Performance of Data Security and Privacy Requirements in Edge Computing

Rahul Patel, Dr. Lalji Prasad
PhD Scholar, SAGE University, Indore, Professor SAGE University, Indore
rahulpatelcs@gmail.com, lalji.research@gmail.com

Abstract:

We suggests a data aggregation method for security and privacy applications that use edge computing. This method protects the privacy of users while keeping the data's integrity. In our model, there are three different kinds of people who take part: Terminal device Edge computing will move some storage and computing tasks from cloud servers to devices at the edge of the network. This could create a number of security and privacy issues. Edge computing includes both edge servers and public cloud centres. In general, services that deal with people's safety and privacy seem to be the most important ones. During this research project, what part of edge computing will be the main focus of our attention? This study also talks about privacy, but its main focus is on the information security criteria for edge computing. We have also made a system for creating data security at the edge of the network. This system covers encryption as well as privacy, integrity, authorization, and stopping unauthorized users from getting in. The data is made by the terminal devices, which then encrypt it before sending it to the edge server. With the help of the AES algorithm, data can be both encrypted and decrypted. Edge servers are a type of edge device that acts as a gateway or point of entry into a network. The edge server puts together the information from the terminal devices, which it then sends to the public cloud data centre. The user will get a unique key that can be used to decrypt information that was encrypted in the past. With the user's private key, which the cloud service gives the user, the user can decrypt and download the data. Not only does our system make sure that the data on the terminal devices stays private, but it also verifies the source and checks the data's integrity.

Keywords- Data Security, Privacy, Edge Computing, encryption and decryption, cloud computing, edge data centre

DOI Number: 10.14704/nq.2022.20.9.NQ44278 **Neuro Quantology 2022; 20(9):2374-2387**

I INTRODUCTION

Edge computing was made to fix problems caused by cloud technologies. In distributed computing, the edge network is between all of the clouds and the end users. This brings cloud services and end users much closer together (Sayad et.al.2018). As a result, this opens up a lot of new ways to collect real-time data, reduces latency, saves money on operating costs, encourages interoperability, and makes customers happier. The most difficult thing that can go wrong with edge technology is a breach in the security and privacy of almost all of the devices that are connected to it. In this study, eight different ways that a typical edge computing network needs to be safe and secure are looked into. Considerations about privacy and security can be seen as an evaluation of what a programme is able to do and what it can do well in order to close any possible protection and privacy gaps (Zhang et.al. 2018). When all of the conditions are met, the programme will only work well with the top-secret and long-term goals that are needed, as well as the requirements and suggestions of the relevant laws (Roman, 2018). The requirements include secrecy and trustworthiness, as well as the ability to find attacks, be honest, be effective, keep messages honest, and do well. The specifics of each of the conditions will be talked about. But almost all of these earlier works didn't look into the compliance and security needs of edge computing programmes. This is despite the fact that a number of research papers have looked into the security and privacy problems caused by edge computing. Also, the survey results showed that not nearly enough work had been done on modern regulatory approaches, as well as the tools and procedures that go along with them. In the study that looked at privacy concerns in edge devices, even cryptography-based methods that were emphasized were found to be the key to privacy. His team looked into and talked about the flaws in different approaches to edge computing, such as fog and mobile computing, that leave they open to attack. Their results were written up in (Guan et.al. 2019). Even so, the research study saw tactics related to authenticity, so this is still a requirement, even though all of the other qualifications aren't getting much attention. In (Guan et.al.2019), important information about the energy business was talked about, but most of the attention was on security and privacy issues related to the use of new computer technology in the energy market. (Rapuzzi, 2018) also looked at the technological limits of developing fog/edge techniques for cyber-security methods that are already in use. The goal of the survey research was to make a plan for coming up with new ways to deal with cyber-security. But the research also included a thorough analysis of the criteria for developments in technical approaches, (4) measures used to measure the effectiveness of interventions, (5) the categorization of threats on the edge device and the related technical pattern used to stop attackers, and (6) research directions for future professionals in the field of privacy and security for edge devices.

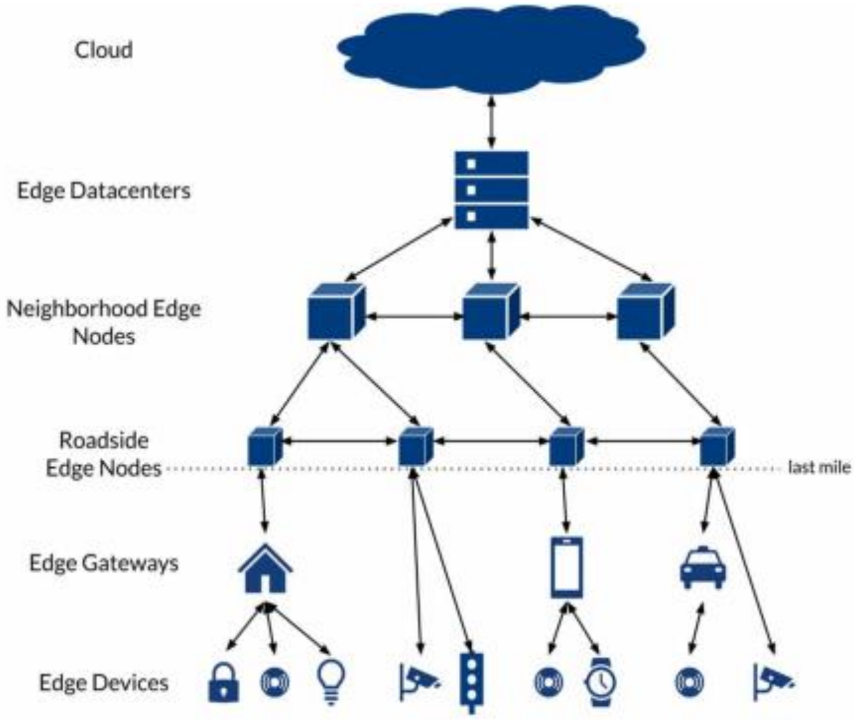


Figure 1. Edge Computing Architecture

In Edge Computing, there was not enough protection for data security and privacy requirements. (Xiao et.al. 2019) showed that it was important to design and study essential security strategies to reduce the number of security holes in the constantly changing field of edge/fog technology in a number of different computing frameworks. In. was the one who did this other study. Several academics who took part in the study said that there is a solid basis for recognizing privacy problems in edge devices. But some of these papers only gave the most general information about how the edge computing programme needs to be safe and private. Also, when problems came up in the early stages of the research, a big part of it was either partially worked on or checked. This piece of analytical work would include not only the current state-of-the-art privacy and security rules, but also the pattern of the technical techniques chosen by ways to reduce the connected risks to future investigations in edge computing that are to be explored. Before the next data preparation phase starts, a systematic analysis framework that outlines all the right steps needed to reach the survey's goals and objectives would be set up and re-recognized in the initiation phase. This would happen before the next phase of getting the data ready. By using this method, it would be easier to make accurate analyses and remember the facts. To meet the needs of this research study, your answers to the research questions and goals should meet the following conditions:

