A Pragmatic Analysis of Security Concerns in Cloud, Fog, and Edge Environment

Manish Jena, Udayan Das, and Madhabananda Das

Abstract With the emergence of Fog and Edge architecture, optimization has become a significant aspect of Cloud computing. Not only do these changing architecture necessitate re-evaluating cloud-native optimizations and uncovering Fog and Edge-based outcomes, but the goals also necessitate a significant shift from focusing just on latency to focusing on energy, security, dependability, and cost. As a result, it appears that optimization targets have become broader, with the Internet of Things (IoT)-specific objectives emerging recently. Furthermore, in certain applications that need low latency, the delay generated by transferring data to the cloud and subsequently back to the application can have a significant impact on their performance. Existing IoT designs are becoming increasingly centralized, relying heavily on cloud solutions for data processing, analytics, and decision-making. This survey highlights the main security and privacy challenges that fog and edge computing confront, as well as in what way security concerns may influence the development and usage of edge and fog computing.

Keywords Cloud computing · Edge computing · Fog computing · Security issues · Edge nodes

1 Introduction to Cloud Computing

Cloud computing has risen to prominence as the most popular data storage and processing platform in recent years. It has extended to a variety of industries, including healthcare, real estate, banking, manufacturing, and so on. Instead of maintaining data on their local systems, businesses preserve it on the cloud. The Internet of

M. Jena · U. Das · M. Das (✉)
Kalinga Institute of Industrial Technology, Bhubaneswar, India
e-mail: mndas_prof@kiit.ac.in

M. Jena
e-mail: 2005240@kiit.ac.in

U. Das
e-mail: 2005280@kiit.ac.in

H. K. Thakkar et al. (eds.), *Predictive Data Security using AI*, Studies in Computational Intelligence 1065, https://doi.org/10.1007/978-981-19-6290-5_3

Things (IoT) is among the most disruptive technologies of the previous decade, and it is at the heart of a number of emerging trends, including smart cities [1]. Latency and network bandwidth are the only problems, which arise in IoT environments. Despite its various capabilities, the cloud's security remains one of its most crucial aspects. Every cloud computing server is concerned with privacy and security in a distinct way. Cloud analysts search for loopholes in the architecture and possible attacks to exploit them for cloud safety and security [2].

The emergence of mobile cloud computing technology is due to the convergence of mobile computing with cloud computing. Using a mobile device's thin native client or web browser, these centralized programs are then retrieved across wireless networks. Processes are enabled by a centralized server that follows a collection of rules. Computer software and middleware are used to allow smooth communication between devices linked via the cloud. Data is frequently copied by cloud computing service providers to defend against security threats, data loss, and data breaches, among other things. We separate cloud systems into two groups to better understand how they function. The front end is one thing, and the back end is another. Both are connected to one another via a network, most often (Fig. 1)

> the Internet. The front end is the user's or client's side of the application. All cloud computing platforms do not have to have the same UI/UX. On the back end, the cloud is made up of several computers, web servers, and storage devices. A cloud computing model may run any program, from data processing to computer games [3].

Cloud computing allows people to access critical data from afar and eliminates the need to invest in expensive computer and storage infrastructure. Cloud Service Provider provides basic infrastructure like a computer-generated interface for users to keep their data in Infrastructure-as-a-Service. Users utilize Operating systems and apps to process, network, and store data on their installed applications. This design includes hardware resources such as CPU, memory, the disc, and bandwidth. Users may run and manage their apps with Platform as a Service. They're given one base operating system, some development packages, and technology for developing applications [4]. Some resources are supervised, such as software frameworks and storage. Under Software as a Service, the cloud merchants provide all of the infrastructure and software, which is also known as 'on-demand software.

Cloud computing reduces the need for expensive computer and storage infrastructure and enables users to access data from any location. According to the demands of the users, resources are allotted dynamically. BNA (Broad Network Access) lets a person manage data from remote places using standard platforms such as smartphones, laptops, etc. Elasticity refers to the ability to scale resources up or down in response to demand [5]. For all sorts of emergency scenarios, including natural catastrophes and power outages, cloud-based systems provide speedy data recovery. Only 9% of non-cloud users claim that in less than four hours disaster recovery can be done. A global study found that around 39% of IT executives desire to invest in cloud-based emergency preparedness methods [6]. Cloud infrastructures enable virtual services to be powered rather than the actual software and hardware, lowering energy costs and cutting computer-related emissions. A cloud owner's full-time task

