EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Cloud, Edge, and Fog Computing and Security for the Internet of Things

Mohammed Al-Alshaqi*, and Danda B. Rawat

Data Science and Cybersecurity Center (DSC2), Department of Electrical Engineering & Computer Science, Howard University, DC, 20059, USA

Abstract

In this paper, a method is purposed that detects the masquerade activity of cloud data. In this method, the combination of the decoy technique and the user's behaviour profile technique are used to improve the security of data in the cloud. This research has the main focus on understanding the use of these computing paradigms with the internet of things. The security concerns and its possible solutions are described. Therefore, the comparative analysis is conducted, which elaborates on each paradigm in the internet of things. The future consent of cloud, edge, and fog computing is also directed, which gives the innovative vision for the data handling with the internet of things.

Keywords: Security for the internet of things (IoT), Cloud Computing, Edge computing, Fog computing with the internet of things (IoT).

Received on 01 August 2020, accepted on 05 October 2020, published on 20 October 2020

doi: 10.4108/eai.20-10-2020.166666

*Corresponding author. Email: mohammed.alalshaqi@bison.howard.edu

1. Introduction

The computing scenario is converting from Cloud computing towards the fog and edge computing. The computing technology is emerging with the internet of things in these days. This technology not only helps to improve the existing application but also used to innovate the new applications. The internet of things is prominent in the data communication system and various devices, which are leading to increasing the amount of data generation. Due to which the cloud attitude uses to store, process, retrieve the data. There is a beneficial process of data processing and storage provided by cloud computing, which provides the entire data -center instead of having a private data center for the clients for batch processing, web applications, and other information processes. It is the primary reason we consider that Cloud computing is more efficient, which helps to reduce the cost of organizations for the storage data for sharing data. This technology minimizes the extra burden of specification and excessive processing of data for the organization. The devices which can connect with the cloud need to interact with the new network and primary requirement of network connectivity. The working principle of a computing network is the same; however, before sharing the data, the network ensures the connectivity of entire devices. It also ensures that every hop is connected. The network can share the information at one hop and share the information towards the multiple hops. The sensors send the data towards the central storage system and computing equipment known as the cloud. The task of collecting the information is more complicated than the execution; the process of execution is explained below (Devkar, et al. 2016).

The first step explains how latency occurs when the customer is far from the cloud. In the communication system, the cloud server reduces the operating cost of computing by providing the data center at various places with minimal resources to which the transition delay of data increases. In the Internet of things, the devices take 1 second to generate the information by the temperature sensor, and this information takes a millisecond to store information in the cloud. The transmission delay is not the only one that can affect the data. These days the Internet of things is exponentially growing and calculating the other delays, which requires extra time to process the information in large quantities.

Cloud computing also can handle the data efficiently. In a complex networking system, the internet of things takes information as a burden because the sensors create this information, which the cloud gets confused about. This burden causes more transition delay in storing the data. The micro and macro organization believe in the cloud service for protecting and storing the data. The cloud is helping to reduce transition delay, and sports mobility of data. However, the cloud is not fulfilling the need for quality of service, which the architecture of IoT needs to improve. This architecture required an efficient response to reduce the extra burden on the cloud.

Fog computing supports the different computing services, for instance, the storing, and communication which it brings to the end-users. The computing technique not only extends the cloud towards the network's edge but also defines the decoy generator, which protects the original data. This technology provides services such as a distributor decoy for monitoring decoys. This service protects sensitive and real data by providing Fog misinformation. Decoys information, for instance, decoy documentaries, honey pots, and honey files are generated when Intruder is detected. Decoy files is the technique used to limit the damage caused by stolen data due to the minimum value of stolen data or information. There is another decoy, which is known as believer decay. This decay creates an illusion for the attackers where they cannot figure out the reality of data. Edge computing also implements in buildings, homes, and transportation systems. The significant advantage of computing technology is the reliability, including the low latency, processing of device, and offload of data with the high bandwidth (Anthony, Toby, and Robert 2010).

