2022 International Conference on Artificial Intelligence in Everything (AIE) | 978-1-6654-7400-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/AIE57029.2022.00091

Artificial Intelligence for Edge Computing Security: A Survey

Francxa Tagne Waguie
Faculty of Science
Department of Information System Engineering,
Near East University
frank.waguie@yahoo.fr

Fadi Al-Turjman
Artificial Intelligence Engineering Dept., AI and Robotics Institute, Near East University, Nicosia, Mersin 10, Turkey
Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin 10, Turkey
Fadi.alturjman@neu.edu.tr

Abstract— **Edge computing is a prospective notion for expanding the potential of cloud computing. It is vital to maintaining a decent atmosphere free of all forms of security and breaches in order to continue utilizing computer services. The security concerns surrounding the edge computing environment has been impeded as a result of the security issues that surround the area. Many researchers have looked into edge computing security issues, however, not all have thoroughly studied the needs. Security requirements are the goals that specify the capabilities and operations that a process that is carried out by a system in order to eliminate various security flaws. The purpose of this study is to give a complete overview of the many different artificial intelligence technologies that are now being utilized for edge computing security with the intention of aiding research in the future in locating research potential. This article analyzed the most recent research and shed light on the following topics: state-of-the-art techniques used to combat security threats, technological trends used by the method, metrics utilize to assess the techniques' ability, and opportunities of research for future researchers in the area of artificial intelligence for edge computing security.**

Keywords— Artificial intelligence, Edge computing, Security, Literature Review.

I. INTRODUCTION

More and more physical things are being connected to the Internet of Things (IoT) via sensors as the deployment of sensors in the real world grows. Smart cities, smart homes, environmental perception, and wearable medical devices are all examples of fields where IoT technology is now large - scale distributed [1] [2]. In traditional IoT services, sensors and devices linked to IoT must upload data to cloud servers to conduct computational duties. The processed data will be send back to the IoT devices later the tasks are performed. Although sensors and devices' processing burden is reduced thanks to the cloud, the vast data transmission overhead is inconveniently large and must be taken into consideration. In 2018, there were 11.2 billion connected IoT devices throughout the world, and that figure is predicted to rise to 20 billion by 2020 [3], resulting in rapid expension in data. However, the current rate of increasing network capacity is substantially lower than the rate at which data growth is

978-1-6654-7400-9/22/$31.00 ©2022 IEEE
DOI 10.1109/AIE57029.2022.00091

occurring, and the complex nature of the communication network makes it difficult to cut down on latency. The bandwidth of the network has become an important obstacle that has to be overcome before ordinary IoT services can be implemented. In order to overcome the challenge described above, a fresh approach to computing known as edge computing (EC) has recently been created and is quickly gaining traction in the industry. The system that shifts computing tasks to the edge of a network is referred to as "EC," and its acronym stands for "edge computing" [4], [5]. EC provides numerous benefits over cloud computing, including safeguarding end-user privacy, minimizing latency during data transfer, reducing the load of network bandwidth, and lowering data center energy usage. Edge computing (EC) eliminates the need for IoT devices to submit their raw information to a central cloud service, instead allowing it to be processed, stored, and transported at the edge nodes (ENs), hence decreasing delay. IoT and mobile computing applications that demand rapid response times will benefit from EC's enhanced support. EC, on the other hand, is not a panacea. EC-backed IoT devices have seen significant improvements in several areas, including compute offloading, precise location, and real-time processing. This is due in part to the proximity of end-user data processing to the source of the low delay. EC, alternatively, introduces new security issues and widens the system's attack enviroment [6].

II. LITERATURE REVIEW

A. *Heterogeneous environment & Distributed layout*

Mobile data collection, sensor networks, grid computing, and wireless sensor networks all fall under the broad category. of technologies used in EC. Establishing uniform security rules and mechanisms across several security domains is difficult in such a heterogeneous environment.

