Computer Networks
Available online 8 July 2022, 109154
In Press, Journal Pre-proof

Review article

Intrusion detection and prevention in fog based IoT environments: A systematic literature review ☆

Cristiano Antonio de Souza [a], Carlos Becker Westphall [a], Renato Bobsin Machado [b], Leandro Loffi [a], Carla Merkle Westphall [a], Guilherme Arthur Geronimo [a]

Show more

Share Cite

https://doi.org/10.1016/j.comnet.2022.109154

Abstract

Currently, the Internet of Things is spreading in all areas that apply computing resources. An important ally of the IoT is fog computing. It extends cloud computing and services to the edge of the network. Smart environments are becoming real and possible through IoT and fog computing. However, they are not free from security threats and vulnerabilities. This makes special security techniques indispensable. Security is one of the biggest challenges to ensuring an optimal IoT and Fog environment. Combined with the significant damage generated by application attacks, this fact creates the need to focus efforts in this area. This need can be proven through existing reviews of the state-of-the-art that pointed out several open aspects that need greater research effort. In this way, this article presents a Systematic Literature Review (SLR) considering the context of intrusion detection and prevention in environments based on fog computing and IoT. This review addresses more than 100 studies that were included after going through an extensive inclusion/exclusion process, with well-defined criteria. From these studies, information was extracted to build a view of the current state-of-the-art and answer the research questions of this study. In this way, we identify the state-of-the-art, open questions and possibilities for future research.

Introduction

The Internet of Things (IoT) is spreading in all areas. The number of devices connected to the Internet continues to grow. Cisco predicts that the number of interconnected devices on the planet could reach 500 billion by 2025 [1]. Its small and inexpensive devices make it possible for objects used in daily life to be connected to the Internet. The idea is to unite the physical and digital worlds by communicating objects with other devices, data centers, and clouds.

IoT devices have limited resources. Thus, there is a need to transfer, through the Internet, the data generated by these devices, to process and store them in a computational center of greater capacity. Cloud Computing [2] has the latency problem caused by the distance between IoT devices and data centers [3]. Fog Computing, however, provides services closer to the end devices [4]. This way, it stores and processes information close to IoT devices, reducing the traffic sent to the cloud [5]. Also, it allows applications that require real-time processing to obtain a faster response.

Motivations. Smart environments are becoming real through IoT and fog computing, but they are not free from security threats and vulnerabilities. Techniques for exploiting computer infrastructure vulnerabilities are continually being improved. Among the main objectives is the acquisition of access to the systems, the obtaining and improper use of confidential information, and causing unavailability of resources. For example, a recent incident involving IoT devices in October 2016, where a botnet Mirai attack on service provider Dyn brought down hundreds of sites, including Twitter, Netflix, Reddit and GitHub, for several hours [6], [7]. Security in these environments is critical as IoT devices are often embedded in people's daily lives and deal with sensitive information. In addition, some systems perform monitoring and perform critical actions, which need to have uninterrupted operation. IoT and fog computing solutions are made up of various technologies, services, and standards, each with its own security and privacy requirements [8]. The IoT paradigm presents several security vulnerabilities that communication networks, cloud services, and the Internet have [8]. However, traditional security tools have difficulties being applied directly in this context due to three fundamental aspects: the limited computing power of the IoT components, the high number of interconnected devices, and the sharing of data between objects and users [9]. Furthermore, the rapid expansion of IoT solutions has left these networks vulnerable to security and privacy risks. The authors Kolias et al. [10] discovered several security vulnerabilities by creating IoT use cases using popular commercial products and services. Among the main attacks present in IoT is Denial of Service (DoS), Distributed DoS (DDoS), Man-In-The-Middle (MITM), routing attacks, and conventional attacks [10]. Security threats related to conventional technologies that are part of the IoT environment can also apply to IoT systems, for example, unsecured connections, malicious code injection, probing, intercepting, fabrication, and modification of messages [11].

The significant damage generated by attacks in this environment creates the need to concentrate efforts in this area [12]. Special security techniques are indispensable in modern computer systems. Intrusion detection is one of the critical points of security, aiming to identify occurrences of attacks. Fog computing consists of a layer that has a greater computational capacity compared to IoT devices and therefore can work with more complex detection models, such as Machine Learning, Deep Learning and Ensemble Learning. However, this environment also has particularities and restrictions. In addition, training complex detection approaches is costly and can overwhelm the fog. Furthermore, due to the distributed nature of fog computing it becomes an ideal environment for employing distributed and collaborative approaches. Finally, fog computing is situated in a strategic position for both detection and execution of post detection actions to protect the IoT environment. Thus, we carried out this review work to obtain an overview of the current state-of-the-art and provide research directions for detecting and preventing intrusions in fog computing and IoT. This study is a Systematic Literature Review (SLR), which has a well-defined research strategy that allows the reproduction or replication of the work and assessment of the integrity of the same [13]. Hajiheidari et al. [14] and Kaur et al. [15] presented SLRs, in different contexts, very well documented, which inspired several methodological decisions regarding the SLR of our work. However, despite the great reviews that exist, there are still important points that need to be addressed. The existing revisions in the state-of-the-art left several general aspects open, as discussed in Section 2. These aspects need to be deeply studied through further reviews to understand the state-of-the-art, the problems and present future research directions. As presented in Section 2, there is no SLR considering the topics covered in this work in the context of fog computing and IoT.