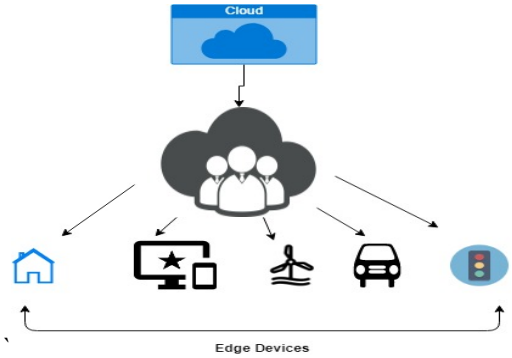

Figure 1. Cloud, Fog, and Edge Computing with IoT

The Internet of things is the collection of embedded sensors, actuators, and software, which we use in communication devices for the security transition of data. These intelligent sensors process data and exchange information that sensors generate. The wireless sensors are IoT devices that generate the experiential amount of big data. These sensors provide the information in real-time, and you can extract the data in the form of a batch. The primary difference between real-time data and batch data is the frequency. The big data has an informative form of data, which includes the high velocity, different variety of information assets, and high volume used to process in the decision-making.

The Internet of things is proliferating in which the critical concept is that a unique variety of equipment can process and work directly and indirectly with the help of program and software (Ali et al. 2016).

We use this technology in every aspect of life, including industrial plants, cars, and home devices. Furthermore, we also use it in the resource management and health department in an innovative way. The most important thing is that we use this technology for the inventory management system of the company in the form of radio frequency identification. Regarding the security, the Internet of things depends on the several layers of abstraction in the computation, sensors, and communication. The semantic layer of IoT devices interprets the data and processes it effectively. According to research, many security attacks occur at the software instead of hardware because it is the prominent section covering many devices and information—the other attacks during the processing of data and decision-making steps (A. A. Laghari, et al. 2019).

The large quantity of devices works in the positive mod without batteries. The energy of these devices requires a minimal amount of hardware since they offer an Ultra-compact security solution. Mostly, IoT devices operate in the unprotected mode. The primary aim of this paper is to provide a security requirement for the Internet of things.

To provide security to the hardware of IoT, a lot of engineering and creative ways will address the fundamental issues. Hardware-based security provides the natural starting point to the IoT protocols (Devkar, et al. 2016).

The primary milestone of this paper is to explore the cloud, edge, and fog computing and make the cloud data safe and secure.

2. Background

There are a plethora of results showing that fog computing is a better option in comparison with cloud computing. The literature review reveals the latest research work regarding fog, edge, and cloud computing, including privacy for the Internet of things. Cloud technology is feasible and flexible for the home controlling system because we can implement a low-cost system via the clouds (Dhiah, Simon, and Ala' 2019). The author purposes that if you use the cloud services in the smart automation system, then transferring data will be secure and save storage. The Internet of things is the fundamental technology in ipv6 smart low-power personal area networking. This technology helps a plethora of domains, including PHP, jQuery, etc. The extraction of the ECG signal is also possible with the help of cloud technology. The heart rates of humans and low latency calculations are achieved in the paper. We use the IoT to implement a remote health monitoring system to monitor every step of the healthcare system. They also make the health care system in IoT, which collects the data in real-time. This method provides privacy and security to the patient's data (Digiteum 2019).

The industrial readings can manipulate the data for the storage for centralized data and use raspberry Pi, Optical recognition, image processing, and the online data manipulating. The author also proposed the fog computing base face identification and resolution framework used to improve the processing capacity to save the bandwidth and observes the protection and privacy issues. A privacy security scheme is for the data encryption and integrity finder to resolve the confidentiality, availability issue, and integrity in the data processing (Farjana, et al. 2020).

The cloud environment requires the certification authority, which involved the physical infrastructure, end-users, and device network. These documents will give green to that PKI certification responsible for security. The virtual and physical entities are essential for the cloud to build security domains in the clouding environment. Currently, the cloud is getting prominent and easy to use. It this platform, every service needs protective authentication and authorization process. The user also wants to keep the application in the virtual account.

