Volume: 5, Issue: 3
Page: 52-60
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

Survey on Edge Computing Security

Baydaa Hassan Husain & Shavan Askar

Abstract:
It's possible to explain Edge computing (EC) as a distributed system of IT that decentralized the power of processing in which the mobile Internet of Things (IoT) computing would be allowed. In EC, data processed by local tools, computers, or servers, instead of being process and transmitted from the data center. However, with the wider capabilities of EC by increasing the network performance and reducing the latency, security challenges, and the risks will increase with data being stored and used on these devices on the edge or end of the network. This paper first provides a definition of EC and explain the reasons that led to the rapid spread of this type of computing with an explanation of the most important differences between EC and CC, in terms of the resources available for each type, processing, storage, as well as the privacy and security factor. Later, explaining the uses and benefits of this type of computing. However, the challenges are also taken into consideration, foremost among which is security. Through reviewing a number of previous researches, security challenges have been identified in four main sectors, including data privacy and security, access control, attack mitigation, and detection for anomalies Finally, choosing a set of solutions that were drawn from previous studies and contributed in reducing and limiting these challenges. Hopping this paper sheds light on Edge Computing security and paves the way for more future research.

IJSB
Literature review
Accepted 1 February 2021
Published 3 February 2021
DOI: 10.5281/zenodo.4496939

Keywords: *Edge Computing (EC), Internet of Things (IoT), Cloud Computing, Security, distributed system of IT.*

About Author (s)

Baydaa Hassan Husain, Information System Engineering, Erbil Polytechnic University, Erbil, Iraq. Email: baydaa.mei20@epu.edu.iq.
Shavan Askar (Corresponding Author), Assistant Professor, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.

1. Introduction

Edge computing (EC) is used every day in different tools, cellphones, iPad, robots, and smart cars used in automotive and manufacturing industries are included. EC also merges in healthcare IoT and medical monitoring devices. In EC, data collection and processing occurs at the end of the network where information is produced rather than in central cloud servers, greatly reducing the distance and eliminate latency. The fundamental thought of EC is to utilize a chain of command of end servers with developing computational resources to perform low-end IoT activities in mobile and large and diverse computing and portable devices, to be specific, edge devices (Yu et al., 2017). EC is likely to supply the location, bandwidth-sufficient, real-time, confidentiality, and the moderate forum to support increasing applications for smart cities. These areas of interest over CC led to the rapid development of this type of computing. Along with Statistic's latest analysis, the market measure of EC within the USA; recorded $85.3 million in 2018 is predicted to reach $1033 million in 2025. Agreeing to another later report, we note that in 2018, in all parts of the world, the estimated number of component that used is just above 11 billion and is expected to be twenty billion for 2025 (Xiao et al., 2019). Nonetheless, compared to CC, EC is more reasonable utilizing IoT tools, which are less costly by shifting the end micro-controller and resource capacity to the end platforms without paying for extra funds (Bajic et al., 2019). The delay in the handling of data is considerably lowered as EC develops storage and computing capabilities directly to users. Furthermore, any activities that do not definitely need the resources of the cloud server can be addressed directly to end nodes. Just from the other side, to mitigate the workload tension, they will execute the activities and data on the cloud server. However, EC can achieve the confidentiality and stability of the confidential system and user data protection by eliminating the possibility of sending user data to the central infrastructure, sending the authentication components on the endpoint. With these characteristics, EC has been steadily evolving in recent years. Although entities have a comprehensive solution in EC technology situations such as intelligent safety, commercial IoT, and smart connected automobiles, there are still some root issues that disrupt EC's rapid implementation and one of them is security. (Zeyu et al., 2020) To shed light on the existing challenges of EC security, this paper reviews a variety of posted paper on EC security. Fog computing was proposed to overcome the problems of cloud computing and complement it to provide QoS provisioning for real-time and video applications that require very low latency (Askar et al., 2011, Al Majeed et al., 2014).