Security and Privacy Issues on Edge Computing - Edge computing will move some storage and computing tasks that are currently done on cloud servers to devices that are closer to the source of the data. This could mean that there will be more security and privacy rules to follow. Concerns about security and privacy seem to be the most important when it comes to edge computing (Donald et.al. 2016). Because of this, we will put them at the top of our list throughout this whole study. This article talks about the security requirements for edge computing and the risks it faces. We have also made a system for creating data security at the edge of the network. This system covers encryption as well as privacy, integrity, authorization, and stopping unauthorized users from getting in.

Requirements of Security And Privacy- If either cloud storage or edge computing is used, the authorised body's information will have to be given directly or indirectly to private entities, or the property will be split between them. This could also lead to the loss of data, security breaches, unauthorized data activities, and other problems with privacy, and it might not be possible to guarantee the integrity and anonymity of data. Because of this, protecting data that is spread out is still the most important thing when it comes to information security in edge computing (Caprolu et.al. 2019). To improve the safety of edge computing, the following criteria should be taken into account.

Confidentiality: It is a basic requirement that must be met. It gives specific data owners and operators access to personal data just at the edges of computers. When sensitive information is shared and retrieved by clients, most of the time in edge or central data centres, and kept or stopped in the same way at the edges or cloud service, it keeps unwanted users from getting access to the material. Even if the data hasn't been changed without the authors' knowledge, there needs to be consistency to make sure the authors get the right information. Integrity means that the data hasn't been changed by someone who shouldn't have been able to. Because there aren't any of the usual authentication steps, it's possible that sensitive information could be at risk of being stolen.

Accessibility: Because edge computing is so mobile, almost all users who have been given permission can access the edge and storage resources from anywhere to meet customer needs, no matter where they are physically located. Then, it makes sure that any user information kept by an edge or cloud storage provider in an encrypted format can be evaluated using a number of performance standards. Because authorization guarantees that the user's identity won't be called into question, authentication must be a way to prove the user's identity in order to be valid.

Access Control: Through the control laws, access management is also a way to make sure that both security and privacy are taken care of. It says who can access the information and what kinds of skills, like reading and writing, those who can access it can use. Access management is an important part of access management, so these laws are in place. The need for personal space with the security measures, opponents who are honest but suspicious can be sure that almost all of the consumer distribution data, such as data, personal identity, and location, is kept secret. Edge computing can also protect customer privacy, either directly or indirectly, through data security solutions like specific encoding, dependability internal audit, authorization, and unauthorized access.

Challenges in Data Security and Issues

Edge computing uses some of the new technology, like data transfer, cloud computing, and privatization, to bring computation close to datasets. In this case, the basic criteria for protecting consumers in the sector, economy, and real activities have been data protection and privacy preservation. In addition, in developing edge computing systems, we have to accept that protection and security will be mentioned in each and every level. In this section we illustrate the possible security and privacy concerns centered on the architecture of edge computing as shown in Figure 1. A description of the identification of data protection and privacy issues is shown in Table 1.

Table 1 identification of data protection and privacy issues

Core Infrastructure	Edge Servers	Edge Network	Edge Devices
Privacy Leakage Data Tampering Denial of Service	Privacy leakage Denial of Service Access Control Authorization	Denial of Service Man-in-the-Middle attack	Injection in information Service manipulation

II RELATED WORK

Edge computing is a strategy that moves processing closer to the datasets themselves by using newer technologies like data transit, cloud computing, and privatization. Near-data processing is another name for what edge computing is. In this case, keeping data safe and respecting people's right to privacy were the most important things to do to protect customers in business, the economy, and real-life activities. This has happened because these are the two most important things an individual can control. Also, when building systems for edge computing, we have to accept the fact that protection and security issues will be dealt with at every step of the way. We have to accept this. In this section, we'll talk about the possible safety and privacy problems that could come up because of how edge computing is built (see Figure 1). Because edge computing is set up the way it is, these problems are likely to happen. In Table 1, you can read about the process that was used to find problems with data protection and privacy. Communication overheads between a customer and a server site are reduced due to a decrease in actual transmission distances (in terms of geography and number of hops) brought about by the Edge computing in the network. As one of the definitions, "Edge computing is a networking philosophy focused on bringing computing as close to the source of data as possible to reduce latency and bandwidth use. In simpler terms, Edge computing means running fewer processes in the Cloud and moving those processes to local places, such as on a user's computer, an IoT device, or an Edge server" [Gezer. V.Um et.al. 2017]. Some other definitions of Edge computing are "a physical compute infrastructure positioned on the spectrum between the device and the hyper-scale Cloud, supporting various applications. Edge computing brings processing capabilities closer to the end-user/device/source of data which eliminates the journey to the Cloud data center and reduces latency" [Mäkitalo, N 2020].

There are many times when architectural designs are made with a specific goal in mind, taking into account how they will be used and setting up the infrastructure to meet their needs. Edge computing is a new way of doing things that is considered to be on the cutting edge of technology. It moves services and applications that have been centralized in the cloud to places that are closer to where the data comes from. The data is then processed at these places, which have the computer power to do so. It also has extra connections for connecting the Cloud to the devices that end users use. Make sure that the number of Edge nodes increases in a certain place. This will not only lower the number of devices assigned to a single Cloud, but it will also be one of the best ways to fix or lessen problems with cloud computing [Sarkar, S.Misra 2016].

Edge services are mostly used by devices with limited resources, like wearables, tracker bands for fitness and medical applications, and smartphones [Mukherjee et.al. M 2017].Fog devices, on the other hand, make up for the problems with the Cloud by moving some of the Cloud's core functions to the network's edge, where they can still be used in a way that is similar to how the Cloud works .For example, Edge and Fog nodes can connect these devices to the Cloud [Ometov, A. et.al.2016].