Furthermore, without the authenticity process, the user maintains many passwords but uses a single effective authentication method. There are two kinds of ITU, the first is the real thing, and the second is the virtual thing. The sensible thing exists in the physical world and has the capacity for sensing and actuating. It is also responsible for the surrounding environment, goods, and electrical equipment. The virtual thing can store, process the information, and get the facility of the multimedia content and its applications. Both have a unique quality, which connects with the cloud, fog, and edge computing. This process provides the secure working domain for the processing of data (Anthony, Toby, and Robert 2010).

Although we are accustomed to relying on the cloud for IoT application handling, the exponential development of IoT gadgets keeps creating enormous measures of information, which implies we cannot rely on any focal substance, for example, the distributed computing worldview to process these colossal measures of information. The fog registering worldview is advancing to serve different administrations while at the same time dealing with various sensors, actuators, clients, procedures, and network by putting preparing offices closer to clients. Likewise, the edge gadgets produce information from their assigned regions and connection with one another or transmit to the neighboring Fog hubs for strengthening investigation and choices. The Fog processing worldview can explain the time-delicate application preparing constraints of the cloud as supporting IoT applications [1]. Mist gadgets dwell at the system edge to encourage registering benefits close to the clients and convey benefits as applications for billions of associated gadgets (Medha and Krishna 2019). This serves to bolster ongoing handling, stockpiling, and systems administration offices at the edge level Fog computing information created by IoT or edge gadgets by expanding individually with the quantity of IoT gadgets. Because of the absence of sufficient assets for IoT gadgets, it is difficult to process all the information on IoT gadgets. IoT gadgets send the produced information to the close by Fog hub. From that point forward, this hub isolates the produced information into a few portions and advances them to different Fog hubs for additional preparation. During this division and dispersion time, the information could be adjusted or controlled by assailants. Consequently, the trustworthiness of the information must be guaranteed. Subsequently, the encryption and decoding process is difficult to actualize due to related asset requirements. Currently, weight encryption and unscrambling systems would be a perfect arrangement. Be that as it may, client information is re-appropriated to the client's information control, which is given to the Fog hub. This is still a security danger related to cloud registering. Security guidelines structure a fundamental part of keeping up insurance for data frameworks. These principles can characterize extension and security capacities to deal with data and human resources.

Principles help to assess the viability of safety efforts and keep up the criteria for continuous evaluations of security. It is required to think about appropriate security models, and generally utilized security rehearses in the Fog figuring condition to build an attainable decision for the endeavor network. To moderate these dangers, a proposed arrangement is to present auditable information stockpiling administrations, which are pertinent for distributed computing information insurance. Regarding a cloud capacity framework, a notable procedure is homomorphic encryption. You could use this to guarantee trustworthiness, privacy, and unquestionable status to allow a customer to research the information which is put away on untrusted servers. The current research business is related to evaluating information stockpiling benefits with distributed computing. Inevitably, from the conditions above, there is still no proposed technique that can meet the criteria dependent on three-level engineering for Mist figuring. In any case, it is a moving assignment to plan a safe stockpiling framework, which will fulfill all prerequisites (dynamic preparing, low-idleness, high-versatility, and so on) and bolster smooth correspondence between the Fog and cloud conditions. To identify system and information assaults info, we need to utilize an Intrusion Detection System (IDS) over different layers.

In the past years, internet devices have grown, and this technology created the name of the Internet of things. The basic concept of this technology is to combine multiple devices, which can work in a hybrid form. These devices enhance ability and efficiency. The basic concept of this technology is to bring different devices to gather protectively, and these devices should connect with the internet (Laghari, He and Shafiq, et al. 2017).

The problem by connecting the devices and the storage of data is the data is available in terabyte size. According to tradition, this data goes towards the organization for the next processing, resulting in taking a long time to show the data. The shifting takes time to expose the sensitive organizational data and convert into the network's vulnerabilities.

