Edge Computing reducing load but at cost

- Term Research Paper

Name: Sudhanshu Jha
Campus ID:DA65613

Table of Contents

1.Introduction:

A new high-tech society is being created in the modern world as a result of the utilization of IOT devices to connect numerous intelligent devices with extensive applications. Due to the significant restrictions on computer resources caused by the amount of data created by these IOT devices, it is becoming more and more common to shift workloads from critical computing resources to computing systems with adequate capabilities, such as servers and cloud computing. The process of reducing load, however, carries a great deal of danger if there is any breach, such as data loss, bandwidth issues, latency issues, or network device failure.

To reduce these risks and challenges, the phrase "edge computing" is utilized in the industry today. Task management needs to be used well with edge computing networks in order to make the most of IOT applications and edge computing devices.(Western Digital, 2021). It happens frequently that edge computing and cloud computing are mistaken with one another. Cloud computing, on the other hand, refers to a situation in which resources can scale up or be utilized as much as possible without restriction. By implementing edge computing on IOT devices, which stores data on edge nodes, the processing strain on centralized servers is reduced.(Ozcan et. ai., 2019).

By processing certain data on a group of connected servers at the network's edge, close to the data source, edge computing is a technique for optimizing cloud computing systems . In turn, less data is sent between local PCs and other devices and the main cloud data center. This research paper explains how edge devices are utilized for parallel processing and can be employed in distributive architecture, along with the models that can help to address security risks and limits with the edge devices to reduce latency problems.

2.Literature Review:

As society becomes more intelligent and human demands keep growing, intelligence is increasingly being used in business and to meet the needs of everyday people. Due to network latency and bandwidth concerns, security paradigms, and other factors, a number of cloud technologies have been developed where data may be stored and processed. However, due to these restrictions, a lot of resources are consumed and utilized. By substituting edge devices close to the data source for servers, the developing technology known as edge computing can address the majority of cloud computing's issues.

Edge solutions helped to transition the cloud model, which includes computing, resources, storage, and networking capabilities, to the edge network, which helped to provide intelligent services over edge to many IT sectors and meets the requirements and standards of IT industries. It is utilized in a variety of fields, such as data optimization applications, real-time data business, intelligence applications, and to solve network latency and capacity problems.(Dong et. al.,2002). The use of edge devices permeates every sector of society, including the military, the armed forces, the transportation industry, autonomous cars, cameras, robots, the internet of things, and more. In turn, this led to a large rise in the number of linked devices online. As a result of the IOT's integration with mobile devices, users now have access to a lot of data.(Song et. al.,2017).

Edge computing and cloud computing should work in tandem to accelerate the digital transformation, not as a replacement for one another. For in-depth analysis and a meaningful outcome, the data on the edge nodes is still converted and sent to the cloud. The phenomenon

that results from combining the two technologies is that big data applications are now being computed and thoroughly analyzed on the edge side. This essay outlines all of these concepts and makes an effort to define a better concept in terms of proposals like the use of edge computing in online education and some related works that have been debated and acknowledged.

3.Technical Details:

When latency must be regulated to lessen network saturation and when a centralized infrastructure is under a heavy processing load, an edge computing solution is necessary. Fog computing is an expanded form of edge computing that employs edge devices for storage, local communication, and computation that takes input and produces output for the physical environment. Fog nodes serve as an intermediary layer that decides whether to process data locally instead of sending it to the cloud.Here is a description of the fundamental three components for input, processing, and output: A data source in the input is any endpoint that collects and receives data from clients or its surroundings. Data sources for the Internet of Things include sensors, databases, social media, etc. Following data collection, the processing function offers useful observations, identifies patterns and trends, generates tailored recommendations, and enhances performance using machine learning or data analytics models. A few doable activities must be completed in order to view the results from earlier stages. For humans and robots to communicate, edge devices must conduct a dashboard, some visualization, and monitoring.