2. EC (EC) Versus (CC)

This section is to equate cloud computing with edge computing. Inside a traditional cloud, the assurance of data protection has the priority, whereas, within Edge Computing, security controls and the privacy of the data can be depicted as powerless or far below clouding computing (Zeyu et al., 2020). The reason for that is, in the cloud computing environment, the end components are mainly fully-fledged computers that link primarily via wired internet to the cloud-residing platforms. But from the other corner, EC implements a centrally controlled structured layout which, as edge servers, can include poor or low-profile media-devices and these end devices are usually IoT and handheld devices that are resource-restricted compared to fully-qualified machines (Xiao et al., 2019). Cloud computing (CC), could be a mixture of centrally controlled, intended to convey, and concurrent system, EC, unlike CC, represents the centrally controlled computing benefit from packaging, processing, and implementation. It usually occurs on the network border which behaves as a central level in the central cloud for end-users and information centers. With this form, It eliminates the path that data on the network would emigrate, thus causing a minor delay. EC and CC advances are comparable in the strategies of putting away and handling data of the user.

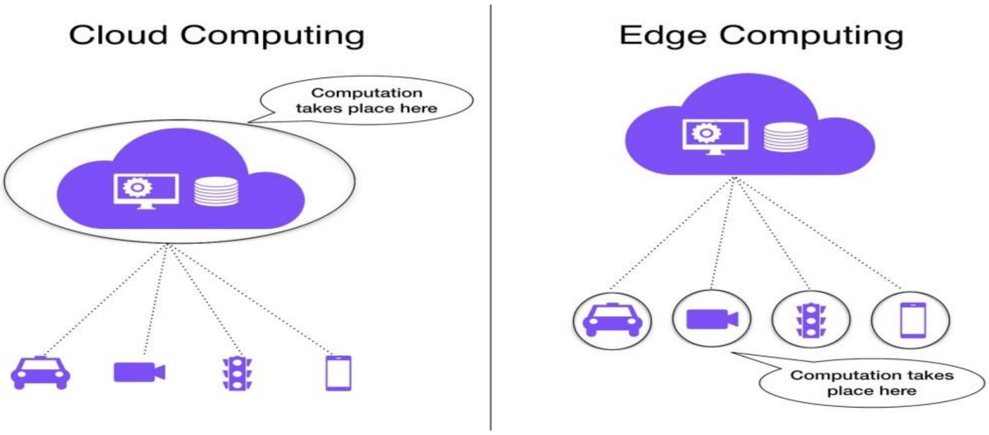

Figure 1: EDGE COMPUTING VERSUS CLOUD COMPUTING

Nonetheless, the contrasts between those infrastructures are based on the physical aspects of storage, analyzing, and processing. The rate of data analyzed, and the handling speed. Another essential difference between two computer systems is the availability of resources that can be described as restricted resources for EC. (Bajic et al., 2019). The differences between both computing systems are illustrated in Table1.

Table 1: Differences Between (EC) And (CC)

	Edge computing(EC)	Cloud computing(CC)
processing	Ideal for a small amount of data (Lin et al., 2017; Zeyu et al., 2020).	Suitable for handling large data storage(Bajic et al., 2019; Zeyu et al., 2020).
Storage	Storage of Micro Data (Bajic et al., 2019; Zeyu et al., 2020).	Storage of Big Data (Bajic et al., 2019; Shi & Dustdar, 2016).
Security and Privacy	Caused by the complex and heterogeneous network environment, it is hard to properly implement much classical security and privacy strategies for them (Zeyu et al., 2020; Zhang, Chen, Zhao, Cheng, & Hu, 2018).	Ensure that the data do not leak and enhancing the cloud servers' security capability to resist threats (Shi & Dustdar, 2016; Zeyu et al., 2020).
Environmental Awareness	Edge nodes bring together diverse IoT devices and wearable technology explicitly so that they have a higher awareness of the environment. (Xiao et al., 2019; Zeyu et al., 2020).	Less environmental awareness(Lin et al., 2017; Shi & Dustdar, 2016).
Resources	Limited resources(Bajic et al., 2019; Zeyu et al., 2020).	Huge central resources (Xiao et al., 2019; Zhang et al., 2018).

