Cloud and Fog Computing Amalgamation for Data Agitation and Guard Intensification in Health Care Applications

L. Arulmozhiselvan[1*] and E. Uma[2]
[1]Assistant Professor, Meenakshi Sundararajan Engineering College, Chennai.
[2]Assistant Professor (SL.Gr), Anna University, Department of Information Science and Technology, Chennai.
[E-mail: arulmozhiselvan@auist.net[1] , umaramesh@auist.net [2]]
[*]Corresponding author : arulmozhiselvan@auist.net

Received August 11, 2022; revised April 8, 2023; revised September 28, 2023; accepted February 9, 2024; published March 31, 2024

Abstract

Cloud computing provides each consumer with a large-scale computing tool. Different Cyber Attacks can potentially target cloud computing systems, as most cloud computing systems offer services to many people who are not known to be trustworthy. Therefore, to protect that Virtual Machine from threats, a cloud computing system must incorporate some security monitoring framework. There is a tradeoff between the security level of the security system and the performance of the system in this scenario. If strong security is needed, then the service of stronger security using more rules or patterns **is** provided, since it needs much more computing resources. A new way of security system is introduced in this work in cloud environments to the VM on account of resources allocated to customers are ease. The main spike of Fog computing is part of the cloud server's work in the ongoing study tells the step-by-step cloud server to change the tremendous measurement of information because the endeavor apps are relocated to the cloud to keep the framework cost. The cloud server is devouring and changing a huge measure of information step by step to reduce complications. The Medical Data Health-Care (MDHC) records are stored in Cloud datacenters and Fog layer based on the guard intensity and the key is provoked for ingress the file. The monitoring center sustains the Activity Log, Risk Table, and Health Records. Cloud computing and Fog computing were combined in this paper to review data movement and safe information about MDHC.

Keywords: Cloud Computing, Fog Computing, Encryption, Virtual Machine, Security

http://doi.org/10.3837/tiis.2024.03.009 **ISSN : 1976-7277**

1. Introduction

Cloud computing is a form of computing that focuses not only on the application management of dedicated servers or smart devices but also on machine learning resources. Depending on the physical location of the computer resources and who can access those resources, cloud computing can be divided into public, private, and hybrid cloud [1]. Usually, services from the cloud are implemented based on the requirements of the end user. SaaS offers remote software access and its web service-based functionality. PaaS is another service that is supplied as a system. There, instead of a company or data center, the device is subcontracted to buy and maintain its own hardware and software layers [2]. IaaS is popular with businesses that enjoy the flexibility of getting their IT infrastructure handled by the cloud vendor. Cloud computing provides a lot of opportunities to the company. With the increasing number of cloud-enabled devices used in modern business settings (e.g. smartphones and tablets), it is even easier to access data [3].

Cloud computing security pertains to a wide variety of initiatives, innovations, applications, and regulations to protect the IP, data, applications, facilities, and related infrastructure of virtualized cloud computing. Implementation of cloud security relies on cloud service or existing cloud-based security solutions [4]. The implementation of the cloud defense system ought to be a joint responsibility between the owner of a business and the solutions provider. To businesses making the shift to the cloud, reliable cloud protection is a must. Security risks evolve and become more sophisticated and there is no less threat to cloud computing than an on-site economy. It is therefore essential to work with a cloud provider that offers a better-in-class safety optimized for services [5].

The Virtual Machine is a computer emulation or reproduction. A Virtual Machine uses Virtualization Software to run on a device. Virtualization and the cloud are both using abstract resources to create useful environments [6]. Virtualization, however, is a technology that enables multiple virtual environments or committed resources to be created from a single specific hardware system and clouds are IT areas that abstract, pool and start sharing scalable resources across a system. Clouds provide the advantages of self-service control, distributed network scaling, and flexible resource pools that differentiate them most distinctly from conventional virtualization [7]. The **Fig. 1** shows the general cloud and fog-based IoT environment.