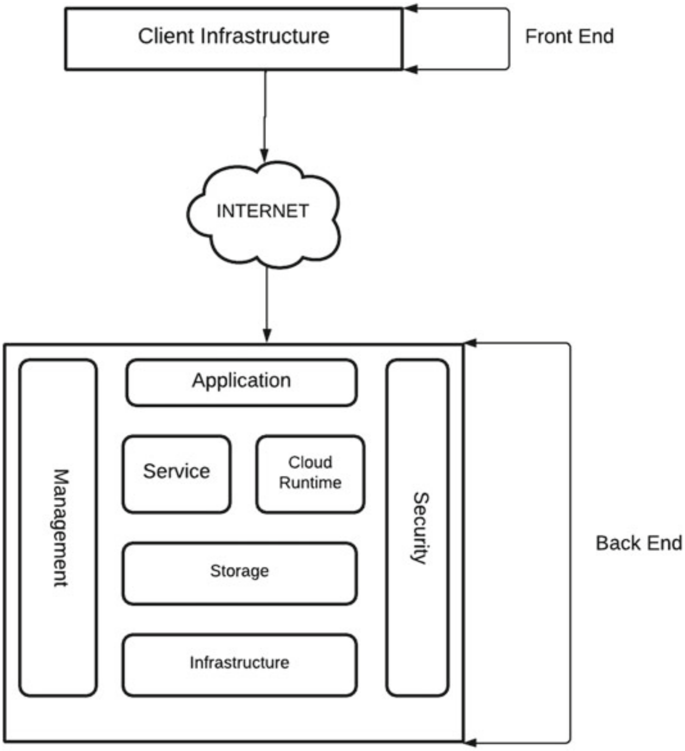

Fig. 1 Cloud computing architecture

is to thoroughly examine protection that is significantly more efficient than a standard internal system. According to Rapid Scale, 94 percent of producers observed a substantial improvement in security after transitioning to the cloud.

2 Introduction to Fog Computing

Fog computing adds a layer between the data's origin and the cloud. It is performed at fog nodes, which gather data from a variety of edge devices. It is a platform with a lot of virtualization which gives network and storage operations between end devices and standard cloud-based servers but not at the network's edge. Fog computing utilizes specialized networking devices known as Fog nodes to execute numerous computational activities at the network edge. Its primary characteristics are edge awareness, low latency, mobility support, real-time interaction, and heterogeneity.

All nodes aren't kept active at all times in fog computing [7]. When the data load is diminished, the computational unit of the Fog nodes may be switched off and activated as needed. As a result, the Fog environment is extremely scalable and of

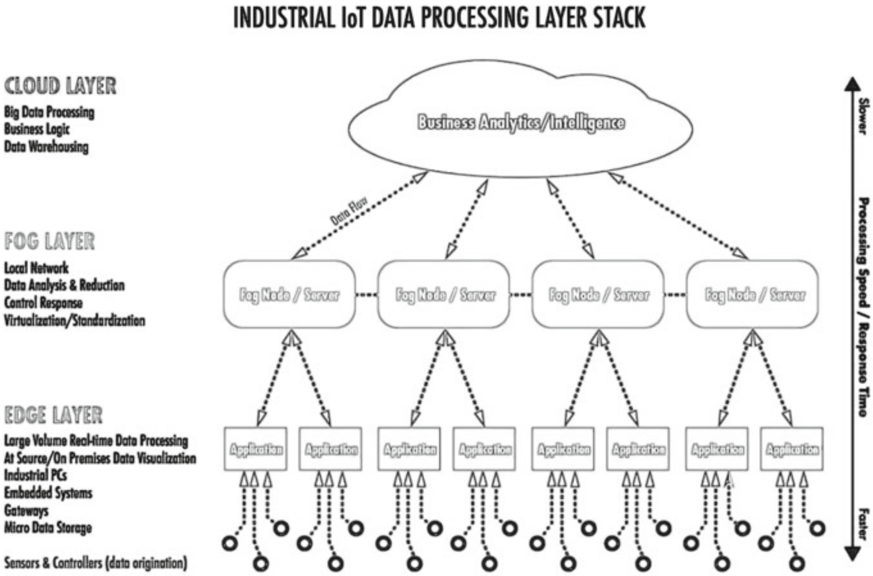
INDUSTRIAL IoT DATA PROCESSING LAYER STACK
CLOUD LAYER
Big Data Processing
Business Logic
Data Warehousing
FOG LAYER
Local Network
Data Analysis & Reduction
Control Response
Virtualization/Standardization
EDGE LAYER
Large Volume Real-time Data Processing
At Source/On Premises Data Visualization
Industrial PCs
Embedded Systems
Gateways
Micro Data Storage
Sensors & Controllers (data origination)
Business Analytics/Intelligence
Data Flow
Fog Node / Server
Application
Slower
Processing Speed / Response Time
Faster

Fig. 2 Fog computing layers [6]

low-energy. In addition, security protections for data privacy and intrusion prevention can be applied to each communication channel between the nodes. As a result, secure data transmission is possible. In rare instances, the fog network may be regarded as a point-to-point network. A fog-based system design is similar to the cloudlet idea, but with a stronger focus on the overall system resilience.