Despite all the above, there are plenty of challenges facing the Edge Computing establishment. Security takes up a large part of these challenges.

3. Security Consideration in Edge Computing (EC)

The distribution of data in vast networks that contain countless devices is a great challenge and could lead to problems. It is not easy to control networks of this kind, and it is difficult to protect released data in it, as each device is a source of weakness and danger to the entire network (Alwarafy et al., 2020). Going to consider that IoT is well known for its lack of security. However, EC devices usually are small in size compared to core devices and are often manufactured with a not high degree of protection, and these gaps may prompt hacker penetrations. Security in EC is foundational thought and incorporates secure communication from the data center to the endpoints on the edge; guarantee the security of information.

Security issues can be figured out in EC in four aspects, access control, attack mitigation, privacy protection, and anatomy recognition (Zeyu et al., 2020).

4. Security Challenges of EC

This part attempt to describe and illustrate the central challenges in Edge Computing, and briefly address their significant security consequences and impacts. Because of the particular properties of EC, For instance, the distributed architecture and, the huge amount of handled data, the conventional information security and privacy methods in CC are not appropriate for safeguarding enormous information security in EC. In addition, for a few resource-restricted conclusion tools, it is difficult to hold a vast volume or to insurance these devices' security. In outline, the information and surveillance security in EC basically confronted with new obstacles (Zhang et al., 2018).

4.1 Privacy and Security of Data

Because of the shortage of end nodes, privacy, and security of information is the biggest issue in EC (T. He, Ciftcioglu, Wang, & Chan, 2017). The computing edge presents privacy concerns. For example, the attacker may benefit a lot by catching details from and to smart-home models. By watching power or water utilization, the attacker may quickly predict in the event that the building is likely empty and hence to robbery. One of the barriers to achieving data security and privacy at the EC is a need for effective tools. (Shi & Dustdar, 2016). First of all, privacy and safety understanding among users. Take safety for Wi-Fi networks as an example. 49 percent of Wi-Fi platforms are unsecured in more than 400 million families that use wireless remote links, and 80 percent of homes also use default passwords. 89percent of the total access points are unsafe when setting up their switches for public Wi-Fi access points. If the user somehow doesn't maintain private confidential data, others can quickly hack tools such as webcams and health displays and snoop individual security information. (Shi, Cao, Zhang, Li, & Xu, 2016). The second privacy challenge is the missing of effective instruments to secure and safeguard the privacy of data and security at the end of the edge of the connection. A few of the elements are exceedingly resource obliged so the given strategies for ensuring protection may not be capable of conveying on the thing since they are starving resource. In addition, the extremely complicated setting at the end of the connection makes its structure become threatened or insecure. We can say most instruments for dealing with various data resources of EC are still incomplete (Mosenia & Jha, 2016). Take into accounts, EC may be a computing framework that gathers numerous trust domains such as trust centers, conventional data encryption, and sharing strategies with approved substances that are not suitable. Hence, it is particularly critical to plan an information encryption strategy for Distinct channels for authorization. The ambiguity of the algorithm should be perceived at the same instant(Cao et al., 2020).

4.2 Access Control

Due to the outsourcing of EC, any malicious clients without an approved character could misuse the gain assets in the edge or center foundation on the off chance that there are no effective verification components in that location(Zeyu et al., 2020). Neighboring edge devices communicate to get to or exchange their content with others. Nevertheless, in the event that hackers can get to one of the non-secured edge devices, it is conceivable to control the rest neighboring nodes (Wang, 2019). This, Establishes a significant safety problem for protected access, for example, the control system of the Virtualization resource of the cloud of edge servers is accessed, misused, and altered if they retain any such rights to edge machines (He et al., 2020).