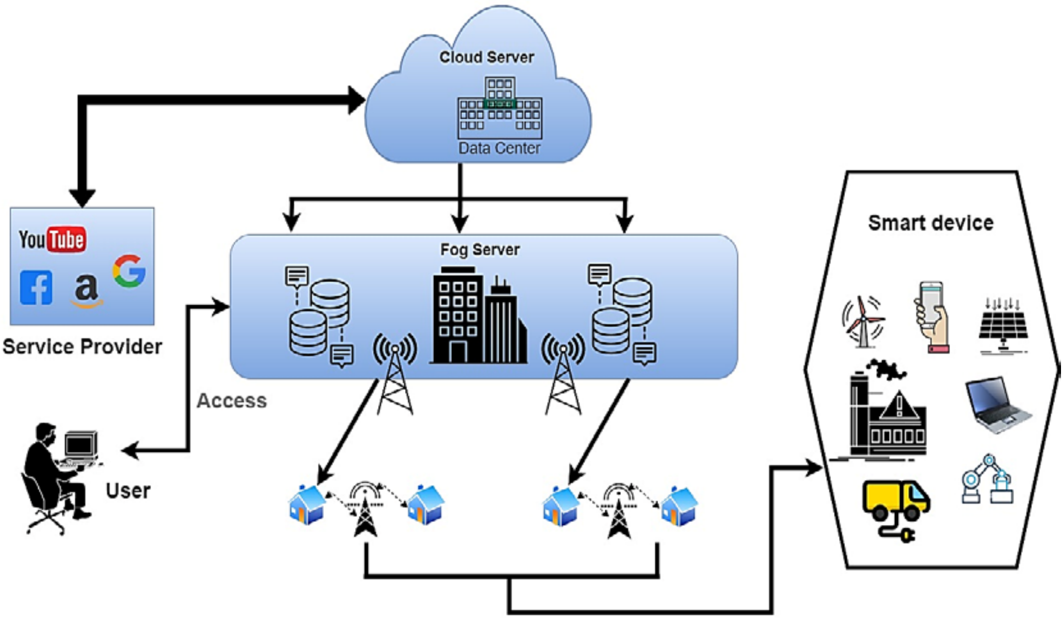

Fig. 1. General cloud and fog-based IoT environment

In 2020, there will be about 30 billion IoT devices globally, and by 2025, based on the most recent Statista, the figure will reach 75 billion linked items [8]. All of these tools can generate vast amounts of data that must be interpreted efficiently and responsibly. Fog computing rises into operation in conjunction with cloud computing to meet the growing demand for IoT solutions [9]. The Internet of Things incorporation with the cloud is a value-effective business practice [10]. Off-premise networks include the requisite interoperability and versatility to handle and analyze data collected from devices connected, while specialized platforms provide creators with the ability to create IoT applications without significant hardware and software resources [11].

Therefore, in this paper, a scheme is proposed that could be improved by a specific discussion of security solutions. Data security is addressed in personal computers and information analysis in the cloud with the security aspects relevant to it [12].

The contributions of this research are as follows.

1. The proposed framework focuses on the amalgamation of fog computing and cloud computing to provide a secure data exchange for healthcare applications.
2. A new model of encryption against attacks is implemented through a secure Attribute-Based Encryption (ABE) technique for reliable data exchange in healthcare units. Here the actual data received from a fog node is segmented and sent to several cloud servers, where the segmented data is encrypted and stored with different sets of secret keys. During decryption, the right set of keys will decrypt the corresponding segmented data. The decrypted segmented data are combined to get the actual data.
3. The proposed encryption technique provides security from attacks such as brute force, where the attacker does an exhaustive search of 2^m to find the key (m is the length of the key). However, in the proposed model, the attacker has to perform $n \times 2^m$ searches since the key is segmented into n subkeys for the n cloud servers. If the length of the sub keys is large, it becomes a very tedious process to get the correct subkey from the search. In

addition to this, the combinations of the sub keys must also match to get the data. Hence, the level of security is increased to a large extent through the proposed model.

As discussed earlier, this works it distinguishes from other recent security methods. It gives the detail as broad as earlier works.

2. Literature Review

The execution of previously created Intrusion Detection/Prevention Systems (ID/PS) in cloud computing can't deliver the ideal degree of well-being and productivity as cloud computing plan engineering is particular from customary registering strategies, for example, framework processing. The extending supply assets of the cloud from its clients demands the requirement of some ideal framework for guaranteeing asset prerequisites as interlopers can collaborate cloud assets and damage the data put away thereby clients.

Kunal et al. [13] detailed that the fog figuring idea looks to modify the situations given by cloud computing conditions, as well as to decentralize and limit information-driven fogs. As a rule, fog gadgets convey just specific data that is routinely utilized in them, and the amount of the information in a fog gadget is generally minimal in contrast with a cloud server. Fog just keeps up with information that is regularly gotten to by clients; the rest is acquired from the actual cloud. The target of entering this calling is to make the information stream in numerous areas consistent and inconvenience-free. Fog registering can be considered a mediator among shoppers and the cloud server, interfacing with end clients rapidly and decreasing assistance dormancy. This study finishes up the three-layered information stream design for fog processing and proposes various extraordinary structures to utilize the thought of fog figuring, including energy grids, MediFog, UXFog, connected stopping framework, and FoAgro.