In a typical design for Edge computing, there are three main nodes: the Cloud, the local Edge, and the Edge Device .Notably, Local Edge has a well-defined structure with many sub layers of different Edge servers and a processing power flow that goes from the bottom to the top. Edge servers are located at what is thought to be the lowest sublayer, which is also where proximity-based communications happen.Access Points (APs) and Base Stations (BSs) are also thought to be in this group. These are used to get data from different Edge devices while they are talking to each other. They do this by using a variety of wireless interfaces to return a control flow. When they get data from Edge devices, cellular base stations (BSs) send it to the Edge servers in the (upper) sublayer. In this case, the work being done on the computer is very important to the higher sublayer. After the BSs send the data, the most basic forms of analysis and computation are done. At a more modern Edge server, the computational limit has been set up so that if a piece of work is more complicated than it, it will be taken off the server and sent to a higher sublayer that has enough computing power. After that, these servers bring the flow control chain to an end by giving control back to the access points, which then sends them to Edge devices [Kozyrev D et.al. 2018].

Based on the fact that the paradigm [Jiang,C. Cheng et.al. 2019] is driven by proximity, the Edge architecture made it possible to move applications that couldn't wait close to the places where computation was needed. Some examples of these uses are augmented, virtual, and mixed reality (AR/VR/MR) gaming, cellular offloading, and other similar uses.

In general, there are two ways to look at the distance between the Edge and the user's equipment: the physical distance and the logical distance. The term "physical proximity" refers to the exact distance between the part of the data computation that is at the top and the equipment used by the user. Logical proximity is the number of hops that must be made between the Edge computing segment and the users' devices. Due to the long path created by multiple hops, there is a chance that there will be congestion, which will lead to higher latency issues.

Logical closeness needs to limit the number of times these kinds of things happen at the back-haul of computer network systems to stop queuing, which can slow things down. Even though normal Cloud paradigm innovations haven't been able to keep up with growing needs, the Edge paradigm is not seen as a good replacement for the Cloud paradigm because it uses less energy, can work in real time, and has security and privacy issues. Everyone knows that the Edge and Cloud paradigms can work together to help solve different kinds of problems. In some network areas, like smart cities, offices, and homes, as well as in self-driving cars and the industrial Internet, the Cloud and Edge paradigms work together. Importantly, when Edge and Cloud paradigms work together, there are many ways to reduce latency in robust software like self-driving cars, organisations' network assets, and information analysis on the Internet of Things [Dolui, K. et.al.2017]. Even so, the Edge activity is done with the help of capabilities from a number of different actors. There are many ways to connect endpoint devices and nodes of the Edge computing layer. These include cellular LTE, short-range Bluetooth Low Energy (BLE), Zigbee, and Wi-Fi. Access modalities are very important because they determine the bandwidth of the endpoint equipment, the scope of the connection, and the types of devices that can get help [Chinnasamy et.al.2019].

III PROPOSED SYSTEM

In our proposed system we are going to implement the privacy protection for the data. Here we use AES algorithm to Encrypt and decrypt the data. Before string into the cloud data are met to the edge server which is going to act as intermediate between the cloud and the uploading file. Data will be stored after getting acknowledgment from the edge server and cloud. A key will be generating form the cloud to encrypt and decrypt the files. Because of this, the trust-aware monitor that was shown can effectively reduce the stress on users and make the system more reliable. A service provider's monitoring of data and commitment to QoS are not always the same. Our trust mechanism will make the service provider less trustworthy. This method is also good for service-oriented cloud computing, like Scientific Computing as a Service, because it uses a number of important service indicators in its direct trust assessment.

Neuro Quantology | September 2022 | Volume 20 | Issue 9 | Page 2374-2387 | doi: 10.14704/nq.2022.20.9.NQ44278
Rahul Patel, Dr. Lalji Prasad/Performance of Data Security and Privacy Requirements in Edge Computing

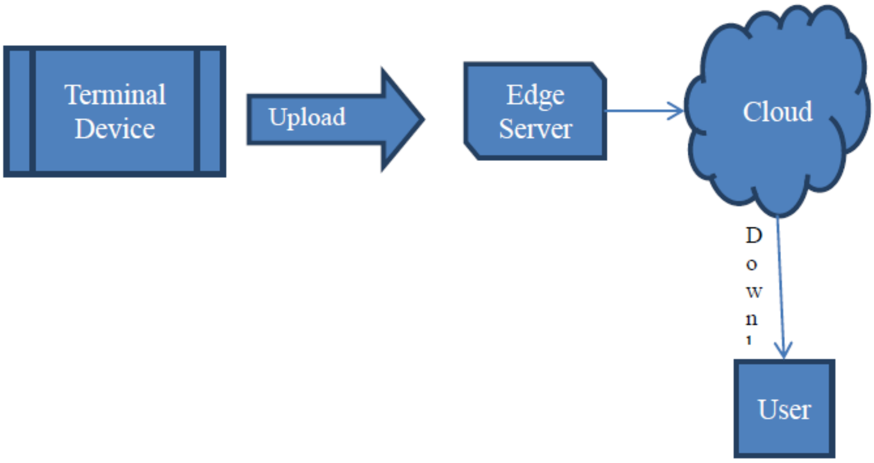


Figure.2 System Architecture

AES Encryption -Figure 3 shows the framework that the AES uses to encrypt and decrypt data. for a scenario in which the encryption key is 128 bits long. (As was already said, if the key has 192 bits, there are 12 circles, and if it has 256 bits, there are 14 circles.) Before starting circle-based encryption, you must first use an XOR operation on the sequence that will be used in the first four words of the key scheme. When decrypting, the same thing happens, except that we now XOR the setting of the cipher text state with the last four words of the key. [Chinnasamy P. et.al. 2018] During the Add Round Key step, the key is added to the state array. This makes the cipher safer. During each round, a sub key is made from the expansion of the main key. The end result of the encryption process is an expanded key that is 176 bytes long and is organized as a linear array of 44 words (using a key length of 128-bit). After the word array has been set up ($W[i]$ for $0 \leq i \leq 43$),the remaining words are made by applying the following relation to the results of putting the key into the first four words of the array[Ghobaei-Arani, M.2020].