In modern technology, a CDN (Content Delivery Network) is a popular way to handle heavy network traffic by efficiently spreading the request to numerous servers spread across various geographic locations. One example of properly leveraging edge computing is CDN, which has been used to effectively provide web content on numerous websites, including Facebook, Netflix, eBay, and others. If an application is service-related, then there may also be a case of SLA violations. For example, an application that provides a request for a high number of users in a specific geographic area will cause a network latency issue.

Data mining, however, is not given enough attention due to a lack of time and resources, and specific applications and principles are no longer taught. This will also be the main focus of the subsequent activity. However, there is more development potential in connecting the "big data" and "Internet" trends, medical data with the two, infectious disease prevention with the medical industry, and broadening the development path. Additionally, encryption is required as well as the development of a defense model to thwart different attacks in order to handle the issue of user data security.(ZHIHAN et. al. 2021)

The network latency problem of CDN is resolved using a straightforward approach. The exchange server and origin server are the two sorts of servers that are employed. Multiple exchange servers are initially connected to the origin server. Exchange servers, also known as point of presences (POPs), are dispersed throughout a certain geographic area and function as edge nodes. Because the POPs servers' caching strategy depends on their performance, the CDN architecture raises system dependability based on the servers. The request is routed to the other close-by servers if one POP goes down.

A smart city is becoming more common in the modern day due to an increase in IOT device usage. Real-time data processing now faces additional difficulties as a result of the large data stream created by the exponential expansion of IOT devices. Due to their proximity to IoT

equipment, edge computing devices in mobile application domains such as smart cars, vessel monitoring, etc., must be both energy and space efficient. The improvement in processing capacity of processors used in mobile devices in the preceding decade motivates the case for using such weak devices in edge computing due to their compact form factor and low power consumption.

Some technology such as WD's Ultrastar Edge make edge more efficient with 40 CPU cores, 512 GiB of RAM, a lightning-fast GPU for artificial intelligence and machine learning needs, more than 60 TB of flash memory storage, and built-in 100 Gigabit Ethernet networking, Ultrastar Edge is a high-performance solution. It also offers support for FIPS 140-2 Level 2 physical security and a Trusted Platform Module for cybersecurity to maximize data protection and security in non-traditional IT situations.(Western Digital , 2021)

4.Risk, Limitations And Strategies:

4.1 Risks

There are two major risks that is identified by this study-;
Attacks In Fog Computing: Attacks such as Forgery, Tampering , Spam, Sybil, Jamming etc. By tackling the major technical problems and complexity of cloud computing, fog computing technology has broken new ground in the realm of modern communication. This technology is subject to several security and privacy risks involving data and services, though. The current security and privacy solutions of cloud computing cannot be used in a fog computing network due to the various properties of fog computing, such as spatial dispersion, mobility, and heterogeneity.(Xiaoming et. al.,2008)
Privacy Risk: The exchange, collection, processing, and transmission of users' sensitive data through fog nodes is posing a severe threat to privacy, which is a key challenge for fog computing. Each user wants their data to be safe and secure when using wireless technology, however due to the presence of malevolent users and intruders in the network, it is sadly very challenging to protect users' personal data. Maintaining privacy is crucial from both the provider's and the user's points of view.(Alwakeel et. al., 2021).

4.2 Limitations

A significant restriction for edge devices is thought to be data storage and protection. Because of its restricted storage capacity and in contrast to cloud computing, this device cannot increase or reduce its storage capacity. The edge devices need to be set up effectively because there is an enormous rise in data coming from various IOT devices, sensors, and robotics. However, if some crucial data is lost in the data sprawl, it could pose a hazard to an organization. Data sprawl is done on edge devices by removing the unnecessary data at the edge nodes without transmitting it to the cloud. Configuring authentication and authorisation is difficult due to the numerous edge devices utilized in a company. Hackers will be able to access the device if the passwords are not correctly set up. A recommended approach can make efficient use of expensive edge devices like the Raspberry Pi, ESP32, Sub Gigahertz, and others.(R. Et. al., 2019)