Kishor et al. [14] mentioned to overcome latency, fog computing brings data processing, storage, and analysis closer to IoT and end-users. In this study, a novel Intelligent Multimedia Data Segregation (IMDS) approach based on Machine Learning (k-fold random forest) is provided for usage in a fog computing environment to separate multimedia data, as well as the model used to assess total latency (transmission, computation, and network). The research achieved 92 percent classification accuracy with the simulated findings, a 95 percent reduction in latency when compared to the pre-existing model, and increased the quality of services in e-healthcare.

Kaur et al. [15] introduced an IoT-based Cloud-Fog helped layered clearing framework for mass departure during a crisis. The framework utilizes the fog-registering worldview to survey alarm wellbeing progressively utilizing the fluffy K-closest neighbor (FK-NN) approach. The fog layer's energy-saving frameworks embrace information determination and information decrease to restrict the amount of information sent to the top layer. The Spatio-fleeting Data Selection layer chooses information for resulting transmission because of its spatial-worldly examination. The information decrease part uses Principal Component Analysis to diminish the elements of information (PCA) proposed in his work, an IoT based Cloud-Fog helped layered clearing framework for mass departure during crisis circumstances. Utilizing the Holt-Winters approach, the cloud layer evaluates the future worldly well-being condition of evacuees. The Geographic Analysis layer in the cloud works out an individual's need departure status in light of their current and future fleeting frenzy condition. Moreover, it demonstrates the locale's needs clearing status in view of the number of individuals who are presently panicked and the normal well-being status. Experimentation demonstrates the efficacy of the suggested method at various levels.

Sun et al. [16] proposed a framework that consolidates property-based encryption (ABE) with search encryption (SE) innovation to give a catchphrase search as well as fine-grained admittance control. Whenever the catchphrase record and secret entryway match are fruitful, the cloud server supplier offers just applicable query items to the client, bringing about a more precise hunt. The strategy is multi-authority simultaneously, and the key spillage issue is settled by separating the client's secret key appropriation obligation. Furthermore, in this work, a portion of the encryption and decryption activities was outsourced to the fog node securely. we re-appropriate a piece of the encryption and decoding exercises to the fog hub in a safe way. It functions admirably with both neighborhood assets and asset-compelled cell phones. The method is secure because it depends on the decisional q-equal bilinear Diffie-Hellman example (q-DBDHE) suspicion and the decisional bilinear Diffie-Hellman (DBDH) presumption. Experiments with simulations reveal that our technique works well in a cloud-fog scenario.

Awotunde et al. [17] mentioned in recent years since healthcare databases get more complex and larger, the likelihood of transmission and data processing delays remains a worry. Fog computing is the most promising alternative answer to these difficulties in terms of lowering data the board intricacy in the medical services framework and accordingly upgrading unwavering quality. In any case, to proficiently deal with medical care information, it is basic to initially research the issues associated with fog processing. Thus, fog applications in IoT-based gadgets get medical services parts a remote cloud nearer to information sources and end-clients, bringing about setting mindfulness and lower idleness.

Abdelmoneem et al. [18] published Fog-Cloud processing structures are new standards intended to develop existing Internet of Things plans (IoT). It gives a cloud-fog based IoT foundation for medical care that is interoperable. It makes sense of its plan, the climate in which it exists, and the client setting. The proposed design works with patient development as well as a variety of ailments. The parts of the singular modules are tended to, as well as the connection between the different fundamental modules and layers. To productively adjust the circulation of medical services obligations, an assignment planning and allotment approach is given. The proposed approach's presentation is assessed utilizing different quantities of errands and cloud hubs. The recreation results show that the cost, and inactivity are altogether satisfactory.

Mahmud et al. [19] examined carrying out Cloud-Fog interoperability and joining requires complex coordination of utilizations and administrations, as well as the requirement for wise help organizations, so arrangements can utilize appropriated assets while keeping up with steadiness, administration quality, and security. In this research, a Fog-based IoT-Healthcare solution structure was provided and the integration of Cloud-Fog services in interoperable Healthcare solutions that go beyond the typical Cloud-based structure was investigated. The situations are tried utilizing the iFogSim test system, and the results are examined concerning disseminated figuring, inactivity decrease, information correspondence enhancement, and power use. The trial results highlight cost, network deferral, and energy utilization upgrades.