$$W[i] = W[i-1] \oplus W[i-4]. \qquad \textbf{(Eq.1)}$$

A particular exception is made for the words with index multiple of four, for which, non-linear relationships, different from bit-to-bit XOR are used:

$$\textbf{Subword (Rotword(w[i} - \textbf{1])))} \oplus \textbf{Rcon[i/4],} \quad \textbf{(Eq.2)}$$

where the Subword sub-function replaces each byte of the word, provided as argument of the function, using the Sbox, whereas the Rot word sub-function simply shifts one byte to left; furthermore, the function Rcon[i] is a round constant, represented by the word array

$$x^{i-1}, \{00\}, \{00\}, \{00\} \text{ , where } x^{i-1} \text{ is the } (i-1)\text{-th } \textbf{(Eq.3)}$$

Exponentiation operator in GF(2^8).Both encrypting and decrypting use different methods, but each step in the encrypting process has a corresponding step in the decrypting process. This makes sure that both processes can read and understand the data. Even so, both are made up of ten rounds, and the step of adding the round key is done the same way in both. So, each iteration of the decryption process is made up of the following steps:

- Inverse Sub Bytes
- Inverse Shift Rows
- Inverse Mix Columns
- Add Round Key

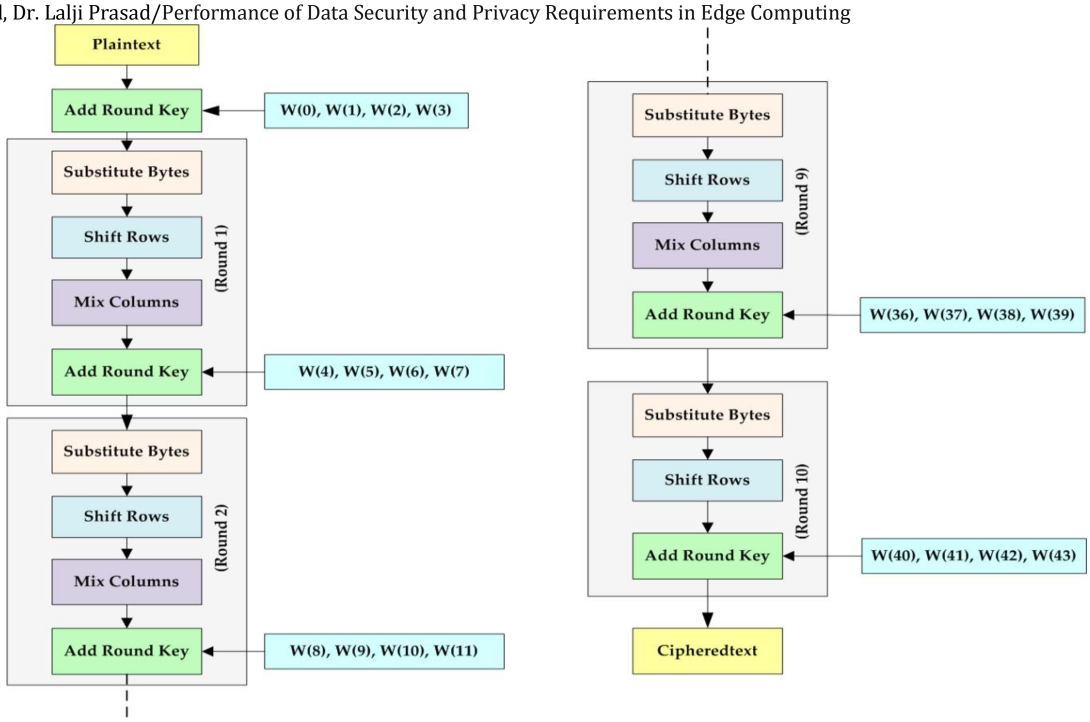
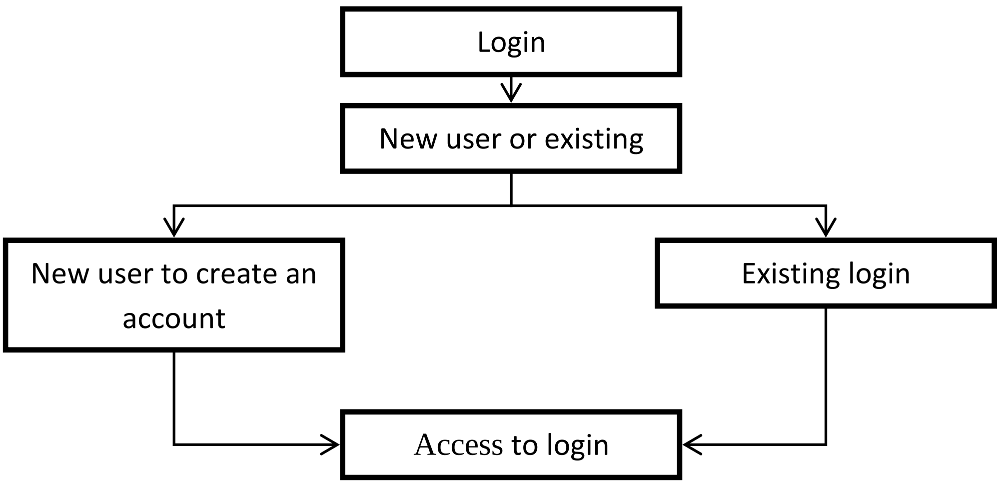


Figure 3 framework of AES

Another difference between the encryption and decryption processes is the order in which tasks are done during a single round. The first step in decryption is called "Inverse Shift Rows." This is followed by "Inverse Sub Bytes," "Add Round Key," and "Inverse Mix Columns." The first step in the encryption process is called "Shift Rows." In particular, the Inverse Move Rows will move to the right in a cycle by the same amount as the Shift Rows step, but in the opposite direction. In the step called "Inverse Mix Columns," the right inverse matrix is used to do the work of turning the Mix Column operation around. The 4-byte columns of the state array are multiplied for the inverse 4 × 4 matrix featured by constant entries for producing the output bytes; all operations involved in the matrix multiplication are performed in GF 2^8 or equivalently by multiplying each column, modulo $z^4 + 1$,with a fixed polynomial $b(z) = 0Bz^3 + 0Dz^2 + 09z + 0E$, where $b(z) = c(z)^{-1} \bmod z^4 + 1$ and $c(z)$ is the polynomial used in the Mix Columns step of the encryption.