4.3 Strategies

Edge computing implements security on edge devices using the 5 P's technique. A) People: The most vulnerable resource is people. They should be educated on cybersecurity

regulations, and ongoing learning should be required. B) Policies and Procedures: In order to know the state of the edge devices, certain rigorous policies and some standard operating procedures must be put into place. C) Process: To reduce the risk of edge security, it is necessary to employ a list of planned procedures that people must adhere to. D) Products: Businesses need to understand the end-to-end devices that link hardware and software and are used in IT operations. E) Proof: All of these are continuously tested and monitored in order to find and fix flaws. Additionally, containerization technology is used to distribute applications in parallel, allowing for edge device and application remote debugging.(Javid et al.,2020).
Security at the physical and network levels is a crucial component of edge modeling with the deployment of 5G networks, and it should be distributed as follows:
Physical security: This covers acts that could lead to the loss of a device or data as well as unauthorized adjustments that introduce malware through physical access.
Operating Systems: The software applications that are used in edge devices are protected at this level. Implementing firewalls that can prevent unauthorized access to the device through the network is another part of the process.(Devi et. al.,2022).
Edge Networks: The edge devices require message encryption approaches and techniques due to the use of numerous networking strategies such as LORAWAN, ESP32, Wi-fi, and many more to connect to them.(Atos, 2021).

5.Implications For Society And Industry:

5.1 E-learning Platform Using Edge Technology

Due to the fact that e-learning has always included technology to make learning platforms easier, the integration of e-learning with information and communication technologies (ICT) has significantly changed the learning environment. Online learning, distant learning, and network learning are only a few of the different approaches used to promote it. Resources are exposed to danger and vulnerability online because they are so easily accessible. The integrity, confidentiality, and availability of data are three aspects that many E-Learning platform companies strive to uphold. Information and data privacy are referred to as confidentiality. The data is protected against unauthorized access by one person and kept confidential. Integrity is the ability to keep data original while retaining its completeness and accuracy in the face of hostile attack. Assuring that the authorized user has access to data and information is known as availability. To provide security for the E-Learning platform, several algorithms were developed on edge devices. Two-Level Access Control is a common authorization mechanism that encrypts the service request and public key to share a secret key and ensure message confidentiality while in transit. According to this algorithm, if a document is changed or updated by an uninvited person or piece of software, the recipient will receive a different digest for the original message. The log files can be used to track down deletions, which helps to ensure the resource's availability and integrity.(Bhat et al.,2022).

5.2 Implication of Edge in Living Technology

The world's expanding population is one factor driving up demand for smart buildings. The issue of what physical and software architecture to employ for their execution, however, is still open. There have been a number of problems with current architectures in the past. Private information, acceptance, and real-world performance are the touchy subjects. In order to deploy computing nodes that serve as heaters inside of homes and workplaces, edge

computing employs a Qarnot model architecture. The four layers of the architecture are the Qrads, the Qarnot smart building resource manager, the composed process of the services, and the smart building processes. When an alarm is detected, the flow routes the data it received from Qrads to the alarm service and sends an SMTP notification.Utilizing Q.rads technology, which is used for local compute, storage, and networking, as well as a platform that can send sensory data to local services and distributed processes, is the overall benefit of Edge computing in smart buildings.(Y. et. al.,2017)

5.3 Recent Implications of Edge with Timelines

The most documents are published in the year 2020, followed by the year 2019. Computer science and engineering was the subject area in which nearly 47.8% of the documents were found. Conference papers and articles are the second and third most common kinds of documents, respectively. According to the examination of the various countries, China has the most documents over the course of the eras. We also looked at documents written by different authors; the average publication had between 5 and 7 authors. The most documents are in the Westerlund t collection. The software for the VOS viewer 1.6.16 version also conducts network analysis. Numerous analysis kinds, including co-authorship analysis, co-occurrence analysis, citation analysis, and bibliographic coupling, are carried out using the same database.(Deshpande,2021).

