobb's journal, 24(12): 21-29.

Sharma, A. (2017). Emerging Trends in Safety Issues in Cloud - The Potentials of Threat Model. International Journal on Future Revolution in Computer Science and Communication Engineering, 3(10): 260-263.

Subasinghe, K. D. B. H., Kodithuwakku, S. R., and Perera, H. S. C. (2014). A Risk Management Framework in the Cloud using Big Data and Security Informatics-An Application of Attack Tree for Analysis of Social Media Networks. International Journal of Scientific and Research Publications, 11(4): 1-5.

Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., and Suciu, V. (2013). Smart cities built on resilient cloud computing and secure internet of things. In 2013 19th international conference on control systems and computer science, pages 513-518. IEEE.

Torkura, K. A., Sukmana, M. I. H., Meinig, M., Cheng, F., Meinel, C., and Graupner, H. (2018). A threat modeling approach for cloud storage brokerage and file sharing systems. NOMS IEEE/IFIP Network Operations and Management Symposium. IEEE.

Vlacheas, P., Giaffreda, R., Stavroulaki, V., Kelaidonis, D., Foteinos, V., Poulios, G., and Moessner, K. (2013). Enabling smart cities through a cognitive management framework for the internet of things. IEEE communications magazine, 51(6): 102-111.

Wang, H., Chen, Z., Zhao, J., Di, X., and Liu, D. (2018). A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow. IEEE Access, 6: 8599-8609.

Wang, P., Ali, A., and Kelly, W. (2015). Data security and threat modeling for smart city infrastructure. Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC). IEEE.

Wen, L. (2014). Research on Multilayer Security Audit Research Based on Attack Graph in Cloud Computing. Applied Mechanics and Materials, 644: 3408-3411.

Xiong, W., Krantz, F., and Lagerström, R. (2019). Threat modeling and attack simulations of connected vehicles: a research outlook. In Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP).

Xiong, W. and Lagerström, R. (2019). Threat modeling – a systematic literature review. Computers & Security, 84: 53-69.

Zimba, A., Chen, H., and Wang, Z. (2016). Attack tree analysis of Man in the Cloud attacks on client device synchronization in cloud computing. Computer and Communications (ICCC), 2nd IEEE International Conference on. IEEE.