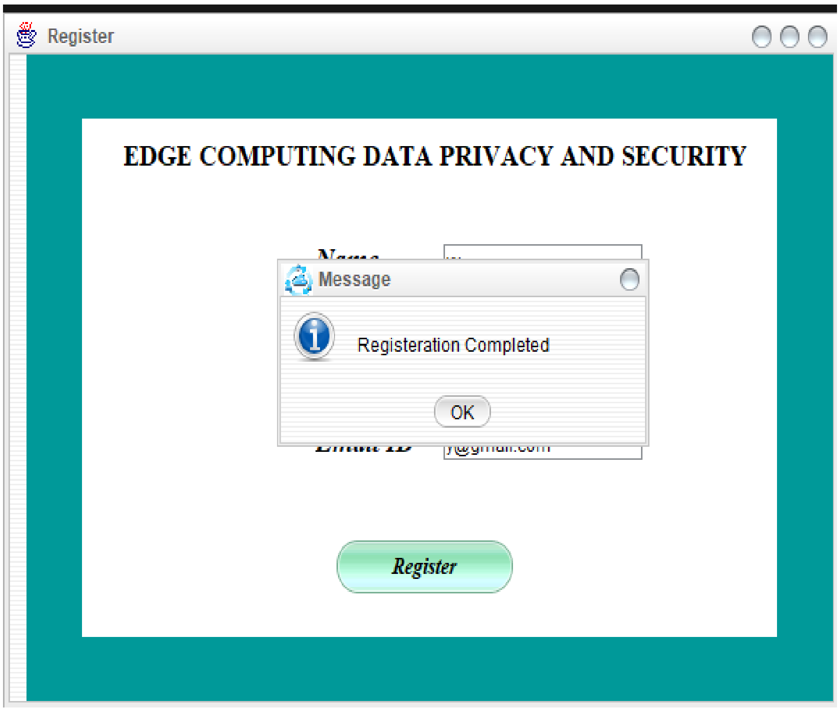


Figure 4 User Registration

It is the act of signing up for the cloud or being signed up for the cloud. Each Data Owner and Data User needs to sign up in order to use the cloud documents. During this process, basic information about you, like your email address and list of contacts, will be collected and stored in the cloud. When a user signs up for the cloud service, a cloud id will be made for them right away and automatically.

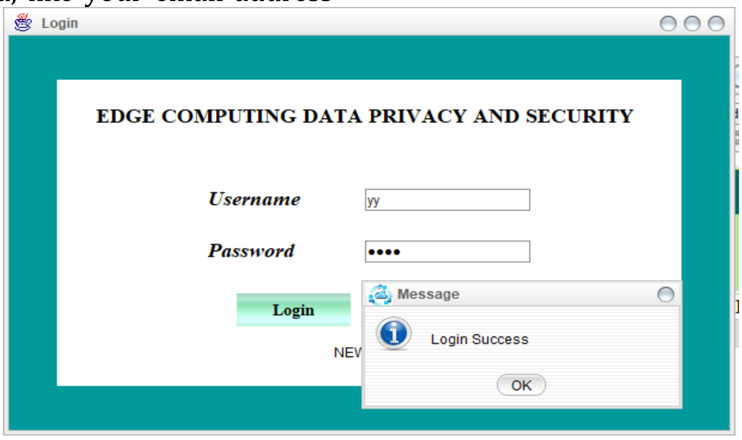
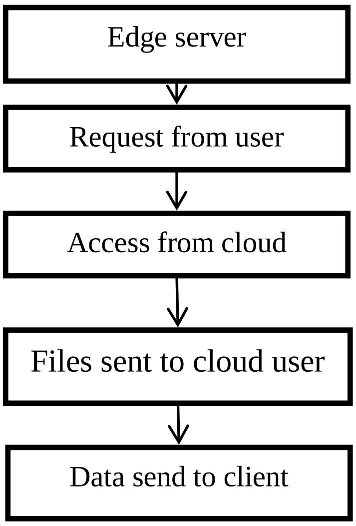


Figure 5 User Login

Module Description – Authentication Users can set up a new cloud storage account by using the login module. If the user already has a login and password for an account, they can use those to upload or download files from a reliable cloud storage service. In that case, they must sign up with their email address and make up their own password.

Edge Server- Within the context of this module, the user can choose where in the cloud to store the data that goes with a certain secret key. The user is then asked by the edge server to save the data on the server using a certain access. After that, the data can be saved, and at a later time, they can be downloaded from different clouds on a set schedule.



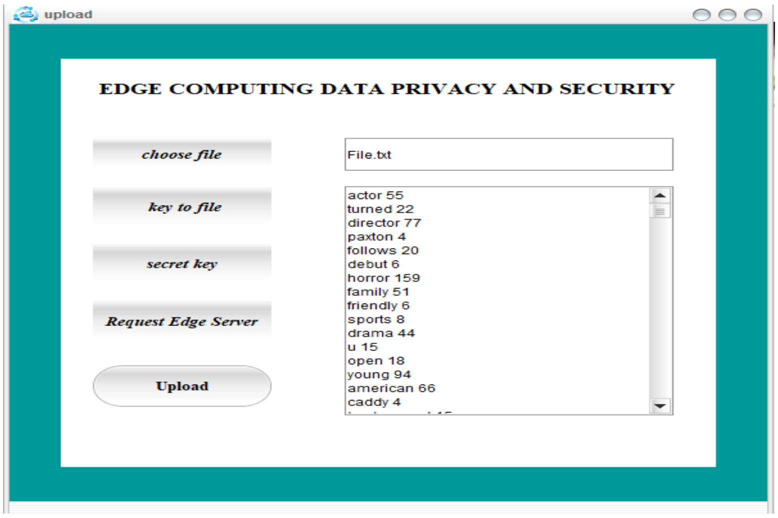
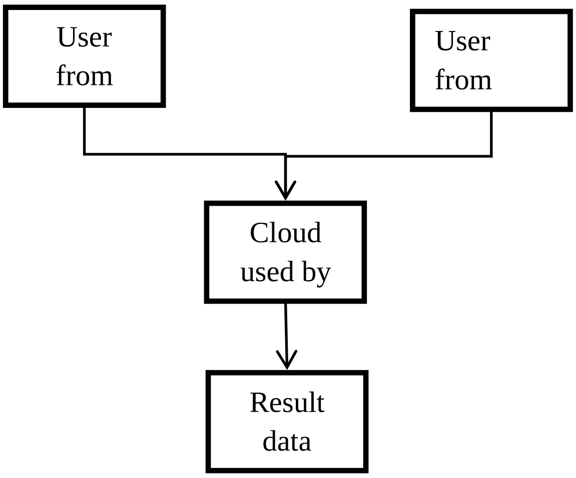