Fog computing is a three-tier system, with the lowest tier consisting of edge devices such as sensors, vehicles, or apps that generate data, the second level consisting of fog nodes that help in collecting data from multiple edge devices, and the topmost layer consisting of cloud data centres that gather data from fog nodes, as shown in Fig. 2.

As a result, fog systems must work together with cloud servers in order to perform tasks like orchestration, big data analysis, and distinct service delivery, implying that fog couldn't completely substitute cloud computing, and the two must work together to offer users on-time value-added services.

3 Introduction to Edge Computing

Edge computing was initially introduced around 2002, and it was primarily used to deliver applications across Content Delivery Networks. Taking advantage of the close proximity and resources of CDN end nodes in order to achieve a lot of scalabilities is the main purpose of this. Routers, base stations, and switches make up an edge node, which directs network traffic. In order to manage the packet data from several subnetworks they integrate, these devices perform complex processes. Edge computing, in a larger sense, may be defined as an agreed-upon strategy that additionally considers node ownership. Edge nodes, resembling cloudlets, are located near end nodes [8]. Edge Computing for Mobile was launched by the European Telecommunications Standard Institute (ETSI) in 2014 as a unique platform that provides IT and cloud computational power within the Radio Access Network close to users.

In an edge computing paradigm, data generated by devices is stored on the device or near the device rather than being transmitted to the cloud. Before delivering the information to the cloud, these gateways pre-process it. They provide a layer of protection against illegal access from other devices. The primary feature of Mobile Edge Computing is the presence of network control and storage resources at the mobile Radio Access Network's edge, with the goal of lowering latency. As a result, MEC is not a replacement for cloud computing, but rather a complement: The delay-complicated component of software can operate on Data centres, whereas the delay-tolerant compute-heavy component of an application can run on a cloud server [9]. Recently, fog computing was proposed as an extension of MEC, and edge devices are now defined as anything from smartphones to set-top boxes. These two regularly conflict & terminology is frequently interchanged (Fig. 3).

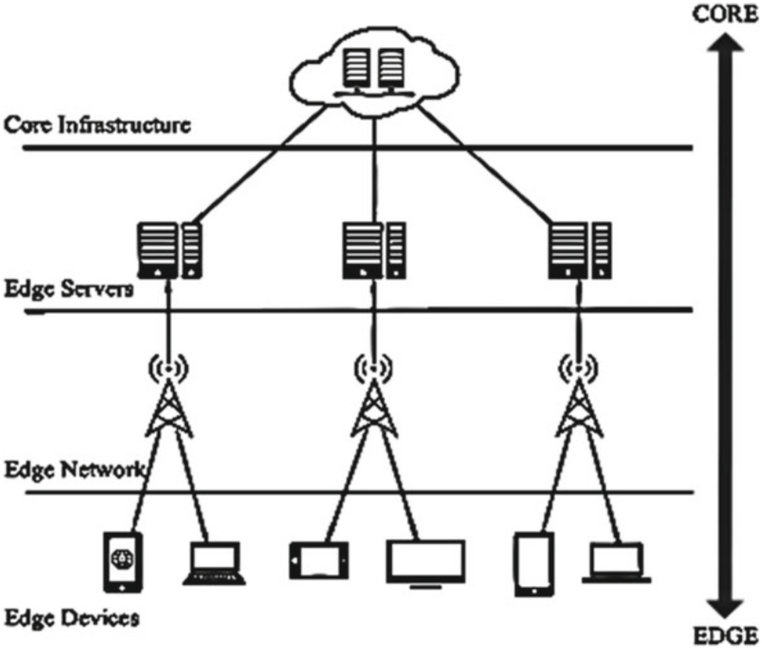

Fig. 3 Edge computing architecture [17]

In manufacturing, adaptive diagnostics in an industrial setting can advance the uptime of systems and equipment, deducting service expenditures. Edge-compute-generated fault codes get combined with historical repair information which can provide the framework for technicians, speeding up troubleshooting and repairs [10]. Computation on the edge permits public infrastructures and facilities to be checked for greater productivity in lighting, heating, etc. In traffic management systems, cameras and signals can mend safety and traffic flow. In the coming years, self-driving vehicles, where near-zero latency is critical, will be the most noticeable and dramatic examples of real-time edge computing. Smart wearable devices can store data on heart rate, temperature, and other metrics, then offer reminders for medication. Also, edge computing enables creators to ensure sensitive data, such as therapeutic imagery, which does leave the device to boost security and confidentiality. Cloud gaming establishments are looking to create edge servers in close proximity to gamers in order to decrease latency and deliver a fully receptive and immersive gaming experience.

It is preferable to cloud computing since it allows for real-time data processing with little latency. There will be less network traffic and faster data processing as a result. By filtering out sophisticated data and delivering it to the data centre at the edge device, the data's safety is increased. Low latency and bandwidth limits are important aspects of edge computing. The effect of low bandwidth at a certain site is reduced when the burden is moved closer to the user. Data analytics, Network Function Virtualization (NFV), and web monitoring are some of the examples of edge computing applications. Performing NFV on the edge layer increases efficiency while cutting expenses. On the gadget, data may be examined, and a single data summary should be stored in a centralized cloud.