3. Cloud computing

Cloud computing has altered the working environment from traditional to virtual. The clouding phenomena attracts many due to their unique services with a minimum capital cost. Cloud computing also has critical factors in which users do not move toward, which includes security challenges. Cloud computing is updating itself, increasing security, and exploring the different techniques that can cover the large domain of data. The Internet of things is an innovation in the field of cloud computing (Medha and Krishna 2019). In cloud computing, challenges remain of a network system from a traditional method to the cloud environment. The primary applications of the cloud are the software, platform, and infrastructure as services. These services perform different applications in different fields such as games tasks CRM; the second is in the development of App. The last is the IaaS in the infrastructure for the server storage network and the security challenges with IoT devices. We categorize the cloud service in different types, which include the private cloud, community, public, and hybrid cloud. These clouds perform a specific role in the clouding infrastructure that includes the concerns of privacy used by a single institution such as the private cloud (NARENDRA 2020). We use the public cloud for services of emails and by multiple users. The community clouding is where the excess of clouding needs to share with multiple hosts, and limited members work within that cloud. In the hybrid cloud, there are many benefits because it works in the infrastructure of the clouding on both private and public loading, and the temporary computational process proceeds with the work ahead. There are multiple servers of clouding, which include the data center, distributed server, and server of client computers. The working of this computing service with internet devices such as IoT makes the technology extraordinary (NARENDRA 2020). The primary reason for clouding support towards the IoT device is because these devices get live information, and this information is important to store to analyze the data effectively. The cloud service helps the IoT device in storing a large amount of data efficiently and protectively. These devices bring revolutions in different fields such as medical and electrical, which includes the smart grid system, etc. The cloud layer also provides the data processing and services of analysis. Different steps can perform, which include the encryption of data by users, defining the keys, and the user identification code. This data is processed, and the results move towards the fog layer, which connects with the raw data of users (Narayana et al. 2015). There are multiple challenges externally and internally, which include the cyber-attack at the data placed in the clouding infrastructure, insider attaches, lack of support, lack of standardization, data integrity, lack of transparency, and Insure APIs. While dealing with threats, the cloud infrastructure includes the middle man threats, denial service attacks, networking sniffing, port scanning, SQL injection attacks, etc. These threats are handled by developers that make the environment robust and efficient (Prachi, Kulkarni, and Kute 2016). There are some internal attacks on the clouding, which include the denial of service attack and the users who illegitimately forward the messages to the clouding network for the request of authentication. There is another attack that can affect the Internet of things, and the clouding environment, which is the injection of malware. Interception communication intercepts the connection among the users, which creates the problem between the communication. There are many solutions to secure these networking systems, the first is monitoring the network, and the second is the firewall's implementation, and last is the network segments (Prachi, Kulkarni and Kute 2016).

4. Edge Computing

Edge computing works by storing and manipulating critical data on the data center's network, which are called edge. This is the processing of data completed before sending the data to the data center for the combination of memory and computing power. The essential purpose of these computing services is to work in the IoT environment because it collects the data there. At the local stage, this data is collected and then moves toward the cloud for the storage and next process. The Internet of things uses edge computing with its devices, networks, and computing abilities (Hina et al. 2020). It is also known as the mini data center device, which carries out the edge network. The term edge computing is short but creates a significant impact because it processes the data instantly instead of transporting it to a center. This activity enhanced the speed of providing real-time analysis, which is the requirement of many enterprises (Robert, 2019). We define edge computing as the distributed IT architecture, which makes the processing possible at the border, so it brings the originating source. With the help of edge computing, the microdata center of the IoT devices carries out the edge processes in real-time, with the speed of the entire process increased [1]. The manipulation of data provides the ease of decision-making. Regarding security, edge computing is secure because it stores the data in the cloud pattern, which provides effective security. The primary benefit of edge computing is to cut down the cost of storing and manipulating the data (Robert 2019, Safavat 2020). The organization does not need hardware devices to maintain the record of data. Furthermore, it permits enterprises to filter useful data. This technique not only filters but also minimizes the time by milliseconds.