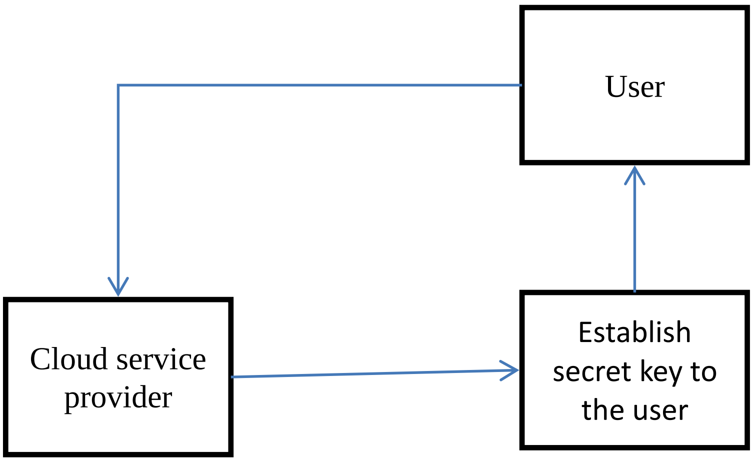
Figure 6 Data Upload

Cloud server Module: In the cloud server module the user can request from the provider to download or upload the data to the client. The user can download the data from any cloud using a cloud server access with a certain file key in it. The cloud server can grant the access to download the file from the cloud.



Key Generation

In this module a key will be generated to upload and download the file. This key will be provided for the security purpose. A key will be provided for the both file and the user



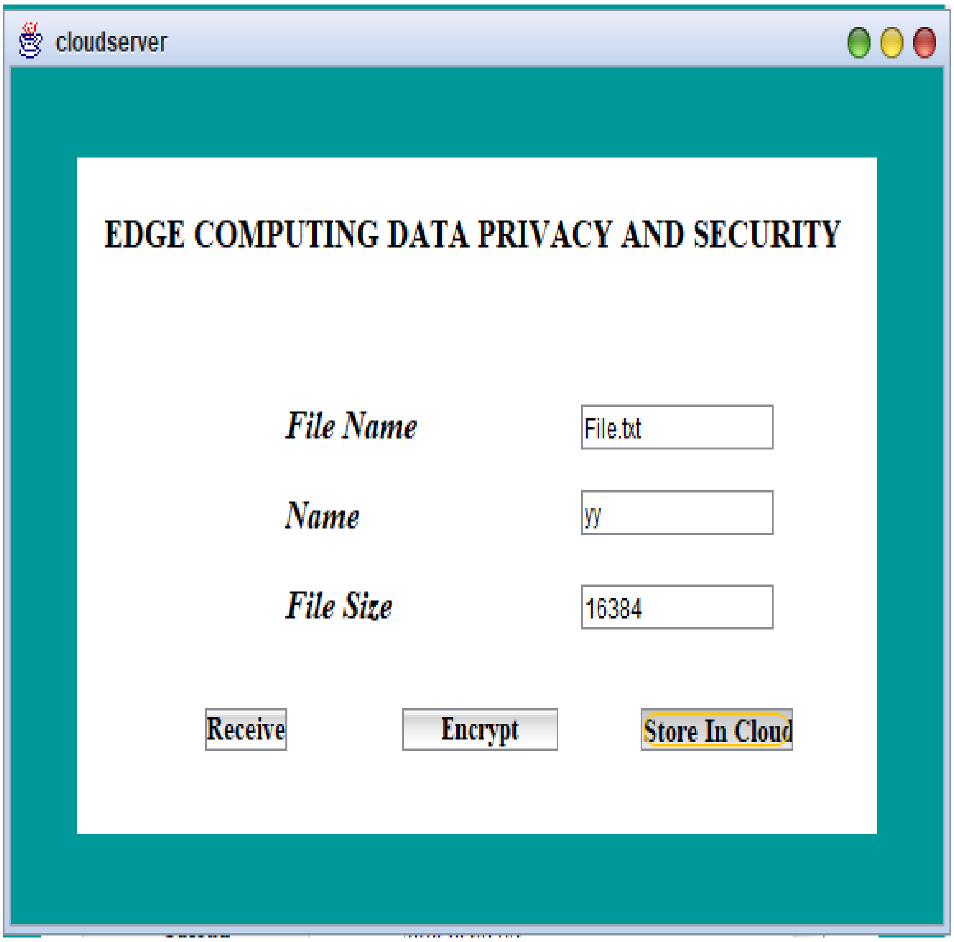


Figure 7 Data Store On Server

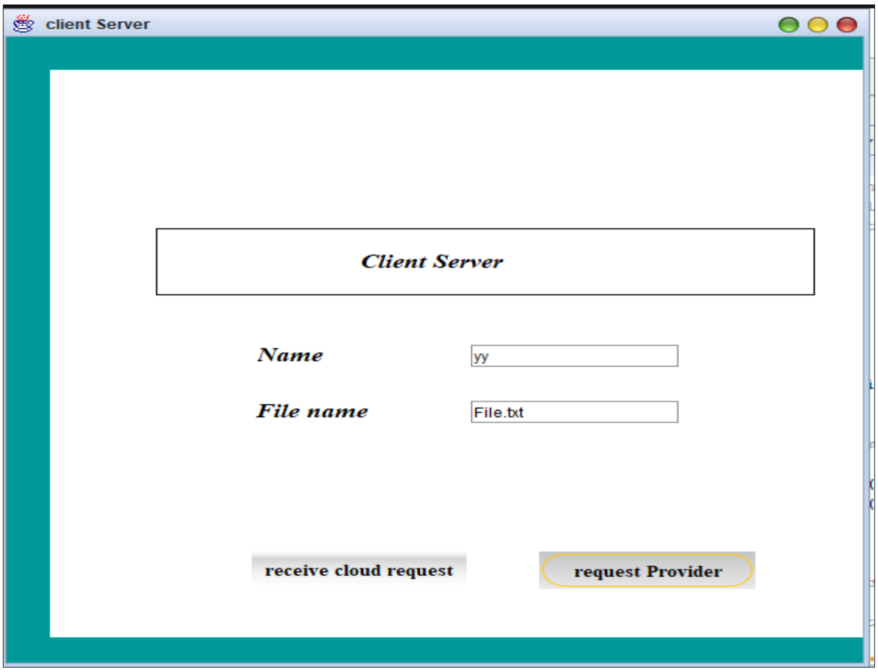


Figure 8 Client Request for Data

A pooled, centralized server resource that is hosted and delivered over a network typically the Internet and accessed on demand by multiple users