4.3 Attack Mitigation

Contrasted with servers in the cloud, data centers on the edge are more sensitive to DDoS attempts. Since they are technically functionally least powerful than cloud servers, providing superior defense mechanisms. Furthermore, edge servers generally provide edge users with facilities that are considered to be error-prone in terms of security conditions As a consequence, minimal computation for their hardware, large and diverse frameworks. However, the attacker begins with compromising a different range of edge nodes and converting computers into weapons targeting the whole connection. The Mirai Cyberattack is an extreme case where, during the first 20 hours after its discharge, The attacker took full charge of about 65,000 IoT devices. At that point, these rebel IoT nodes were used to dispatch DDoS threats. focusing on high-efficiency edges, benefit suppliers such as Krebs, OVH, and Dyn (Wang, 2019). Due to the enormous number of digital edge nodes, the control area is quite narrowly restricted and this can increase the dangers of privacy attacks. For the future, the fast expansion in the range of networking equipment may raise the hazard of IoT DDoS hits (Guo et al., 2019). In spite of the fact that edge tools can confine most of the network-edge IoT data, and have the opportunity to detect and disrupt attempts during the first time in the nearest location to the source., there is a number of challenges in the practical field. The explanation is that neither edge devices, just like the elastic cloud, cannot gain the total network traffic required for the IoT-DDoS location, or measure the resources needed for tolerance (Bhardwaj et al., 2018). Furthermore, a client may have restricted details about a device's working condition, if it was shut down or hacked. Thus, indeed in the event that an attack tends to happen on an edge tool, the majority of clients would never be capable of observing it (Xiao et al., 2019). Another sort of attack represented by the attempt to introduce malware into a computer device appropriately and invisibly is known as the malware injecting case. This method of attack is considered high risk, as malware can pose a serious risk to system security and the uniqueness of data. A conventional firewall can hardly secure Edge nodes and low-level edge servers, rendering them more vulnerable to malware infusion attacks (Li et al., 2019). Between both computing frameworks is the availability of resources where resources for EC can be described as limited (Bajic et al., 2019).

4.4 Detection for Anomalies

Detection for anomalies can be defined as the method of recognizing unusual signals or perceptions inside a bigger information set and is an important assignment in numerous diverse areas from cybersecurity to the battlefield. The goal of anomaly location isn't only to identify anomalous perceptions accurately, but moreover to play down occurrences wrong positives by quickly changing place to the new developments in the information observed. Utilizing the conventional IoT model, the edge devices would send all assembled information to the servers where all preparation would happen and activity would be taken. This requires a steady tall transfer speed association to the central control servers and presents extra inactivity into the process(Schneible & Lu, 2017). In case an anomaly isn't dealt with appropriately its effect can be transmitted to all of the other edge nodes from one edge center, thereby decreasing the consistency of the complete EC structure. In expansion, once the implications of the anomaly have distributed, it is impossible to locate the real cause of its existence, leading to increased maintenance costs and delay in recuperation. (Zeyu et al., 2020).