6.Suggested Course Of Study:

In order to solve the latency and bandwidth problems and improve the user experience, investments in edge computing require a lot of engineering work, capital expenditures, and services. Due to its distributed nature and the fact that the majority of devices in industrial edge computing are exposed, this technology must solve numerous security difficulties. The majority of security and safety techniques used in industrial computing are recognized to be domain-specific. ISA84 and HARA (Hazard Analysis and Risk Assessment), on the other hand, should be combined to identify the additional concerns.Cloud computing will pose a severe danger to the security of data depending on how the data is distributed and how much data is generated at the source. To serve many IOT applications that are time-sensitive and data-intensive, fog computing can be employed in conjunction with edge nodes. In order to manage and monitor all of the edge nodes' resources, edge computing needs well-designed API services.

To maintain the latency and bandwidth, cameras are mounted on a number of edge computing devices, and deep learning algorithms are run on the edge devices. It gives people the chance to store a lot of data and offers a visualization that many organizations that support robotics and video processing applications can use to help them make informed decisions.

7.Conclusion:

Discovering and demonstrating how Edge Computing is used to address latency and bandwidth challenges in the current environment was the main goal of choosing this topic and doing the research. The security risk and network delay will increase as more data is transferred to the cloud and analyzed there. By positioning it close to the source device and

applying a deep or analytical method to address the problem, edge computing technology will be able to resolve this issue. The utilization of Edge Computing in the blockchain and how the technology is applied in real-time applications and industry are also covered in this article. By contrasting typical cloud architecture versus edge computing in terms of cost and energy use, this paper also gives information. Utilizing an end-to-end solution for edge computing and offering customizations in the IOT sector, which can be useful, along with consulting services that can aid customers with emerging technologies.

8.Annotated Bibliography:

Alam, Malik Zaib, Sarfaraz Ahmed, Haneef Khan, Md Imran Alam, Mohammad Rafeek Khan, and Shams Tabrez Siddiqui. (2022). "Mobile Edge Computing: Security and Privacy Issues, Challenges and Countermeasures." *IUP Journal of Computer Sciences*.

In this article, the author talks about MEC (Mobile Edge Computing) and MEC-related security. A cutting-edge technology called mobile edge computing enables effective and quick data processing on 5G networks. Given that it creates an environment for cloud computing and IT services, it may be advantageous in Internet of Things (IoT)-based situations. Furthermore, as MEC is frequently installed close to the edge of the network, it lacks terminal servers. However, a number of new security and privacy-related issues will arise as a result of the distinctive characteristics and operating principles of MEC. The many solutions to the security-related problems are discussed in this study. Finally, recommendations are made to increase the security of MEC services.

The paper addresses five MEC security concerns: availability, mutual authorization, authentication, confidentiality and integrity, and access. Security measures outline mobile edge network issues, their many defenses, and attack types. The examination of the security challenges and solutions offered in the article are predicated on MEC deployment in the near future. The paper also explored security concerns with regard to MEC.

Alwakeel, Ahmed M. (2021). "An Overview of Fog Computing and Edge Computing Security and Privacy Issues." *Sensors (14248220)*.

Fog computing and edge computing, two novel cloud computing paradigms, are covered in this article along with their security and privacy implications. Fog and edge computing, which differ from cloud computing in that they have unique characteristics, pose some new security and privacy problems. The authors displayed a variety of attacks, including some particular to each environment as well as attacks that are common to both technologies, such as DDoS attacks and attacks on shared resources. A few potential defenses that might lessen some of the listed threats are also presented by the author in this work Sensors 2021, 21, 8226 17 of 20. Through investigating the vulnerability of these technologies, we discovered that there are many unexplored potential research areas and that the security aspects of the two technologies are still far from being satisfied. The paper concludes with a summary of the key dangers for the two technologies, as well as references to several works in the literature that examined these dangers and the associated assaults. In order to develop a security reference architecture for fog computing, we believe that the authors'

recommended fog computing pattern might be improved and expanded upon with security patterns.

This essay discusses the dangers, security concerns, and different security measures that apply to edge and fog computing. Additionally, authors discuss the protective measures that one should take against threats and assaults.