Network edge devices (ENs) are challenging to integrate for centralized control [7], since they are spread out beyond the network's perimeter. The attacker can use the hijacked nodes as a launching pad to penetrate the whole system by focusing on ENs with known security flaws.

B. *Limited computing source*

Cloud computing and EN computing functionality are limited due to their physical structure. Consequently, Distributed denial-of service (DDoS) assaults can have a substantial impact on the ENs.; Since ENs do not support heavyweight security mechanisms.

Many security strategies and algorithms have been developed to compensate for the dangers posed by the edge computing characteristics [8]. Algorithms and models that follow the same design for intrusion detection, data confidentiality, or access control are used in the bulk of today's security systems. Traditional defence measures are frequently abandoned as assault approaches and methods are constantly upgraded. What is fascinating, though, is that Artificial intelligence (AI) is providing new solutions to privacy and security issues.

III. METHODOLOGY

To guarantee that the search and retrieval of data is accurate and objective, this review effort applies to a systematic review. Before commencing the literature and data extraction search process, A protocol for the review has been developed, which details the search strategy, the establishment of specific criteria for inclusion/exclusion in the choice of papers to be regarded or discarded, as well as a plan for evaluating the articles that have been chosen for review. Prior to deployment, one of the authors authorized the protocol. **Figure 1** depicts the processes involved in the approach of the review task.

A. *Search Strategy*

A comprehensive search was conducted across all works, both review and technical, that concentrate on the application of artificial intelligence to the topic of tackling security issues in edge computing. Web of Science, Scopus, IEEE-Explore, Wiley, Springer, and Science Direct were all used to carry out the search. This is because they include papers from prominent journals and conference proceedings, providing a representative sample of where things stand in terms of our understanding of artificial intelligence in the

context of edge computing security. Because the search will only look through the four online electronic databases that have been suggested, only a small portion of the literature that is pertinent to the planned review will be found.

To keep the scope of the review effort limited, the search was limited to only computer science and information, computer science and theory, and engineering topic areas. During the first search, we only considered papers presented at conferences or published in peer-reviewed journals between January 2015 and November 2019. The articles were found using the following search tip: {"Artificial intelligence" AND "Edge Computing" AND "Security" OR "Edge Computing" AND "Security" AND "Artificial Intelligence" OR "Security" AND "Edge Computing"}. The inclusion criteria comprised: Being a journal or conference paper with a higher level of significance achieved, to have been published between January 2015 to 2019, to have been written in the English language; and the exclusion criteria included: if the paper was not focusing on the application of artificial intelligence for edge computing security and if the paper was not fully accessible.

Scopus yielded 273 papers, Web of Science 271, IEEE-Explore 1328, Science Direct 354, Springer 371 articles, and Wiley 405. There were a total of 3,002 articles discovered. The title and abstract of the items that were searched were scanned. After the scan, 2,730 items were discovered to be outside