5. Investigation of the Research Status of EC Security

In the latest years, scientific investigation on EC security could be collected in four types, counting: access control, privacy protection, attack mitigation, and anomaly detection. In spite of the fact that CC as of now has relatively developed arrangements in these areas, numerous of them are not appropriate for EC because of the precision of nodes on the edge, such as dispersed sending, restricted peripherals resources, complex organize the surroundings, etc. This encourages researchers to introduce more advanced arrangements for EC functions(Lin et al., 2017). Taking the computation to edge nodes increases the issue of preservation of the confidentiality of user records, undertake, and location. Information of clients can easily seep, mistreated, or damaged, which may deter people from using EC networks (Zhang et al., 2018). Privacy protection can still be either by Identity and Data Privacy or location privacy. A number of researchers strongly recommend a privacy mechanism with machine-learning for the extraction and collection of data which compose of three phases, system-level performance. The middle layer represents the middleware layer at the host step of the system design. The network level layer is the last one, safeguarding the gathering of data on the arranged layer (Ma et al., 2020). A number of machine learning EC arrangements have been recommended to conserve the protection of the user 's location and information, transfer processing to the edge unit. Transmission of details to the edge node or database server is now not requisite, and thus confidential user information persists preserved in edge nodes (Alwarafy et al., 2020). A great location protection method may be found in an approach that represents a framework for versatile online social outlets, which gives an adjustable utilization in the privacy information sector. The system can distinguish unreliable to certain level, social partnerships. It masks location data by isolating identity information and private position storage data and after that putting away those in two separate entities. In case that one load leaked or targeted entities, information around the location will be safe since it will not uncover user identities (Yang et al., 2020). Based on the perception that EC may experience an assortment of network attacks, many of them inquire about improvements that are referred to as IoT Cyberattacks. Full usage edge nodes are shaped to master the challenge of IoT DDoS attacks; Ketan Bhardwaj et al.(Bhardwaj et al., 2018). Stated a DDoS relief model, the structure totals the flow exportation of numerous edge nodes in three phases to distinguish DDoS hits. Even though the model can distinguish DDoS hits way quicker in a hypothesis, if a node on the edge catches well as small traffic, DDoS attacks with remarkably dispersed attack sources would be hard to find. Qiao Yan (Ioulianou & Vassilakis, 2019) stated a multi-layer DDoS relief system, including the EC layer, fog computing(FC) layer, and the CC layer. The first two layers are connected to the collection of documentation from the network. The servers in the cloud are taking responsibility for gathering awareness regarding network operation and finding of DDoS hits. The outcomes of the analysis will be converted back to the fog layer. The role for coordinating the attack event is on the Fog servers. The system requires guidelines of snort to identify DDoS hits and employs switches SDN-driven to reduce threats (Zeyu et al., 2020; Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015; Sulaiman & Askar, 2015; Fares & Askar, 2016). In order to find and synchronize edge node abnormalities in a period with many different edge configurations, experiments were conducted out by the scientific community on either side, and new protocols have been made using the machine learning approaches. The EC anomaly location illustrates the shift of edge cloud coordination from current research achievements. As edge nodes investigate slight anomalies, cloud servers can undertake a machine learning algorithms and interpret the location of the node on the edge more properly. Not only implementing the edge nodes' anomaly location, but also fully realize the anomaly expectation for edge nodes. Furthermore, the anti-attack study on the identification mechanism of anomalies is also being increasing (Samir & Pahl, 2019). Believed that the study accomplishments of the edge anomaly discovery focused on intellectual ability on the end nodes will be widened almost in the years ahead. Finally, consequently, the research conclusions of EC access control are primarily partitioned into two types, which are the mechanisms under the ICN network design and the mechanisms under the design of the non-ICN network (Zeyu et al., 2020).

5.1 Mechanisms under the ICN network design

Scientific research on the access control model centered mostly on encryption of communication content isn't much. Satyajayant Misra submitted a report on how to get to a framework of a control system based on encryption of material. In spite of the fact that it may be used to guarantee that only authentic clients can encode relevant content, and a central identity certificate authority, which is always available, does not need it. It can indeed solve the issue of benefit revocation very well. In either event, the drawbacks of this form of research can still not be avoided by this scheme: malicious parties can still retrieve information that cannot be decoded. It wastes strictly limited network capabilities (Misra et al., 2017).

5.2 Mechanisms under the design of the non-ICN network

The Blockchain technology's influence makes analysts attempt to implement it to EC. Guo et al. (2019) Presented a blockchain arrange established on end nodes for the provision of vehicle access control. They divide the blockchain organized to increase the pace of character verification into a three-tier system. However, in the event that Blockchain technology is to be used more frequently, in EC, it still ought to illuminate the inadequacies of the convoluted nature of infrastructure, the steep cost of computation, moderate verification speed (Zeyu et al., 2020).

6. CONCLUSION

The previous years witnessed a development Within the sector of Edge Computing (EC) research. As a matter of fact, for the rising use of such devices in various aspects of life is a result of the significance of protecting these devices, scientists have taken this aspect seriously into account. After considering the percentage of research in this field, experts recognize, on one hand, the value of these devices and, on the other hand, the nature of the challenges and complications that are linked to such devices. Much research has focused on the challenges side and how to provide satisfactory solutions to them, particularly mentioning the challenges of security and privacy. Nevertheless, there are still gaps and challenges related to secure these devices and the need for a fair amount of future work in these areas. After looking through a number of scientific researches, first, this paper presents the background information on EC. Secondly, the paper determined the security challenges of EC from four perspectives. Thirdly, the paper details the latest primary research accomplishments of EC security into four categories; At last, this paper reviews some suggested solutions in these four areas in academics. Finally, form the basis for future research, by focusing attention on the importance of security in edge computing.