Atos. (2021). “A 2021 perspective on edge computing”. *White paper Published by Atos.*

This white paper talks about the organizational view of edge computing and devices used in it in order to implement the security and computation in edge computingSince there are many devices, choosing the right class that offers multiple storage and compute capabilities will be useful. The Edge technology is based on the devices being picked. Data has been divided into many categories, including distribution alone, simple processing, complex processing, and multi-application processing, in order to handle modeling. The distribution of security at the physical and network levels, which is a key component of edge modeling with the installation of 5G networks, is as follows Physical security: This covers acts that could lead to the loss of a device or data as well as unauthorized adjustments that introduce malware through physical access. Operating Systems: The software applications that are used in edge devices are protected at this level. Implementing firewalls that can prevent unauthorized access to the device through the network is another part of the process. Edge Networks: The edge devices require message encryption approaches and techniques due to the use of numerous networking strategies such as LORAWAN, ESP32, Wi-fi, and many more to connect to them.

Key takeaways from this whitepaper by Atos is , these analyses are made possible by the fact that Atos is a company that offers an all-inclusive edge computing solution, IOT adaptations that can be beneficial in a certain industry, and consulting services that can assist clients in using emerging technologies. This company gives its clients and workers access to a secure and sustainable information space from anywhere in the world.

Bhat, Sameer Ahmad, Dalia Alyahya, Muneer Ahmad Dar, and Saadiya Shah. (2022). “Edge-Computing Based Secure E-Learning Platforms.” *2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Artificial Intelligence in Information and Communication (ICAIIC).*

The use of information and communication technologies for e-learning is discussed in the article, which has had a significant impact on the field of education. The learning market curve is anticipated to reach a value of 840.11 billion, according to statistical data collected from throughout the world. Despite the fact that e-learning is a platform for students, lecturers, or instructors to deliver a learning resource, the online learning resources are vulnerable to threats on the internet. The edge computing paradigm has been introduced as a solution to the authentication and data access issues that arise when employing cloud storage for e-learning systems. Since the edge users and EC (edge computing) resources are close by, location-based services are used to give authentication and authorisation. As edge computing makes use of numerous trust domains, identity assignment on those domains is crucial for mutual authentication.

Cross-domain authentication protects a user's data and privacy security in heterogeneous networks and multiple domains. Therefore, the users allocated to those networks can be authorized without the requirement for actual server authentication, a specific database will be grouped in edge computing and stored in an edge network

The author of this essay discusses the problems with authentication and data models in e-learning systems as well as possible fixes. It described how edge networks can function as a proxy server for authentication, reducing the load on the primary authentication server and speeding up response times for users.

Deshpande, Sonali, and Nilima Kulkarni. (2021). "Recent Trends in Cloud Computing and Edge Computing."*Library Philosophy & Practice.*

This study establishes the fact that a bibliometric survey on edge computing, fog computing, and edge intelligence is conducted by taking into account Scopus, the most widely used and biggest database globally. 2016 to 2020 are taken into account for the database. The keyword search with AND and OR operators is used for database searching. As a result of the search, 204 documents in total were found. For this database's analysis, various parameters are taken into account. The majority of the documents are in Chinese, followed by English, it can be seen. The results of the keyword search show that the term "fog computing" is used most frequently in publications. The year 2020 publishes the most documents, followed by the year 2019. Nearly 47.8% of the documents were in the subject field of computer science and engineering. When it comes to document type, conference papers and articles come in second and third, respectively. China has the most documents over the course of the periods, according to the analysis of the various nations. Documents by various writers were also examined; the average number of authors per publication was between 5 and 7. Westerlund t has the largest amount of documents. The VOS viewer 1.6.16 version software also performs network analysis. With the same database, several analysis types like co-authorship analysis, co-occurrence analysis, citation analysis, and bibliographic coupling are performed. The results of all these various network analyses provide some very important information regarding the many topics discussed above. Additionally, it is possible to see that the two years 2019 and 2020 are when the majority of the work on edge computing is completed. It is anticipated that this area would see very extensive and significant work in the future years.

This article basically gives the timeline of advancement of edge technology and cloud technology over the years. The major takeaway from this article is the most of the advancement in the field of edge technology is recent around 2019 and 2020.

Devi, Odugu Rama, Julian Webber, Abolfazl Mehbodniya, Morsa Chaitanya, Parag S. Jawarkar, Mukesh Soni, and Shahajan Miah. (2022). "The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence." *Scientific Programming*.