4 Security Threats of Cloud Fog and Edge Computing

A plethora of new security concerns and risks was introduced in the cloud. Data is stored in the cloud by an unauthorized provider which is accessible over the internet, restricting both discernibility and handling of data. It is vital for all people to understand their role and the safety risks that cloud computing entails. The risks and difficulties related to cloud security are primarily the responsibility of cloud providers. Consumers are responsible for the security of their data stored on the cloud, whereas the cloud service provider is in charge of the cloud's security. Every cloud computing user is constantly responsible for safeguarding and controlling access to their data [11].

There are three services, namely:

I. **Software as a Service (SaaS)**: Cloud security concerns in this service are unquestionably data and access-related. 'On-demand software' is another term for this service. Every company should be worried about the sort of data it sends to the cloud, who has access to it, and what fortifications it has in place [12]. The

SaaS provider's role as a possible access point to the administration's data and procedures should also be evaluated. All of these occurrences demonstrate that attackers regard software and cloud providers as a tool to target more resources [6]. As a result, attackers are concentrating their efforts on this potential flaw.

Below is a list of security issues in this service:

- Authentication and authorization are ineffective.
- Data breaches and data losses.
- There is a lack of staff with the requisite skills to manage cloud application security.
- Data to and from cloud apps cannot be monitored.
- Identity supervision on the cloud is immature.

II. **Infrastructure as a Service (IaaS)**: In this, protecting information is risky. When consumer concern spreads to apps, OS, and network traffic, new risks develop. Administrations must analyse the current evolution of risks that extend beyond data as the focal point of IaaS risk. Clients obtain the hardware configuration as a virtual medium to host their information from the Cloud Service Provider. Users may create their own OS and apps, as well as process, network, and store data on them. Analysing the ability to prevent theft and govern access when developing cloud infrastructure is risky. Choosing who can send data to the server, tracking resources varies in order to detect anomalous behaviour, protecting and toughening instrumentation gears, and Increasing network traffic evaluation as a possible indicator of infiltration are all swiftly emerging common processes in defending large-scale cloud installations. Bad actors grab computing resources to mine bitcoins, then reuse such assets to target different aspects of the firm.

Some of the security issues in this service are:

- An assault that spreads from one cloud capacity to another.
- Unable to supervise the cloud activities and applications.
- Observing a virtual computer from the perspective of another virtual machine.
- Using the host computer to inspect virtual machines.
- Malicious actors are stealing data hosted in cloud infrastructure.

III. **Platform as a Service (PaaS)**: This solution enables organizations to create, manage, and accomplish Web applications without having to invest in costly setups. Consumers are given a base operating system, development tools, and the infrastructure they need to create apps. Providers of PaaS might specialize in a variety of fields. Database-specific PaaS providers exist, as well as a newer form known as the highly efficient application PaaS, which generates applications utilizing a graphical, low-code approach. PaaS includes infrastructure such as servers, storage, and networking, the same as IaaS does. Database management systems, middleware, programming tools, and business intelligence elements are all addressed.

- Deficiency of Secured Software Development Process with CSPs.
- Legacy software's given by the merchants.
- PaaS Platform's security controls and self-service rights aren't properly organized.
- Hackers can gain unauthorized access and modify configurations.
- Insufficient necessities in Service Level Agreement (SLA).

Computing in fog has recognized unique archives in the contemporary communication era by overcoming fundamental technological difficulties and restrictions in cloud computing. However, this technology is expected to pose a number of security and privacy risks in relation to facts and services. Several academics have planned literary works alleging that security vulnerabilities are prevalent in fog computing. As illustrated in Fig. 4, the changing characteristics for fog computing, like spatial dispersion, motility, as well as variability, prevent current cloud computing security and privacy solutions from working in a fog computing network. In the future, new cutting-edge security technologies will be necessary to solve the security and privacy concerns highlighted by fog computing [13]. Although fog computing offers advantages over cloud computing, there are a number of security problems that may prevent future fog-based systems from being implemented (Fig. 5).