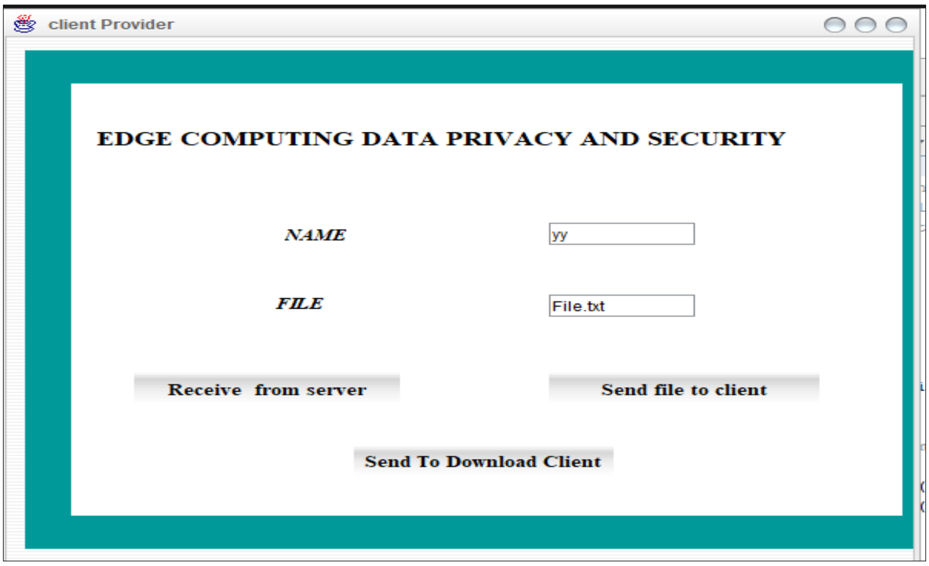
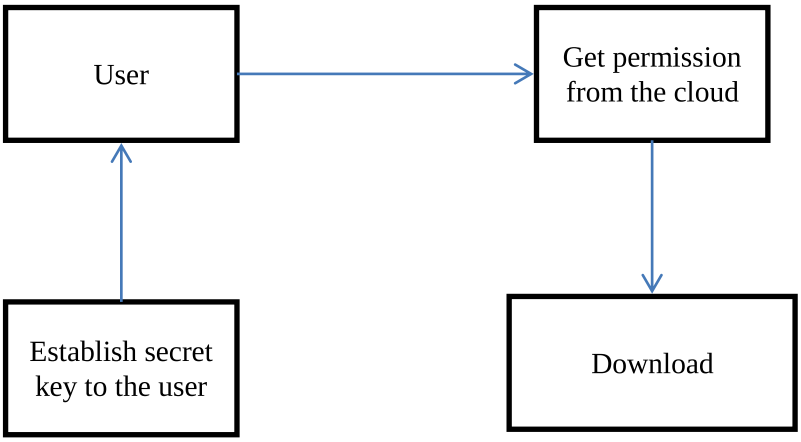


Figure 9 User Authentication

For storing data in the cloud that provides servers and applications access to data through shared file systems.

Download-In this transmission module the data can be transmitted to the different users related to the key provide during the upload of file by the users. The same key can be used by the related user's login to download the data from the cloud. The verification can be done during download of file from the cloud by the related users in it



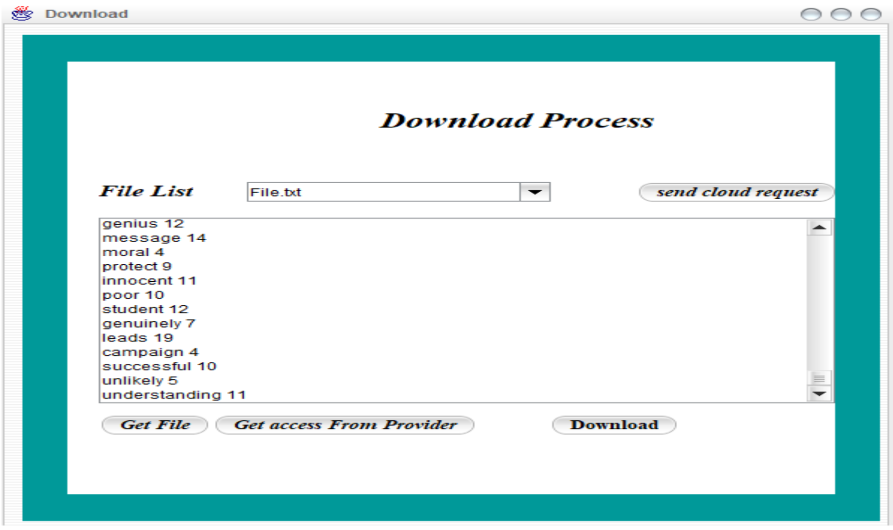


Figure 10 Data Download

Servers (compute resources) that run the processing at an edge location, Cloud Storage for Firebase allows you to quickly and easily download files from a Cloud Storage bucket provided and managed by Firebase.