The foundations of how the brain processes information are described in this article. The study also looks at how different apps handle edge-registering safety. The paper splits its primary research successes in edge-registering safety into five categories and then provides an in-depth analysis of the current state of safety in each of the aforementioned sectors. In conclusion, the likely exam topics for the future have been

predicted. Edge Intelligence offers cloud-computing capabilities on the edge network, enabling it to satisfy the demanding standards of the future 5G, particularly the low-inactivity and high-data transfer capacity standards. Due to its basic attributes of proximity awareness, little idleness, high data transmission capacity, etc., Edge Intelligence offers a wide range of applications. In this post, we present a thorough analysis of Cloud Computing, Edge Computing, and 5G as latency since Edge Intelligence is so crucial in the 5G era. It is typical for stations to be finished more quickly, and users can take advantage of the convenience that edge knowledge provides while remaining safe by addressing these pressing edge processing security problems later.

The author in this essay discusses current and future developments of 5g networks over the Edge technology and the security concerns in the Edge intelligence in the Era of 5G era and network.

Dong, Jingya, Chunhe Song, Tao Zhang, Yuanjian Li, and Hao Zheng. (2002). "Integration of EdgeComputing and Blockchain for Provision of Data Fusion and Secure Big Data Analysis for Internet of Things."*Applied Energy 325.*

In this work, they suggest a way to combine edge computing and blockchain to provide data fusion and secure big data analysis for the IoT, given the current condition of the rapidly increasing scale and amount of IoT data. In order to decrease the quantity of data transmitted by IoT and assure the security of IoT data, we offer a node-level lightweight data fusion approach and a hierarchical fuzzy hashing method. We use a lightweight data fusion technique to lower the quantity of data transit at the node level. To lessen the load on the cloud server, the edge node computes the local model, and the cloud node merges the local model to increase the model's representativeness. They suggest two techniques to decrease the quantity of data transmitted by the Internet of Things and guarantee the security of IoT data: node-level lightweight data fusion and hierarchical fuzzy hashing. They use a lightweight data fusion technique to lower the quantity of data transit at the node level. To lessen the load on the cloud server, the edge node computes the local model, and the cloud node merges the local model to increase the model's representativeness.

Key takeaway of this paper is that it discusses utilization to guarantee the consistency and validity of local and global models while ensuring data privacy, hierarchical fuzzy hashing and blockchain technology are used.

Javid, T., & Shuiguang, D. (2020). "Edge Computing: Models, Technologies, and Applications." *The Institution of Engineering and Technology.*

As edge computing is utilized as a model to develop the cloud services that employ edge networks, the author illustrates an overview and evolution of the field. By taking into account edge computing models, it will be possible to relocate processes that are connected to decision-making to potentially nearby data sources that can serve as an intermediary layer between data centers and edge sensors. Moving the data closer to the sensors is a solution to this problem because latency and bandwidth are the main issues in the modern digital era when sending data from the network edge to data centers for processing. In order for numerous computers to function in parallel and complete various tasks, a distributed computing resource was first developed. These

computers typically exchanged messages to communicate. This is where edge computing first emerged. Distributed systems were widely employed by companies all over the world as a result of the decline in computing power and storage costs. Due to this, the engineers decided to use the cloud computing approach to build a virtual computer inside the actual machine. However, this approach did not fully utilize the available resources, which prompted the creation of the containerization model, which called for the use of the same 11 operating systems by numerous programs but separate runtimes. With the help of all these models, edge computing was able to develop a setting that would undoubtedly change as computing technology advances.

This article provides a comprehensive explanation of how edge computing entered the market. The disadvantages of various computing model architectures and the application of containerization, which aids in the resource distribution of edge computing, were also discussed.

Ozcan, M. O., Odaci, F & Ari, I. (2019). Remote Debugging for Containerized Applications in Edge Computing Environments.