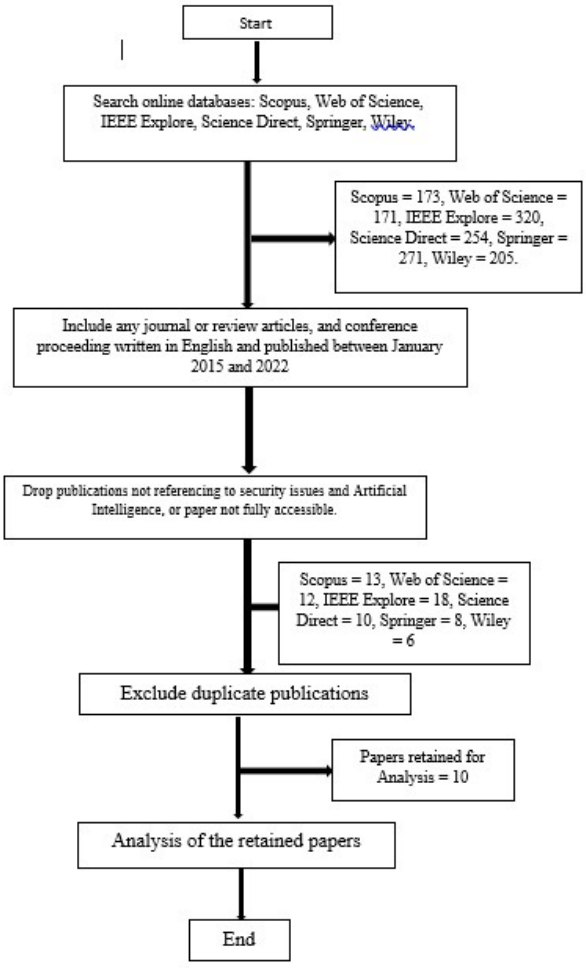

Figure 1: Architecture of the implemented review.

The figure presents the different steps involved in this review. The arrows represent the succession of steps and the square on the right represent the results from a previous step.

that met the inclusion criteria were thoroughly abstracted for relevant data that would address the study objectives. The following details were recorded: Authors,

IV. RESULTS

The review looked at 10 publications from four separate electronic databases from various journals and conference proceedings. **Figure 2** depicts the distribution of

publications among several journals covering a wide variety of subjects. The bulk of the papers came from the IEEE Xplore Magazine (70%) and the ACM Digital Library journal (20%), with Science Direct accounting for the remaining items (10 percent). In each article retained, we extracted the description of the study (study purpose and the aim of the study), the method used for attack detection, the method used for performance analysis, the advantage of the method, and its limitation (**Table 1**).

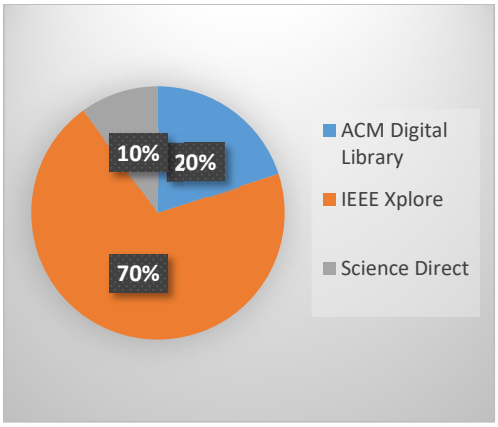

Figure 2: Distribution of article according to their respective journals.

V. Discussion

Although past review studies have provided a noteworthy basis for understanding edge computing security and privacy challenges, range between the evaluations were restricted in offering complete assessment of the security and privacy needs. Furthermore, the methods employed to make certain that the specifications were met using the technical means deployed were not adequately examined. This review used a methodical approach to provide a thorough knowledge of security and privacy in the edge computing system.

According to the findings, ten strategies for edge computing security were offered from the analyzed papers, all with the goal of attack detection. These techniques included SDN Architectural framework, MAB Architectural Framework, Game Theory Algorithm, Greedy Algorithm, Clustering Algorithm, Machine Learning, Novel Method (D2D Communication), Novel Method (Hybrid Feature Analysis), Novel Method (GPS), Novel Method (ANDROIDS). The performance indicators used to assess the approaches' efficacy were also investigated. It can be seen that the strategies used specified metrics to evaluate their effectiveness under each class of criteria, confirming the desired goal. Table 11 highlights the goal of evaluating the strategies using a specific criterion. This will aid future scholars in understanding why each measure is used in specific ways.

The research aimed to complete the review as quickly as feasible. However, various circumstances may influence the conclusion reached, reducing the results' quality. The following are a few contributing factors:

- The data collection procedure is skewed by the fact that Only one of the authors searched for the original research papers.
- As a result, just four electronic databases were examined for the purpose of gathering data. As a result, research from other databases that are relevant may be excluded. As a result, the breadth of the review job was constrained.
- Only works published in academic journals and those presented at conferences were taken into consideration, with patents, periodicals, and symposiums being omitted as sources of supplementary information.