This article presents a survey conducted in the form of a systematic review of the literature on research efforts to detect and prevent intrusions in fog computing and IoT. This review has more than 100 studies, which were included in this review after going through an extensive inclusion/exclusion process, with well-defined criteria, applied to more than ten thousand articles searched in seven reputable databases of scientific articles. Further details of the search and selection process performed are presented in Section 3. From the articles included, a lot of information was extracted to answer the research questions in this study.

With the discussion and analysis performed, we build a vision of state-of-the-art in detection and prevention of intrusion in fog computing and IoT. In addition, we identified the main problems encountered, open questions, challenges, and possibilities for future research.

Contributions. The contributions obtained in this work are presented below:

1. we describe the main machine learning techniques applied in fog computing intrusion detection;
2. we clearly describe the different collaboration strategies employed in distributed intrusion detection approaches;
3. we describe existing strategies to mitigate attacks in fog computing and IoT environments;
4. we present an updated set of datasets that, together with the information extracted, can be an important contribution to future researchers in the decision-making process of their projects.
5. analysis of the weaknesses and difficulties found in state-of-the-art and survey the main open questions and directions for future research.

The rest of this article is organized as follows. Section 2 presents the review works present in the research area. Section 3 presents the systematic mapping protocol, information about planning and execution. In Section 4, the current state-of-the-art in intrusion detection and prevention in fog computing and IoT environments is discussed. In addition, research questions are answered. In Section 5, we discuss the problems found in state-of-the-art, open questions, and possibilities for future research. Finally, Section 6 concludes the article.

Section snippets

Related works

In this section, we summarize the existing SLR and research on the topic studied and highlight their contributions, difficulties and differences in relation to our SLR.

Before carrying out a systematic review procedure, it is necessary to ensure that it is necessary, that is, to verify that there is no similar and high-quality study in the literature. However, in Kitchenham et al. [16], there is no defined procedure for implementing the survey to identify the need to conduct a systematic review...

Methodology of the systematic literature review

As can be seen in Section 2, there is a need for a systematic review procedure on fog and IoT based intrusion detection and prevention approaches. The process of conducting systematic mapping is divided into three stages: planning and construction of the protocol, execution, and summary of the review results. These steps were carried out using the techniques demonstrated in [13], [14], [15], [31], [32], [33]. The Section 3.1 presents the protocol of the search and selection process of articles. ...

Intrusion detection and prevention in fog computing and IoT

The basic feature of IoT is the pervasive presence of a wide variety of intelligent objects in people's daily lives, such as sensors, actuators, mobile phones, among others [35], [36]. The significant heterogeneity, the high number of devices, and the rapid production of the technologies involved in IoT networks can leave them vulnerable to security and privacy risks. These vulnerabilities are used by malicious entities to cause damage [10].

Intrusion Detection Systems (IDS) are an essential...

Issues, challenges and future research directions

This section presents a full discussion of the current state of the art in intrusion detection and prevention in fog computing and IoT, the open questions, and the possibilities for future research.

Table 20 presents a comparison between the various works included in the mapping, considering several characteristics. Regarding the column **D**etection **M**ethod **C**ategory (**DMC**), the works can be classified into anomaly, specification and signature. **D**etection **T**ype (**DT**) indicates whether the job performs **M**...

Conclusions

IoT is spreading in all areas due to its ability to make objects smart. In this way, they can monitor and act on the environment in which they operate. IoT devices have limited resources and need to send information to places with more computing resources. Fog computing then emerged as an excellent processing solution close to devices. IoT and fog are not free from security threats and vulnerabilities. Adding to the significant damage generated by attacks in this environment, this fact creates...

CRediT authorship contribution statement

Cristiano Antonio de Souza: Conceptualization, Methodology, Writing – original draft. **Leandro Loffi:** Data curation, Writing – original draft....

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper....

Acknowledgment

The authors sincerely thank the Federal University of Santa Catarina (UFSC). Also, this study was partially funded by the Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC) and by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Financial Code 001....

Cristiano Antonio de Souza is a PhD student in Computer Science at the Federal University of Santa Catarina (UFSC). He holds a degree in Computer Science from the State University of Western Paraná (2015). Master in Electrical Engineering and Computer Science from the State University of Western Paraná (2018). Participates in research groups: Research Group on Information Security, Networks and Systems (CNPq-UFSC); and Computational Security Research Group (CNPq-UNIOESTE). His research...