This article talks about the Industrial Revolution, which was brought about by the fusion of big data platforms, cloud computing, and industrial processing applications. The Industrial Internet of Things (IIOT) uses mobile edge computing (MEC) to process sensor data at large volumes and speeds. By bringing edge devices closer to one other, this method reduces latency and increases bandwidth per device over LAN networks. Application containerization is used in environments where virtual machines cannot be used, making it easier and faster to create and deploy applications. Adopting the containerization concept has few ramifications, yet, as it is difficult to replicate industrial scenarios with synthetic data, real data is needed, and processing these data necessitates a high-speed data server. In order to examine a potential risk early on in the development process, a remote debugging technique was built, enabling docker containers to build the program with all dependencies. The developer debugs using the Visual Studio IDE. On the edge devices, the security is implemented by the encrypted connection. It is possible to enable the ports that can be used to send data between edge devices by using the docker compose file.

The paper describes the new standards used by IIOT apps and discusses how remote debugging and containerization technologies can be implemented on the server to overcome storage and resource limits. Remote debugging of the edge application is made possible by opening the server port and turning on SSH inside the server.

R., Lombardi, F., Caprolu, M., Di Pietro, & Raponi, S. (2019). Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues.

The focus of this article is edge computing, which has grown in popularity over the years due to its advantages over cloud computing in some use cases. In order to more accurately reap the benefits of edge computing devices, this security problem makes use of the underlying technologies, namely virtualization and containerization. The most frequent problem with cloud computing is resource concentration, which renders it unsuitable as a general solution. It widens the gap between users and clouds, increasing network jitter and latency whereas less sensitive apps like gaming, customer records in shopping malls, and e-health care only need low latency and

mobility support.The data and services that are geographically closer to the area where those services are sought are delivered. Edge devices use "Fog Computing," a technology that makes use of IOT or IOE platforms with a single CPU and MBs of RAM to do the majority of tasks such local storage, computing, and communication. Due to the fact that the majority of server distributions and operating systems on edge devices are built on the Linux platform, this technique improves security across a wide spectrum of technology.

This article talks about how deploying virtualization might lessen the security risk on edge devices. Finding the edge devices that can be containerized to transport the data to a nearby place is a crucial aspect of this. It puts a lot of emphasis on the Operating System, which can assist in achieving the first degree of security for an application. In order to reduce latency, it also emphasizes network virtualization on edge servers that link directly to nearby IOT networks.

Song, Y., Yau, S.S., Yu, R., Zhang, X & Xue, G. (2017). An Approach to QoS-based Task Distribution in Edge Computing Networks for IoT Applications.

The author of this study described a method for distributing jobs in the edge computing network on a regular basis in order to enhance the number of tasks that can be processed there while also meeting the QoS requirements for edge computing. IOT has become a crucial component of the development of the infrastructure since it has the ability to connect numerous intelligent devices. Despite the IOT applications' quick development, a bottleneck in the computing infrastructure limits storage capacity, CPU power, and other resources, which creates issues for big data analysis and real-time application processing. Offloading the unneeded resources helped the IOT application operate better and is the short-term fix for these problems. Offloading, however, led to an additional problem with data transmission across WAN, which increased network congestion and latency for an IOT application. Due to the disadvantages of task offloading, the researcher is now using cloudlets, computing-enabled switches, and computing-enabled base stations at the network edge. The author suggests a task allocation strategy that greatly simplified the edge world. As incoming tasks are continuously provided by IOT applications, the task distribution should be applied on the edge network on a periodic basis. The time difference for task allocation between the two apps is noted, and this serves as an input for the upcoming jobs that will be processed on these applications.

The article explains how task dispersal was used since dumping resources had disadvantages. It is discussed how time intervals play a role in forecasting how tasks will be distributed among applications and in maintaining the quality of service on the edge network.

Western Digital. (2021). “High-Value Solutions That Make Edge Computing Effective and Efficient.”*White paper published by WD*.

The main point made by WD in this whitepaper is that Western Digital offers cutting-edge edge computing solutions to decision-makers for both commercial and military applications. These technologies give edge computing applications the performance, resilience, adaptability, and agility they require.

They also make it possible to design cloud-like experiences, albeit in a more confined space. This business provides its customers and employees with global access to a safe and sustainable information space.