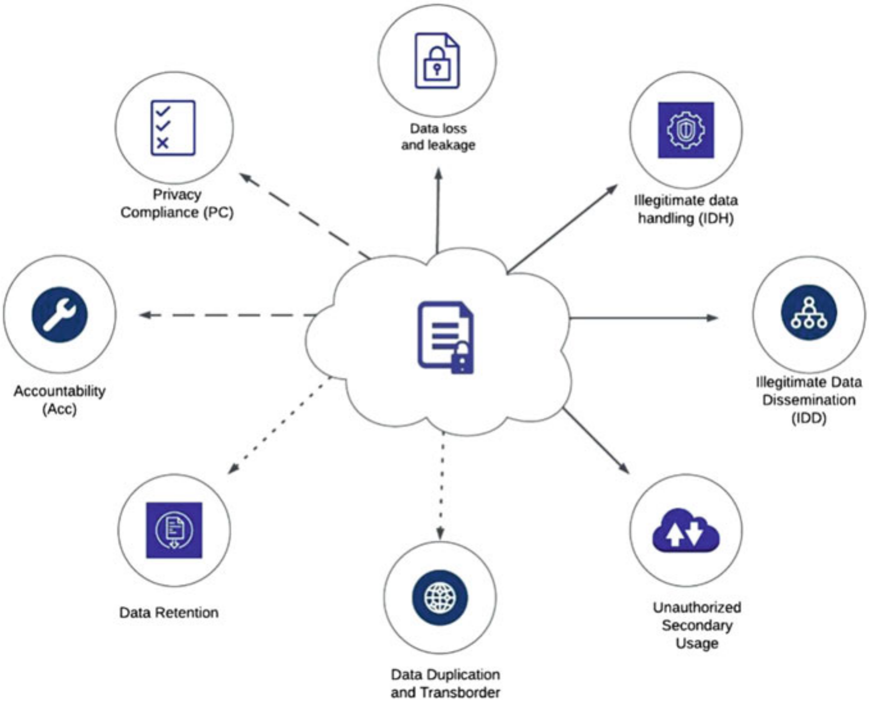

Fig. 4 Privacy in the cloud computing environment

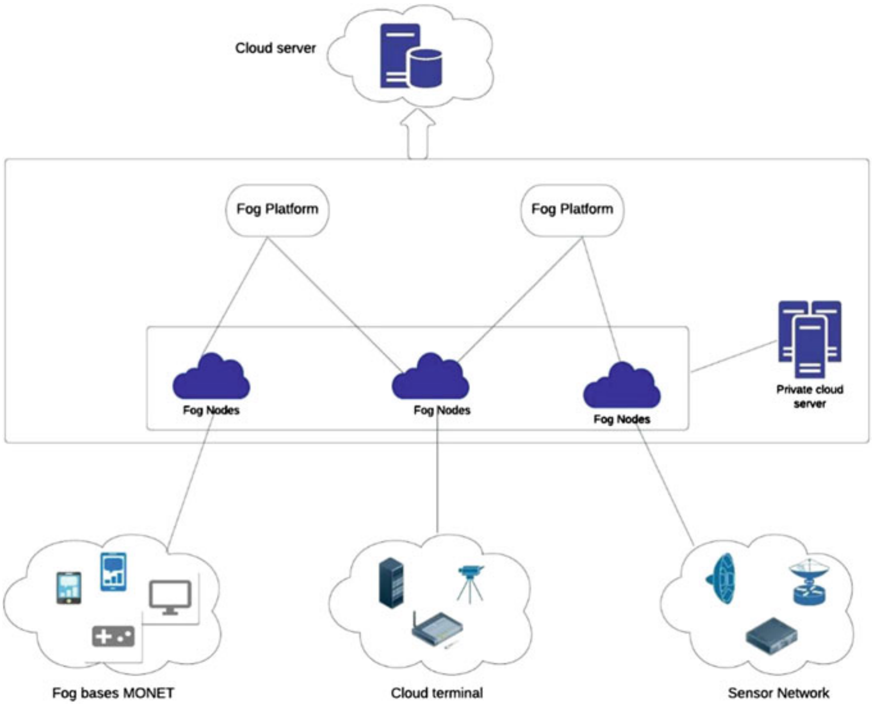

Fig. 5 The architecture of fog computing

Some privacy and security concerns are:

- Malicious fog node problems.
- Ways of attack recognition are ineffective.
- Multitenancy issues.
- Data recovery and backup are difficult when a system outage happens.
- Risky communication meetings between devices.
- Virtualization issue.

Besides the above privacy and security threats, there are other kinds of attacks in Fog Computing namely:

(a) **Tampering**: In this type of attack, attackers playfully modify the information to be communicated. It's difficult to detect this intrusion because data transfer may get delayed due to the flexibility and the transmission route's wireless nature in end-user.

(b) **Spam**: It is related with the unwanted data created by hackers, such as erroneous data received from people's computers and supplementary data. Spam causes enormous resource consumption in the network and deluding.

(c) **Virtual Machine Based Attack**: This is an exploit in which a hacker steals control of the hypervisor and uses it to create a virtual atmosphere within a virtual system. On a virtual machine, there are four basic forms of attack: guest to host, virtual machine to virtual machine manager, virtual machine to virtual machine, and virtual machine to virtual machine manager external attacks.

(d) **Denial of Service (DoS)**: It is a well-known exploit that can have an impact on a range of scenarios, including but not limited to fog computing, in which attackers send bogus information to fog nodes, which are then bombarded with limitless fake requests, rendering them unavailable to real clients.