VI. Open Research Issues

In the majority of the paper examined, Before the introduction of the methodologies, notably authentication and privacy-preserving measures, assaults had not been adequately researched or dealt with in any meaningful way. These assaults pose a serious threat to the confidentiality of the gadgets on the edge of interaction, as they may divulge sensitive information.

Intrusion Detection Systems (IDS) is used to identify and mitigate many types of network intrusions. When it comes to edge computing, on the other hand, the intrusion detection system must be implemented on every level of the edge network (Edge nodes, end-users, and cloud). If IDS is only applied to one or two levels, it is possible that this will not prevent malicious attacks from spreading throughout the whole edge network.

VII. CONCLUSION

The edge computing paradigm has great promise that aims to eliminate nearly all of the disadvantages of cloud computing. One of the major obstacles to its acceptance is the question of security. As a result, figuring out how to deal with the issues is critical. The results reveal that the developed comprehensive literature review in edge computing security and artificial intelligence is the first of its type. Its goal was to provide a complete and thoughtful grasp of current processes for top-of-the-line security, in addition to the cutting-edge technical approaches utilized by the ways. In light of this, a total of ten papers were extensively examined using normal Systematic Literature Review processes. The findings indicate important conclusions after a comprehensive review of the retrieved data. According to the findings of the study, there are eight different categories of criteria to consider regarding the privacy and security of edge computing. Second, the study revealed that each need has its own set of approaches built specifically for it, with the exception of integrity, nonrepudiation, and dependability, which were all evaluated together in four separate schemes. Finally, in order to determine the trend, the findings categorized the discovered procedures under their relevant technological ways. Fourth, the review effort has found limitations in each of the methodologies, resulting in research prospects for future scholars. Furthermore, it was discovered that each category of procedures under a certain need has distinct metrics for measuring their effectiveness in order to achieve a specified goal. Finally, future research open problems were mentioned for the advantage of academics interested in working on edge computing security using artificial intelligence.

VIII. ACKNOWLEDGMENT

We will like to aknowledge the Resaearch Center for AI and IoT, AI and Robotics Institute,Near East University and Door of Grace LLC .

IX. REFERENCES

[1] C. Livadas, R. Walsh, D. Lapsley, and W. T. Strayer, "Using machine learning techniques to identify botnet traffic," *Proc. - Conf. Local Comput. Networks, LCN*, pp. 967–974, 2006, doi: 10.1109/LCN.2006.322210.

[2] F. X. Ming, R. A. Ariyaluran Habeeb, F. H. B. Md Nasaruddin, and A. Bin Gani, "Real-time carbon dioxide monitoring based on IoT & cloud technologies," *ACM Int. Conf. Proceeding Ser.*, vol. Part F147956, pp. 517–521, 2019, doi: 10.1145/3316615.3316622.

[3] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," *Proc. IEEE*, 2019, doi: 10.1109/JPROC.2019.2918437.

[4] X. Xia, F. Chen, Q. He, J. C. Grundy, M. Abdelrazek, and H. Jin, "Cost-Effective App Data Distribution in Edge Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 31–44, Jan. 2021, doi: 10.1109/TPDS.2020.3010521.

[5] W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer (Long. Beach. Calif).*, vol. 49, no. 5, pp. 78–81, May 2016, doi: 10.1109/MC.2016.145.

[6] P. K. Manadhata and J. M. Wing, "A Formal Model for a System's Attack Surface," *HP Lab. Tech. Rep.*, no. 115, pp. 1–28, 2011, doi: 10.1007/978-1-4614-0977-9_1.

[7] P. Lai *et al.*, "Optimal Edge User Allocation in Edge Computing with Variable Sized Vector Bin Packing," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11236 LNCS, pp. 230–245, 2018, doi: 10.1007/978-3-030-03596-9_15.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.