Xiaoming Bi, Wenan Tan, and Ruohui Xiao. (2008). “A DDoS-Oriented Distributed Defense Framework Based on Edge Router Feedbacks in Autonomous Systems.”

DDoS (Distributed Denial of Service) attacks are a hazard to today's modern Internet generation, according to the majority of cybersecurity experts. By installing malicious software that blocks the system's upstream link and uses a lot of resources, DDoS allows attackers to take control of the majority of personal computers. This article suggests using the Internet autonomous system as a defense unit as a DDoS defense strategy. When an intrusion occurs, the victim collaborates with the edge routers of the autonomous system to choose the best edge router to filter information based on recurring traffic feedback, maximizing the effectiveness of defense. A BGP protocol is used for traffic exchange between Autonomous Systems (AS), which are networks connected to Internet service providers. Edge routers are routers or networking devices connected to AS's on the periphery. Distribution Through edge routers, packets are routed. To launch a DDoS attack, transmit a lot of traffic on the and flood the target with data packets, making it impossible for the victim to respond to requests. Such requests arrive at the edge devices from outside of ASs. With the help of edge routers, the traffic is screened. Utilizing an algorithm based on optimization concepts and allowing for a small number of routes DDoS assaults are restricted.

This article defines the usage of autonomous systems (AS) to prevent DDoS attacks. A concrete mathematical function is used in the algorithm that is suggested, and the results demonstrate that the survival ratio is high.

Y. Ngoko and C. Cérin. (2017). "An Edge Computing Platform for the Detection of Acoustic Events,"

The model presented in the paper describes the edge computing platform used for the detection of acoustic events. In the article, the Qarnot platform is introduced as a tool for designing smart buildings with servers that double as heaters. Qarnot's utility computing concept, which is deployed inside homes, workplaces, and other buildings, uses edge nodes that double as heaters. The heaters in question are referred to as Q. rads, and they have CPUs and sensors for CO2, humidity, temperature, etc. Data from the sensor devices are gathered and sent to the appropriate service by the Q. rads. The architecture is separated into four layers in accordance with the Qarnot vision: Q, the Qarnot smart-building resource manager (QSBRM), the services that make up the 14 processes, and the smart building process itself. rads. Three systems make up the platform for the acoustic framework: the data provider system, which generates data; the training system, which analyzes the data and performs statistical learning on it; and the decision system, which incorporates the server program and 12 calls into the training system for the occurrence of events. The primary benefit of the Qarnot architecture is data privacy, as activities carried out inside smart buildings also involve storage systems for keeping data there.

In this article, the author provides a summary of the Qarnot model, which aids in the development of edge computing-based acoustic event detection for smart buildings. It

has two benefits, the first of which is the edge platform, where local Q. rads serve as storage, network, and computing. The second is a platform for sensing data delivery to services and distributed operations.

ZHIHAN LV, RANRAN LOU, and HAIBIN LV. (2021). “Edge Computing to Solve Security Issues for Infectious Disease Intelligence Prevention.”

This paper discusses how the work develops an intelligent infectious disease prevention system based on an edge computing algorithm, and then further installs and improves the system's security defense strategy to guarantee the protection of users' private data. The simulation results indicate that it can guarantee security performance, increase prediction accuracy, achieve the best defense strategy for user privacy information at a lower cost, and do all of this while maintaining a user's privacy at a minimum cost. This provides an experimental basis for the later prevention and monitoring of infectious diseases. But there are some shortcomings. The edge computing algorithm serves as the foundation for the intelligent preventative system for infectious diseases. There are several shortcomings, though. The edge computing algorithm is the basic foundation of the created intelligent infectious disease prevention system.

However, due to a lack of time and resources, data mining is not given enough attention, and specific applications and principles are no longer explained. The following action will center on this as well. Meanwhile, combining the "big data" and "Internet" trends, fusing medical data with the two, fusing infectious disease prevention with the medical sector, and widening the development path will all have more development potential. Additionally, in order to address the issue of user data security, it is necessary to rely on encryption as well as build a defense model to fend off various attacks.