(e) **Sybil**: Network attackers occasionally utilize bogus identities to manipulate fog computing's efficacy and performance, as well as the consistency of the nodes. This type of attack is known as a sybil attack. The attackers generate entirely untrustworthy crowd-sensing reports. They are also capable of hiding a legitimate end user's personal information.

(f) **Collusion**: This type of security breach includes more than two organizations conspiring to deceive and cheat lawful end users. They trick and attack a group of fog nodes, fog nodes combined with IoT nodes, or IoT nodes combined with cloud nodes in order to maximize the assault's effectiveness.

Edge computing design, like Fog Computing, is plagued by major security issues, putting customers' private or confidential data at risk, current edge computing security and privacy challenges, as well as encryption techniques and solutions [8]. Edge computing faces two major challenges: First, majority of the edge nodes are linked to a huge number of IoT devices with limited resources and different core components, resulting in a variety of routing processes to broadcast messages. This type of modification in the components might result in certain security issues. As a result, there may be a number of challenges with access control in the IoT context [14]. The key management of communications is the second problem that has some people concerned about edge computing security. While edge computing can enable end-to-end connection for IoT devices via multiple routing protocols, data concealment and integrity remain a concern. To address these problems, a superior key management and circulation method should be created.

Before we go into the security risks of Edge Computing, let's have a look at some of the factors that lead to these vulnerabilities in edge computing networks, which expose end users' personal information:

I. Edge nodes are closer to consumers in edge computing, which might result in the receiving of a large volume of sensitive data. If any of this information is taken, the repercussions will be disastrous.

II. In comparison to cloud computing, edge computing only has a portion of the network resources, hence advanced encryption methods aren't available.

III. The dynamic environment of the edge computing network is always changing. As a result, assailants may easily blend in with the group. Furthermore, developing security mechanisms for such a dynamic network is quite difficult.

Some of the common privacy and security risks are as follows:

(a) **Data storage, backup, and protection risks**: As previously stated, data stored on the outside lacks the physical safety barriers seen in data centres. In fact, it is possible to steal an entire database by removing the disc from an edge computing resource or inserting a memory stick to transfer data.

(b) **Perimeter defense risks**: Edge computing obstructs the entire perimeter protection as it widens the IT perimeter. It’s possible that edge systems may be needed to validate their apps with data centre partner apps, and the authorizations for this are commonly maintained at the edge. This means that a compromise of edge security might disclose access credentials to data centre assets, posing a severe security risk. Threats might be more difficult to deal with because security capabilities may be constrained at the edge due to changes in hosting architecture when dealing with perimeters.

(c) **Distributed Denial of Service (DDoS) Attack**: It’s a type of attack in which the attacker uses distributed resources, such as a set of compromised edge devices, to compromise the routine services offered by numerous servers. When an attacker sends an unlimited number of packets to the victim’s device from a hacked distributed device, it drains the target’s hardware resources, making it impossible to handle any other packet. As a result, any valid request is not met on time.

(d) **False Data Injection**: False data injection is a network attack in which an intruder injects false code that collects all stored data from the database and transfers it to the attacker.

(e) **Physical Attack**: It arises when the physical protection provided by edge technology is insufficient or shoddy. Physical threats will impair services in particular geographical zones as the deployment of edge servers spreads.

(f) **Cloud adoption risks**: Because cloud computing is still a new topic in IT, the hazards connected with edge computing in conjunction with cloud computing are very important. The risks are determined by the precise interaction between the edge and the cloud, which is easy to ignore because different cloud computing platforms and services address edge aspects differently. If the edge devices are simple supervisors, granting them secure access to cloud resources and apps may be problematic, needing a detailed examination of the cloud-to-edge connection, access control, and overall security protocols.

5 Potential Solution of Cloud Fog and Edge Computing

Security issues in cloud computing must be addressed effectively. If proper measures are not implemented, the cloud environment will grow increasingly exposed to hackers and invaders. To address the issues, the following are some of the solutions that should be considered while thinking about cloud computing [15].

- **Data Encryption**: When it comes to data security, encryption is said to be a more secure way. Before sending data to the cloud, it should be encrypted. The owner of the data can provide access to certain members.
- **Security check events**: We must guarantee that the cloud service provider provides specifics on promise fulfilment and problem reporting. These security