3. System Model

Fog computing will offer all the edge-computing features, such as flexibility, interoperability, decentralization, etc. Large-scale IoT installations produced scenarios that cloud computing could not flexibly handle. For example, applications that require low latency while processing the data at the network edge. In addition, with the growing data generated from each device;

the conventional cloud computing model has become inadequate in addressing issues such as high latency, limitation of bandwidth, and limitation of resources [20].

Existing framework disadvantages are wastage of assets, no appropriate reaction, increment consumption, and absence of QOS. The staggered interruption discovery framework is an apparatus for executing dynamic IDS in cloud computing [21]. The staggered IDS approach adds to the ideal utilization of assets by applying a separate degree of safety force in light of the level of oddity to clients. The proposed strategy increments cloud computing framework asset accessibility and addresses possible dangers by sending staggered IDS and overseeing inconsistency-level client logs per bunch. The fog helped information model purposes IoT devices to give medical care as a cloud administration. IoT medical services area might be an assailant's objective as gadgets and applications oversee private data and present medical services information. The attention is on classification, uprightness, verification, accessibility, versatility and adaptation to non-critical failure to accomplish related administrations [22].

The file can be transferred through a communication link, so vital data are continuously collected by the sensors during this process and sent to the server to provide a connection between the IoT subsystem and the cloud infrastructure. It performs basic information processing and consolidation producing clear signals rendering the information available to subscribing organizations for notification or to move the data out to the cloud for more analysis and sharing of personality across healthcare. Functions that involve processing storage and evaluation of the patient health data collected from the IoT subsystem are conducted in the data center [23]. Data-driven patient assessment and intervention take place in applications and services. There is a doctor, emergency response service, medical research center, and health professionals. The center for monitoring involves many staff in the observation, diagnosis of patients, and processes of intervention. Furthermore, all requests for patient data access are handled by the monitoring center. Authorized users wishing to obtain sensor data must submit a data proposal to the cloud via the monitoring center. The data will be returned to the user if the requested data is available in the data storage of the sensor.

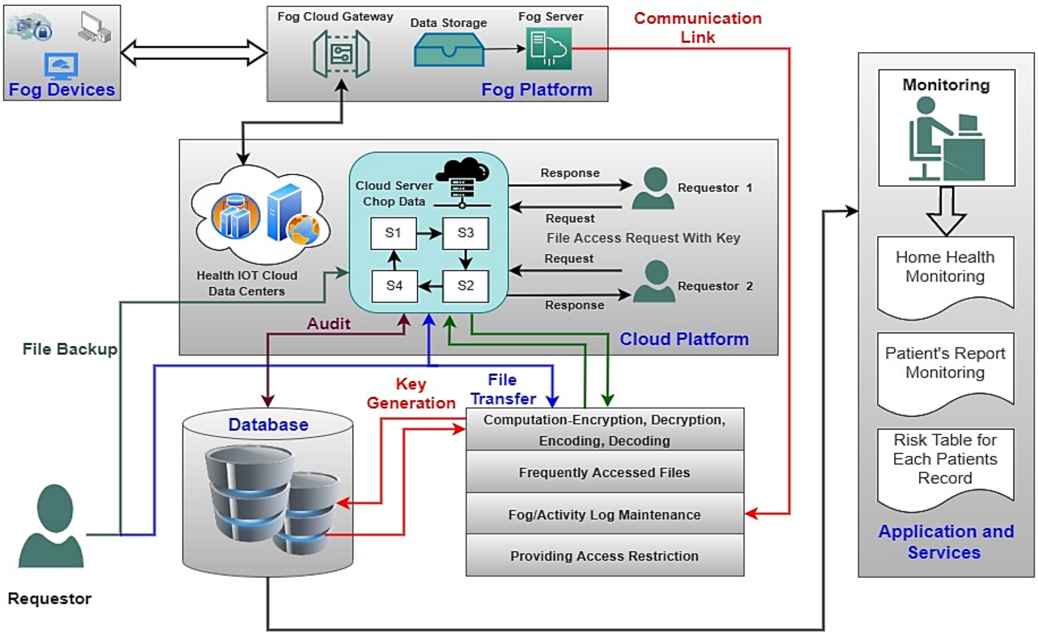

Fig. 2. Architecture of cloud and fog-based secure IoT environment

4. System Setup

a) System Initialization

The system algorithm picks bilinear guide e: G0 * G0 → GT, where G0 **is** bilinear gathering of prime request p and g is the generator of G0. Then, at that point, the further quality authority haphazardly picks h ϵ G0 and α, β ϵ Zp, where the range of Z_p is [1, p]. Now choose hash functions H_1 : {0,1}* → G_0.