5. Fog computing

The fog computing also helps store the data, including the files, documents, and provides the facility to control the service remotely. We can assess this service from any node after the connectivity with the internet. The vexing issue is the primary concern for the end-user because the data needs to secure, so the ownership of data is given to the user via a unique user name and password. The confidential information of data limit up to the directory, but the information is at risk (Yang 2019). The hybrid approach of decoys protects the data from intruders. Decoys information, including the decoy documents, honeypots, and random data, can be created on-demand. The server prevents the unauthorized person. Decoys data remains secure, but it confounds when the information is missing. Regarding the security, this technology can combine the different prominent technologies at one platform to protect the data of users in the cloud. The technology provides the facility to return the data if it identifies abnormal access by the cloud service (Yang 2019). This technology is prominent regarding the protection of data processing and use by large and small enterprises.

They download the traps in the file systems from the fog computing site, and electric service provides several kinds of decoys documents such as the return forms, credit cards, and medical records. There are many benefits to the decoys, including the file system. The first is the masquerade activity detection. Secondly, it confuses the intruders by creating the trace between the real and bogus information, and the effect of deterrence plays a crucial role in preventing the masquerade activities by risk averse. In this paper, we combined the two techniques to secure the information. We compiled the comparative analysis of existing research in this paper to minimize the risk of data security (Laghari, He and Khan 2018).

6. Issues with IoT.

In reality, the 5G network cannot meet the performance goals regarding the minimum tendency without using edge computing because it takes time for traveling. The data must travel from the fiber network connecting with the core and radios. The primary benefit provides the content close to the radio of the edge network. It minimizes the latency. Fog computing provides better between distributed computing and the Internet of things with ongoing communications. It conveys quicker, registering functionalities sitting near client applications and has neighborhood stockpiling choices. Despite these possibilities in hazing, keeping up the secure information correspondence is a difficult issue and needs a further turn of events. Currently, we have introduced an Identity-Based Encryption (IBE) conspire that guarantees secure information transmission to approved clients. To give information security, we proposed a four-level Hierarchical Identity-Based Architecture for Fog Computing (HIBAF). Furthermore, we assessed our plan to dissect the presentation as far as client load, memory use, reaction time, and postpone time over various sizes of datasets. Lastly, we contrasted our outcomes and other cryptography frameworks to make sense of the viability of our plan and discovered it 30% effective.

The software implementation of the network is an excellent technique that helps to move the 5G networking system securely. This system enhanced the protection of the data effectively. This technique needs the purchasing of the local router to transfer the information from one domain to another. The important thing is that the end node will decide the quality of the services which require specific information and route the node in an innovative way (WINSYSTEMS 2017). This information can increase by changing the high-performance laptops or personal computers, which can help to minimize the latency. The mobile edge computing uses fog computing and gives the space to the data for storage. We can use

these techniques in IoT devices and implement them in every domain of the world. For instance, the IoT technology in working in the IT department, engineering department including electrical, mechanical, and chemical. The hybrid working of these devices increases the efficiency of the machines and workers because they provide exact output (Wagan and Umrani 2020).

The administration's hierarchy within the service providers of the cloud gave an example of attacks from original threats cases. In this paper, they discussed how the cloud environment allows the hacker to breach the security system. They presented additional clouding system risk, which can affect the data and its processing. They also mentioned the challenges faced by the customers and service providers. Many purposes secure the information remotely using the latest techniques of cloud computing. They based these designs on encryption and unique access controls. The standard solutions for securing the data have been failing with the variation in time (Xu, Wendt, and Potkonjak 2014). The entire data destroyed after the incidents, and the other problems can affect the data, including the buggy codes and the wrong implementation of the algorithms. After applying these algorithms, incidents still happened and provided the results in the form of disasters.