References (239)

ReyV. *et al.*
Federated learning for malware detection in IoT devices
Comput. Netw. (2022)

RazaqueA. *et al.*
Energy-efficient and secure mobile fog-based cloud for the Internet of Things
Future Gener. Comput. Syst. (2022)

RahmanM.A. *et al.*
Scalable machine learning-based intrusion detection system for IoT-enabled smart cities
Sustainable Cities Soc. (2020)

KavianiS. *et al.*
Application of complex systems topologies in artificial neural networks optimization: An overview
Expert Syst. Appl. (2021)

DevV.A. *et al.*
Gradient boosted decision trees for lithology classification

KumarP. *et al.*
An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks
Comput. Commun. (2021)

RokachL.
Decision forest: Twenty years of research
Inf. Fusion (2016)

de SouzaC.A. *et al.*
Hybrid approach to intrusion detection in fog-based IoT environments
Comput. Netw. (2020)

AlmianiM. *et al.*
Deep recurrent neural network for IoT intrusion detection system
Simul. Model. Pract. Theory (2020)

de SouzaC.A. *et al.*
Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments
Comput. Electr. Eng. (2022)

View more references

Cited by (0)

Recommended articles (6)

Cristiano Antonio de Souza is a PhD student in Computer Science at the Federal University of Santa Catarina (UFSC). He holds a degree in Computer Science from the State University of Western Paraná (2015). Master in Electrical Engineering and Computer Science from the State University of Western Paraná (2018). Participates in research groups: Research Group on Information Security, Networks and Systems (CNPq-UFSC); and Computational Security Research Group (CNPq-UNIOESTE). His research interests focus on network security, intrusion detection and artificial intelligence.

Carlos Becker Westphall is Full Professor (since 1993) at the Federal University of Santa Catarina - Brazil, where he acts as the leader of the Network and Management Laboratory and also coordinates some projects funded by the Brazilian National Research Council (CNPq). Obtained a degree in Electrical Engineering in 1985 and a M.Sc. degree in Computer Science in 1988, both at the Federal University of Rio Grande do Sul, Brazil. Obtained a D.Sc. degree in Computer Science (Network Management) at the University of Toulouse (Université Toulouse III - Paul Sabatier), France, in 1991. Editorial board member of periodicals and technical program and/or organizing committee member of conferences. He was the founder of LANOMS. He has contributed to Elsevier as editorial board member of the Computer Networks Journal; to Springer as board of editors and senior technical editor of the Journal of Network and Systems Management. He acted as a local group coordinator in the European MAX/ESPRIT II project which involved the Alcatel- TITN, British Telecom, HP, CSELT, SIRTI and NKT Companies. Best paper of CLEI 2011. Awarded International Academy, Research, and Industry Association Fellow (award plaque), in 2011. Paper at IEEE ComSoc Technology News, in 2012. Achievement award - tutorial at WorldComp 2013. Awarded - best paper of ICN 2013. IEEE Communications Society 20 years member (Certificate of Appreciation), in 2014.

Renato Bobsin Machado graduated in Computer Science from the State University of Western Paraná (1998), master's degree in Computer Science from the Federal University of Santa Catarina (2005) and a PhD in Sciences from the State University of Campinas (2013). He is currently a professor and researcher at the State University of Western Paraná, working in the Graduate Program in Electrical and Computer Engineering (PGEEC). Conducts research in the areas of computer security, intrusion detection, cryptographic methods, distributed systems and data communication. He coordinates the Laboratory for Research in Computational Security (LaPSeC) and participates in research groups: Research Group on Information Security, Networks and Systems (CNPq-UFSC); and Computational Security Research Group (CNPq-UNIOESTE).

Leandro Loffi is a PhD student in Computer Science at the Federal University of Santa Catarina (UFSC), Trindade campus. He received the B.Sc. degree in Computer Science from the Federal Institute Catarinense (IFC) Rio do Sul campus in 2017 and the M.Sc. degree in Computer Science from the Federal University of Santa Catarina (UFSC) Trindade campus in 2019, and also a postgraduate degree in Computer Forensics by IPOG - Florianópolis in 2020. He is currently student of the Post-Graduate Program in Computer Science at the PhD level, and an active researcher at the Network and Management Laboratory.

Carla Merkle Westphall is Associate Professor (since 2007) in the Department of Informatics and Statistics at the Federal University of Santa Catarina, Brazil. She acts as a security researcher of the Network and Management Laboratory. She is advisor of Ph.D. and Master students in the Graduate Program in Computer Science at Federal University of Santa Catarina. Carla received a Doctor degree in the subject of Information Security in 2000. She obtained a bachelor's degree in 1994 and a M.Sc. degree in 1996, both in Computer Science at the Federal University of Santa Catarina. She is a committee member of security conferences and journals. Her research interests include distributed systems security, computer networks, internet of things, identity management, blockchain and new generation networks.

Guilherme Arthur Geronimo graduated in 2006, Master in 2012 and Doctor in 2016 in Computer Science from the Federal University of Santa Catarina. He is currently a Federal Public Employee, in the position of IT Analyst, under the role of Datacenter Coordinator, located at the Superintendence of Electronic Governance and Information and Communication Technology (SeTIC) of the Federal University of Santa Catarina (UFSC) and in parallel researcher-collaborator in the Network and Management Laboratory (LRG), in the Informatics and Statistics Department (INE).

☆ This document is the results of the research project funded by the Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC) and by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES).

View full text