check events will reveal the cloud computing service provider's accountability and actions.
- **Monitor the Data Access**: Cloud service providers must assure who, when, and for what purpose data is being utilized. For example, several websites have a security issue with attackers listening to phone conversations, reading emails, and accessing personal data, among other things.
- **Taking the backup of the data**: The cloud service provider should back up the data that is kept in their cloud, but only with the user's consent. That backup data will be useful in the event of a data breach or loss.
- **Access control**: Multi-factor authentication, strong passwords, and automated key rotations should all be used by cloud service providers to safeguard and control access. If these measures are implemented, there will be many fewer instances of unwanted access, and the threat of data theft from cloud data centres will be better managed.
- **Use of firewall**: In spite of the fact that new techniques of safeguarding networks have grown popular in recent years, an efficient firewall is still the best approach for preventing unwanted access. It may be feasible to prevent malevolent hackers from gaining access to the server by taking extra precautions to ensure that the firewall only allows as much access as is required.
- **Password security**: When it comes to cloud server security, the password is the most important component. A common error made by many individuals when setting up a cloud is being careless with passwords. Because the cloud is based on trust, a single compromised password might destroy it.
- **Restricted Access**: Restricted user access entails securing some login forms using basic username/password protection and a challenge-response test. When a user or employee no longer needs access to the cloud data centre, their data centre access credentials must be withdrawn promptly.

Fog computing is now in its infancy, and there is still a long way to go. Because of its distinct characteristics, this computing faces a variety of obstacles. As we all know, it takes advantage of user devices' idle resources, which are not completely reviewed by any standard body, causing security and privacy risks in the fog network. Because multiple devices are involved in fog application processing, safe and quick authentication techniques are required.

Some of the methods proposed are:

- **Authentication plan**: The user's identity can be authenticated by comparing the user credentials to the information stored in the database through an authentication server. This aids in the protection against hostile invasions. If a user is completely authorized in the system, fog computing allows them to access fog nodes from the fog infrastructure.
- **Blockchain Security**: The blockchain idea was created to provide safe transactions in cryptocurrency applications. However, as time went on, everyone realized that the blockchain method was the way to go, with its exceptional security properties, may also be utilized to safeguard computing networks. As a result, the blockchain approach can improve the security of the fog environment.

- **Decoy Technique**: It's a method for verifying a user's data on a network. It substitutes the user's genuine information with a phony version, which is subsequently sent on to the attackers. When a hacker compromises the system's security, it discovers a bogus file in lieu of the real one. The decoy file is the name of this file, and the decoy methodology is the name of the approach. To provide greater security, fake files are produced from the start. The system hides the genuine data, which can only be viewed by authorised users, and replaces it with a decoy file by default for system intruders.
- **Modified Decoy Technique**: It's an improved and updated form of the original decoy strategy, in which attackers are provided fictitious data and system or user nodes to exploit, while the hidden file collects information about their identification, such as their Mac address or IP address.

  Edge computing, as demonstrated in this study, has unique properties, therefore security solutions developed for cloud and fog computing services are ineffective with edge computing. As a result, some proposed solutions that may be implemented using edge computing's unique qualities include [16]:
- **Full-time Monitoring**: To protect computing from bad users or hackers, it's critical to keep a continual check on all edge networks and nodes and to give network awareness to all users through an interactive interface.
- **Cryptographic Techniques**: To cope with security breaches perpetrated by hackers or intruders, cryptographic measures are employed. In these methods, a secret key is employed that is only shared by the sender and the recipient. This secret key is used to decode the message that was received. However, if a thief could gain this secret key from the network's delivered packets, he could also steal the data included in the message.
- **Data Confidentiality**: Several data confidentiality strategies based on encryption techniques have been suggested to address the numerous privacy issues caused by network attackers' illegal data activities, data loss, data manipulation, data breach, and so on. The author of the article [17] suggests Query Guard, a latency-aware query optimization tool, as a privacy-preserving solution. This method fulfils two objectives: first, it handles the problem of privacy-aware distributed query processing, and second, it optimises requests for transmission without delay. When compared to typical query optimization methods, it yields better results in terms of computation time and memory use.
- **Edge Node Security**: Edge node security refers to ensuring that all nodes in the edge network have the same level of security and that suitable safety standards are followed. In the event of varying security levels, a hacker may be able to get past the node with the weakest protection, triggering a system issue [18]. Furthermore, numerous security levels might make it difficult for system administrators to determine which node has inadequate security, allowing a security compromise**.**
- **Proper Encryption**: New state-of-the-art encryption algorithms that are incredibly difficult to decrypt are being employed as modern technology advances. These algorithms use a highly secure secret key that is only shared by the sender and receiver. Only real users have access to this secret key, which allows them to decrypt the file and read the data [19].

- **User Behaviour Profiling**: It is the practice of watching and tracking a user's activity in order to detect any divergence from normal behaviour that might indicate the presence of a malicious user.