7. Comparative analysis regarding the security of the Cloud, Fog, Edge with IoT

There is a plethora of researches, which is evidence of computing methods to enhance the productivity of data with IoT. The remote monitoring needs effective technology for collecting the data in real-time; for instance, we use drones to analyze the review and respond to the information in real-time. In the existing research, they provided the identity-based encryption scheme, which ensures the data transmission to the authorized users. In this paper, we provide four-levels of the hierarchy to ensure secure data transmission based on the architecture of Fog computing (HIBAF). Additionally, we evaluated the scheme to analyze the performance of the user's load, memory utilization, including time response (Mhidi, Nabil and Adnane 2019).

The Internet of things provides an ease to every industry by giving innovations. The vehicular cloud computing increases the efficiency of the vehicle and supports the vehicle's computing and storing system. This technology not only reduces energy consumption but also works on low traffic vehicles. The critical facility of VCC is to provide the virtual platform for processing information using the centralized server's data. To ensure a proactive platform, we use new decoy technology and user behavior profiling. The behavior profiling presents the alternative solution to overcome the security and the privacy in the servers of cloud using the fog architecture (Xu, Wendt and Potkonjak 2014). AI and virtual assistants such as google assistance provide an integrated solution.

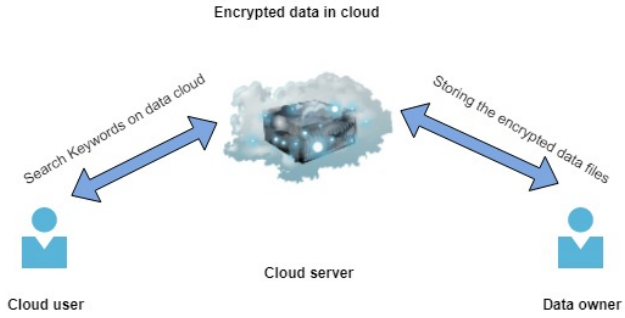

Figure 2. Encrypted data system of cloud

The methodology is purposed to protect the information in the could using hostile distraction innovation. We observed data of access through the clouding and found the information access design. This technique confirms that data access is authorized or not. The section method confuses the attackers with the help of false information, which is known as the decoy technology. Cloud computing is revisionary for smart devices. The business sectors are getting benefits from this technology. In recent studies, they used different methods to provide the security of the cloud, but the prominent method was decoy technology (Yang 2019). This technology is useful and prevents hackers from the extraction of data by providing wrong information. The second is user behavior profiling, which helps the user by giving proper identification.

In comparison, cloud computing has a high tendency concerning fog and edge computing. The location of service for cloud computing is the internet, and this service is the edge of the local network. The mobility of cloud computing is minimal, but the mobility for fog and edge computing is highly supportive (Nazir, et al. 2020). The type of connectivity for cloud computing is the leased line, whereas the fog and edge computing connectivity types are wireless. There is also a significant difference between these computing techniques; the cloud is providing the facility of many, whereas the edge computing has the distance between server and client is only for one.

8. Purpose method

The method is the combination of the decoy technology and behavior profile technology because, with the help of decoy technology, it generates a trap to which nobody can reach the original data. There are many advantages to this method, including data storage and internal attach detection. The original information cannot be detected by

hackers, and we can find the attack easily. The advantage of the decoy system is to detect the activity of masquerade and misleading attackers.

The profiling of user behavior technique and decoy technology both have unique methods in the cloud database. The combination of both provides a sustainable and reliable method for masquerade detection. The legal user does not know the file system and its location where these files are stored; whenever any masquerader tries to reach the user system illegally, they are unlikely to be familiar with data and file structure (Laghari, He and Karim, et al. 2017). The fake search of users will be untargeted, or we can say that the search for masquerade will not be the point. The user behavior profiling critically observes the database of the cloud and checks how much users access the information from the database. It also detects the exact timing and abnormal access to any intruder. This technique identifies if any divergence is in the database. This method can detect any illegal activity. The combination of both techniques will create confusion for the attacker. The combination of decoy technology and user behavior profiling will show evidence of illegal activity. It is also effective to improve the detection accuracy.