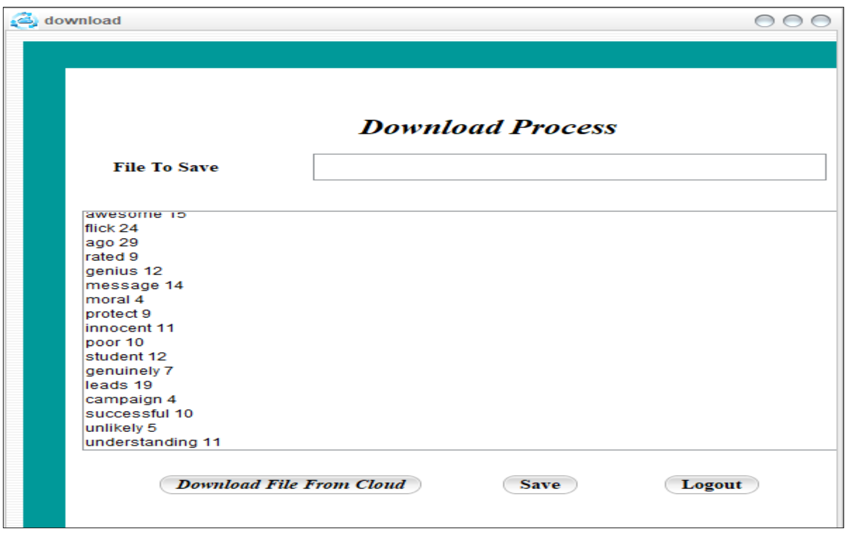


Figure 11 Data Download From Server

IV CONCLUSION

In our system, we have set up the aggregation of data for different security applications that benefit from edge computing in a way that protects privacy. This not only cuts down on the communication costs of the whole system, but it also keeps the terminal devices' privacy. The proposed system can protect the privacy of users while also authenticating the source and keeping the data's integrity. The small amount of work that has been done has mostly been focused on making a reliable feedback system for environments with more than one cloud. Depending on the different trust management conditions, the window could be made shorter or longer. The goal of this feedback system is to make the trust system more reliable. It is set up in a hierarchical structure. Low levels of both latency and bandwidth use are the most important benefits of using edge servers. With edge computing systems, this article looks into and describes threats to data security and privacy, as well as defences that protect privacy. In the beginning, we talk about what edge computing is and how it differs from cloud computing. We also talk about the limitations of cloud technology, the coming age of security applications, and the shift from user to consumer. After that, we talk about the concept, architectures, and a few important edge computing applications. Next, we'll look at the security risks to data protection and privacy, as well as the security measures that are actually possible. The user will be able to use both encryption and decryption. Also, cryptographic approaches are talked about as possible ways to solve problems with data protection and privacy.

REFERENCE

1. El-Sayed, Sankar, Prasad, Puthal, Gupta, Mohanty, & Lin. (2018). Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. IEEE Access, 6, 1706-1717.
2. Zhang, Chen, Zhao, Cheng, & Hu. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE Access, 6, 18209-18237.
3. Roman, Lopez, & Mambo. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Gener. Comput. Syst., 78, 680-698.
4. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge Computing Security: State of the Art and Challenges. Proc. IEEE 2019, 107, 1608–1631.
5. Guan, Zhang, Si, Zhou, Wu, Mumtaz, & Rodriguez. (2019). ECOSECURITY: Tackling challenges related to data exchange and security: An edge-computingenabled secure and efficient data exchange architecture for the energy Internet. IEEE Consum. Electron. Mag., 8(2), 61-65.
6. Rapuzzi & Repetto. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Gener. Comput. Syst., 85, 235-249.
7. Donald, A. C., & Arockiam, L. (2016). Key Based Mutual Authentication (KBMA) Mechanism for Secured Access in MobiCloud Environment. In MATEC Web of Conferences (Vol. 40, p. 09002). EDP Sciences.
8. Caprolu, D. P., Lombardi, & Raponi. (2019). Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues. 2019 IEEE International Conference on Edge Computing (EDGE), 116-123. doi: 10.1109/EDGE.2019.00035
9. Gezer, V,Um, J., Ruskowski, M. An Extensible Edge Computing Architecture: Definition, Requirements and Enablers. In Proceedings of the UBICOMM, Barcelona, Spain, 12–16 November 2017.
10. Mäkitalo, N.; Flores-Martin, D.; Berrocal, J.; Garcia-Alonso, J.; Ihantola, P.; Ometov, A.; Murillo, J.M.; Mikkonen, T. The Internet of Bodies Needs a Human Data Model. IEEE Internet Comput. 2020, 24, 28–37.
11. Sarkar, S.; Misra, S. Theoretical Modelling of Fog Computing: A Green Computing Paradigm to Support IoT Applications. IET Netw. 2016, 5, 23–29. [CrossRef]
12. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. IEEE Access 2017, 5, 19293–19304.
13. Ometov, A.; Olshannikova, E.; Masek, P.; Olsson, T.; Hosek, J.; Andreev, S.; Koucheryavy, Y. Dynamic Trust Associations over Socially-Aware D2D Technology: A

Practical Implementation Perspective. IEEE Access 2016, 4, 7692–7702

14. Kozyrev, D.; Ometov, A.; Moltchanov, D.; Rykov, V.; Efrosinin, D.; Milovanova, T.; Andreev, S.; Koucheryavy, Y. Mobility-Centric Analysis of Communication Offloading for Heterogeneous Internet of Things Devices. Wirel. Commun. Mob. Comput. 2018, 2018, 3761075.
15. Jiang, C.; Cheng, X.; Gao, H.; Zhou, X.; Wan, J. Toward Computation Offloading in Edge Computing: A Survey. IEEE Access 2019, 7, 131543–131558.
16. Dolui, K.; Datta, S.K. Comparison of Edge Computing Implementations: Fog Computing, Cloudlet and Mobile Edge Computing. In Proceedings of the Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6
17. Chinnasamy, Deepalakshmi, & Praveena, Rajakumari, & Hamsagayathri. (2019). Blockchain Technology: A Step Towards Sustainable Development. International Journal of Innovative Technology and Exploring Engineering, 9(S2).
18. Chinnasamy, P., & Deepalakshmi, P. (2018a). A scalable multilabel-based access control as a service for the cloud (SMBACaaS). Transactions on Emerging Telecommunications Technologies, 29(8), e3458. doi:10.1002/ett.3458
19. Chinnasamy & Deepalakshmi. (2018b). A Survey on Enhancing Cloud Security through Access Control Models and Technologies. International Journal on Computer Science and Engineering, 9(5), 326–331.
20. Ghobaei-Arani, M., Souri, A., & Rahmanian, A. A. (2020). Resource Management Approaches in Fog Computing: A Comprehensive Review. Journal of Grid Computing, 18(1), 1–42. doi:10.100710723-019-09491-1