References

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge computing-assisted internet of things. IEEE Internet of Things Journal.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 16th European Conference on Networks and Optical Communications, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Bajic, B., Cosic, I., Katalinic, B., Moraca, S., Lazarevic, M., & Rikalovic, A. (2019). EDGE COMPUTING VS. CLOUD COMPUTING: CHALLENGES AND OPPORTUNITIES IN INDUSTRY 4.0. Annals of DAAAM & Proceedings, 30.

Bhardwaj, K., Miranda, J. C., & Gavrilovska, A. (2018). Towards iot-ddos prevention using edge computing. Paper presented at the {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18).

Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An Overview on Edge Computing Research. IEEE access, 8, 85714-85728.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters. International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Guo, S., Hu, X., Zhou, Z., Wang, X., Qi, F., & Gao, L. (2019). Trust access authentication in vehicular network based on blockchain. China Communications, 16(6), 18-30.

He, H., Zheng, L.-h., Li, P., Deng, L., Huang, L., & Chen, X. (2020). An efficient attribute-based hierarchical data access control scheme in cloud computing. Human-centric Computing and Information Sciences, 10(1), 1-19.

He, T., Ciftcioglu, E. N., Wang, S., & Chan, K. S. (2017). Location privacy in mobile edge clouds: A chaff-based approach. IEEE Journal on Selected Areas in Communications, 35(11), 2625-2636.

Ioulianou, P. P., & Vassilakis, V. G. (2019). Denial-of-Service Attacks and Countermeasures in the RPL-Based Internet of Things. In Computer Security (pp. 374-390): Springer.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. 6th International Conference on Intelligent Systems, Modelling and Simulation, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Li, Q., Meng, S., Zhang, S., Hou, J., & Qi, L. (2019). Complex attack linkage decision-making in edge computing networks. IEEE access, 7, 12058-12072.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

Ma, Z., Ma, J., Miao, Y., Liu, X., Choo, K.-K. R., Yang, R., & Wang, X. (2020). Lightweight privacy-preserving medical diagnosis in edge computing. IEEE Transactions on Services Computing.

Misra, S., Tourani, R., Natividad, F., Mick, T., Majd, N. E., & Huang, H. (2017). AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge. IEEE Transactions on Dependable and Secure Computing, 16(1), 5-17.

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602.

Samir, A., & Pahl, C. (2019). Detecting and predicting anomalies for edge cluster environments using hidden markov models. Paper presented at the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC).

Schneible, J., & Lu, A. (2017). Anomaly detection on the edge. Paper presented at the MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM).

Shi, W., & Dustdar, S. (2016). The promise of edge computing. Computer, 49(5), 78-81.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

Wang, S. (2019). Edge Computing: Applications, State-of-the-Art and Challenges. Advances in Networks, 7(1), 8-15.

Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. Proceedings of the IEEE, 107(8), 1608-1631.

Yang, G., Luo, S., Xin, Y., Zhu, H., Wang, J., Li, M., & Wang, Y. (2020). A Search Efficient Privacy-Preserving Location-Sharing Scheme in Mobile Online Social Networks. Applied Sciences, 10(23), 8402.

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2017). A survey on the edge computing for the Internet of Things. IEEE access, 6, 6900-6919.

Zeyu, H., Geming, X., Zhaohang, W., & Sen, Y. (2020). Survey on Edge Computing Security. Paper presented at the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE).

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE access, 6, 18209-18237.

Cite this article:

Baydaa Hassan Husain & Shavan Askar (2021). Survey on Edge Computing Security. *International Journal of Science and Business, 5*(3), 52-60. doi: https://doi.org/10.5281/zenodo.4496939

Retrieved from http://ijsab.com/wp-content/uploads/685.pdf

Published by

IJSAB
International