6 Conclusion and Future Scope

As a consequence of our research, we've determined that Cloud Fog and Edge Computing is an ever-growing industry, but that as data and devices rise, we'll need to improve our cloud system. Because the entire system of systems is only as safe as its weakest component, network and data security are major concerns that can only be addressed by employing secure hardware and conventional security techniques in the cloud. Machine learning is used in all of these processes to analyse, transform, and categorize data. To date, much of the research in this field has concentrated on the cloud as the execution environment. There is still research that can be done to lower the cloud's latency and bandwidth requirements even more without affecting the system's security. After all of the requirements have been met, the system should be able to operate on its own. For efficient resilience orchestration in modern systems, there is a critical requirement to develop a logical knowledge of the capabilities of nodes and roles, and at the same time, research on security and privacy in this context must be deeply done, since these are vital elements for cloud computing to gain the trust of their users. Finally, after initial configuration of the cloud to meet all of the requirements, it should operate without the need for human intervention. Cloud computing will probably be replaced by fog and edge computing in the future. More research may be done in this sector to improve latency without affecting the user's privacy.

References

1. Alwarafy, A., Al-Thelaya, K.A., Abdallah, M., Schneider, J., Hamdi, M.: A survey on security and privacy issues in edge-computing-assisted Internet of Things. IEEE Internet Things J. **8**, 4004–4022 (2020)
2. Badidi, E., Ragmani, A.: An architecture for QoS-aware fog service provisioning. Procedia Comput. Sci. **170**, 411–418 (2020)
3. Mebrek, A., Merghem-Boulahia, L., Esseghir, M.: Efficient green solution for a balanced energy consumption and delay in the IoT-fog-cloud computing. In: Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017, pp. 1–4
4. Marbukh, V.: Towards Fog Network Utility Maximization (FoNUM) for managing fog computing resources. In: Proceedings of the 2019 IEEE International Conference on Fog Computing (ICFC), Prague, Czech Republic, 24–26 June 2019, pp. 195–200
5. Naha, R.K., Garg, S., Georgakopoulos, D., Jayaraman, P.P., Gao, L., Xiang, Y., Ranjan, R.: Fog computing: survey of trends, architectures, requirements, and research directions. IEEE Access **6**, 47980–48009 (2018)
6. https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/

7. Zeyu, H., Geming, X., Zhaohang, W., Sen, Y.: Survey on edge computing security. In: Proceedings of the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Fuzhou, China, 12–14 June 2020; pp. 96–105
8. Suma, V., Bouhmala, N., Wang, H.: Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020; Springer: Berlin/Heidelberg, Germany (2021)
9. Novak, M., Shirazi, S.N., Hudic, A., Hecht, T., Tauber, M., Hutchison, D., Maksuti, S., Bicaku, A.: Towards resilience metrics for future cloud applications. In: Proceedings of 6th International Conference Cloud Computing. Services Science, vol. 1, pp. 295301 (2016)
10. Mariani, L., Monni, C., Pezze, M., Riganelli, O., Xin, R.: Localizing faults in cloud systems. In: Proceedings of IEEE 11th International Conference Software Testing, Verication Validation (ICST), April 2018, pp. 262273 (2018)
11. Mishra, S., Thakkar, H.K., Mallick, P.K., Tiwari, P., Alamri, A.: A sustainable IoHT based computationally intelligent healthcare monitoring system for lung cancer risk detection. Sustain. Cities Soc. **72**, 103079 (2021)
12. Tripathy, H.K., Mishra, S., Thakkar, H.K., Rai, D.: Care: a collision-aware mobile robot navigation in grid environment using improved breadth first search. Comput. Electr. Eng. **94**, 107327 (2021)
13. Aldossary, S., Allen, W.: Data security, privacy, availability, and integrity in cloud computing: issues and current solutions. Int. J. Adv. Comput. Sci. Appl. (IJACSA), vol. 7, no. 4, pp. 485–498
14. Tripathy, H.K., Mishra, S., Suman, S., Nayyar, A., Sahoo, K.S.: Smart COVID-shield: an IoT driven reliable and automated prototype model for COVID-19 symptoms tracking. Computing 1–22 (2022)
15. Tripathy, H.K., Mallick, P.K., Mishra, S.: Application and evaluation of classification model to detect autistic spectrum disorders in children. Int. J. Comput. Appl. Technol. **65**(4), 368–377 (2021)
16. Rajegore, P.B., Kadam, S.G.: Issues & solution of SAAS model in cloud computing. IOSR J. Comput. Eng. (IOSR-JCE) 40–44
17. Zhang, J., Chen, B., Zhao, Y., Cheng, X., Hu, F.: Data security and privacy-preserving in edge computing paradigm: survey and open issues. IEEE Access **6**, 18209–18237
18. Mishra, S., Tripathy, H.K., Thakkar, H.K., Garg, D., Kotecha, K., Pandya, S.: An explainable intelligence driven query prioritization using balanced decision tree approach for multi-level psychological disorders assessment. Front. Pub. Health 9 (2021)
19. Mishra, S., Tripathy, H.K., Mallick, P.K., Bhoi, A.K., Barsocchi, P.: EAGA-MLP—an enhanced and adaptive hybrid classification model for diabetes diagnosis. Sensors **20**(14), 4036 (2020)