9. Research challenges and perspectives

It is well-known that sometimes IoT devices have a problem with the weak connective, and we can resolve this problem by using the edge clouding. It stops the data from transmitting towards the center, and the connection of the local network is enough for the manipulation of data. It also provides the surety about the processing of data. The latency is the second issue at the networking side during the transmission of data. A delay is created at the sending and receiving side, and this problem has occurred in many IoT devices. We use computing techniques to solve this matter and enhance the speed of the transition. These delays are problematic for users. We use edge computing to minimize the latency smoothly (Shalin, et al. 2019, Safavat 2020). In the processing of data, IoT devices should not create a millisecond delay. The example of this technique is the flight in which millisecond delay can create a horrible impact.

Table 1. Advantages and disadvantages of existing research work connected with the Cloud, Edge, and Fog computing.

Approach	Goals	Specialties+ Limitations-
Shifting from cloud computing to fog.	Techniques are discussed to transform from cloud to fog.	+ resolves the compatibility issues and data storage problem. -Restricted up to two computing techniques
IoT security including design and challenges.	Resolve security problems, challenges, and future opportunities.	+ security issues are solved. -Explored the new domain of opportunity
Decoy technique and fog computing for data protection.	Security of big data is provided.	+ protect the data effectively. -limit in the medical domain.
Fog computing: mitigating the inside attacks of data.	Capture inside the theft and intruders.	+Algorithms are explained -Use to check the inside theft.
Smart-e-health care using Edge computing.	A system is defined as dealing with the health care department.	+ A efficient data sharing system is defined -Target specific healthcare domain.
Identity-based encryption scheme for fog computing	The encryption scheme is developed.	+ robust scheme is designed to encrypt the data efficiently. -Not specified.

10. Conclusion

This paper concludes that the combination of the Internet of things and cloud, fog, and edge computing provides ease for the data securing. The hybrid technology protects the data, and the efficiency of data processing is enhanced. This paper provides the knowledge of existing techniques that help in making the security secure. We explain the innovative work and computing techniques, and the primary purpose of this paper is to explore how the Internet of things helps to improve data processing and data storage. All in all, it is concluded that the combination of decoy technology and the behavior of profiling can make a data processing system secure.

Our future work include development of detection systems for inside or outside attackers.

References

[1] V. Narayana, A. Khan, M., and K. Kumar, "A Paradigm Shift from Cloud to Fog Computing," pp. 385-389, 11 2015.

[2] T. Xu, B. Wendt, and M. Potkonjak, "Security of IoT Systems: Design Challenges and Opportunities," 2014.

[3] R. Amir, N. G. Tuan, N. Behailu, and A. Arman, "Exploiting smart e-Health gateways at the edge of

healthcare Internet-of-Things: A fog computing approach," in *Future Generation Computer Systems*, 2017.

[4] H. Prachi, P. Kulkarni, and D. Kute, "IoT based data processing for automated industrial meter reader using Raspberry Pi," in *2016 International Conference on Internet of Things and Applications (IOTA)*, 2016.

[5] J. S. Robert, "The Edge of Cloud Computing," 2019.

[6] J. S. Salvatore, B. S. Malek, and D. K. Angelos, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," 2012.

[7] N. Farjana, R. Shanto, N. Md.Julkar, Mahi, and M. Whaiduzzaman, "An Identity-Based Encryption Scheme for Data Security in Fog Computing," 2020.

[8] B. Mhidi, B. Nabil and A. Adnane, "A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System," 2019.

[9] S. Devkar, A. Gokhane, J. Kaudare, S. Kambale and P. Abhonkar, "International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056," 2016.

[10] M. A. A.-J. Nabeel, "A Survey on Cloud Computing Security –Challenges and Trust Issues," *International Journal of Computer Science and Information Security (IJCSIS),* vol. 18, no. 5, 2020.

[11] V. Anthony, V. Toby and E. Robert, Cloud Computing: A Practical Approach, New York, 2010.

[12] E. D. A.-T. Dhiah, B. Simon and K. Ala', "Fog Computing-based Framework for Privacy Preserving IoT Environments," *International Arab Journal of Information Technology,* vol. 17, no. 3, pp. 306-315, 3 May 2019.

[13] R. T. Narendra, "Cloud Computing Security Challenges," *International Journal of Innovations In Engineering Research and Technology,* vol. 7, no. 6, pp. 2394-3096, 2020.

[14] P. Shalin, D. Dharmin, P. Reema and D. Nishant, "Security and Privacy Issues in Cloud, Fog and Edge Computing," *The 3rd International workshop on Recent advances on Internet of Things:,* vol. 160, pp. 734-39, 4-7 November 2019.

[15] D. B. Rawat, M. S. Parwez and A. Alshammari, "Edge Computing Enabled Resilient Wireless Network Virtualization for Internet of Things," Proc. of the *3rd IEEE International Conference on Collaboration and Internet Computing*, Oct 15 - 17, 2017. San Jose, California, USA..

[16] "Digiteum," 8 2019. [Online]. Available: https://www.digiteum.com/cloud-fog-edge-computing-iot.

[17] "WINSYSTEMS," 4 December 2017. [Online]. Available: https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/.

[18] B. Kay, E. Antonio and E. Matthias, "Cloud, fog and edge: Cooperation for the future?," 2017.

[19] Y. Yang, "Multi-tier computing networks for intelligent IoT," 2019.

[20] Medha and c. Krishna, "Medical Big Data Protection using Fog Computing and Decoy Technique," *International Research Journal of Engineering and Technology (IRJET),* vol. 6, no. 2, 2019.

[21] A. A. Laghari, H. He and A. Khan, "Quality of experience framework for cloud computing," in *IEEE*, 2018.

[22] R. Nazir, Z. Ahmed, Z. Ahmad, N. N. Shaikh, A. A. Laghari and K. Kumar, "cloud computing Applications," 2020.

[23] S. Ali, V. Kumar, A. A. Laghari and S. Karim, "Comparison of Fog Computing & Cloud Computing," in *IEEE*, 2019.

[24] Abro, Adeel, D. hongliang, M. a. Ali, L. s. Ali and h. H. Mohammadani, ""A Dynamic Application-Partitioning Algorithm with Improved Offloading Mechanism for Fog Cloud Networks.," 2019.

[25] A. A. Laghari, H. He, S. Karim, H. A. Shah and N. K. Karn, "Quality of experience assessment of video quality in social clouds. Wireless Communications and Mobile Computing," 2017.

[26] A. A. Laghari, H. He, M. Shafiq and A. Khan, "Impact of storage of mobile on quality of experience (QoE) at user level accessing cloud," 2017.

[27] A. A. Laghari, H. He, K. A. Memon, R. A. Laghari, I. A. Halepoto and A. Khan, "Quality of experience (QoE) in cloud gaming models: A review," *multiagent and grid systems,* pp. 289-304, 2019.

[28] L. A. Ali, H. He, M. Shafiq and A. Khan, " "Assessing effect of Cloud distance on end user's Quality of Experience (QoE).," *2nd IEEE international conference on computer and communications (ICCC,* pp. 500-505, 2016.

[29] M. Hina, H. Lei, A. A. Laghari and S. Karim, "Quality of Experience and Quality of Service of Gaming Services in Fog Computing," *In Proceedings of the 2020 4th International Conference on Management Engineering, Software Engineering ,* pp. 225-228, 2020.

[30] A. Wagan and A. Umrani, "Effect of Packet Loss and Reorder on Quality of Audio Streaming.," *EAI Endorsed Transactions on Scalable Information Systems,,* 2020.

[31] Sunitha Safavat, Naveen Naik Sapavath and Danda B. Rawat, "Recent Advances in Mobile Edge Computing and Content Caching," *Journal of Digital Communications and Networks,* Vol. 6, No. 2, pp: 189-194, May 2020.