The final system public key output PK = (g,h,g^{α},g^{β},h^{β},e(g,g)$^{\alpha\beta}$) and master secret key MK = (α, β).

b) Key Generation

The key generation algorithm chooses a random γ ϵ Z_p, then the attribute authority chooses a random Ɛ ϵ Z_p, and random r_j for each attribute j ϵ S, where S is the attribute set of the user. The output secret key and outsourcing key will be:

$$SK = (D = g^{(\alpha+\gamma)\beta}) \tag{1}$$

$$SK = (D_1 = g^{\gamma}\, h^{\mathcal{E}}, D_2 = \ g^{\mathcal{E}}, \{D_j' \ = \ g^{\gamma\beta} H_1(j)^{rj}, D_j'' = g^{rj}\} j\epsilon S) \tag{2}$$

The secret key SK is dependent on the generators, prime orders, and hash function as expressed in equations (1) and (2). The outsourcing key SK' = (D_1, D_2, $\{D_j', D_j''\}\ j\epsilon S$) of the user is sent to the fog nodes, and the user only stores SK. This key is used in the encryption and decryption processes.

c) Data Encryption

Before transferring information to the CSP (Cloud Service Provider), the information proprietor initially picks an irregular DK ∈ Zp, and encodes the information M with DK utilizing symmetric encryption calculation, indicated as C = SEDK (M). Then information proprietor characterizes an entrance strategy Ta and an update strategy Tu, and sends Ta to fog the fog nodes run Fog.Encrypt, a user-defined function to perform the outsourced encryption algorithm. The procedure followed in the Fog.Encrypt function is explained as follows. For every node x in the access strategy tree Ta, the fog hubs pick a polynomial px . Starting from the root node R, the px is picked hierarchically. For every hub x in the tree, set the degree dx of the polynomial px to be one not exactly the edge esteem kx of that node, that is dx = kx − 1. Beginning with the root node R, the calculation picks an arbitrary s ∈ Zp and sets $P_R(0)$ = s. Then, it picks d_R different places of the polynomial P_R haphazardly to characterize it. For some other node x, it sets P_x (0) = $P_{parent(x)}$(index(x)) and picks dx different focuses haphazardly to characterize px. Allow Y to be the arrangement of leaf hubs in Ta, the fog hubs yield a halfway ciphertext CT'.

$$CT' = (T_a, C_3' = \ g^{\beta s}, C_4' = \ h^{\beta s}, C_5 = \ \{C_y' = g^{Py(0)}\ , C_y'' = H_1\big(attr_y\big)^{Py(0)}\} y\epsilon Y) \quad (3)$$

Finally, the fog nodes return CT' to the data owner. The data owner runs Owner.Encrypt algorithm to select t ϵ Z_p at random and computes C_1 = DK. e(g,g)$^{\alpha\beta t}$ with DK, and computes C_2 = g^t, C_3 = C_3'.$g^{\beta t}$, C_4 = $C_4'.h^{\beta t}$. Finally, the data owner outputs the ciphertext CT.

$$CT = (T_a, T_u, C = SE_{DK}(M), C_1 = DK.e(g,g)^{\alpha\beta t}, C_2 = g^t, C_3 = g^{\beta(s+t)}, C_4 = h^{\beta(s+t)},\ C_5 = \{C'_y = g^{Py(0)}, C''_y = H_1(attr_y)^{Py(0)}\} y\epsilon Y) \tag{5}$$

d) Data Decryption

A client initially acquires the ciphertext CT from the fog gadget and {D}k from the cloud. Assume the arrangement of properties S fulfills the entrance structure AS in the ciphertext, and let I ⊂{1,2,… ,l}, I = {i : ρ(i) ϵ S}, then {ωi ϵ Zp}iϵI can be determined where {ωi }iϵI are constants with the end goal if that {λi} iϵI are substantial portions of mystery s, Σ iϵI ωiλi = s. The decoding system is as per the following,

$$\frac{e\ (C',K)}{\Pi_{i\epsilon I}(e(C_i,L)e(D_i,K_{\rho i}))\omega i} \tag{6}$$

$$= \frac{e\ (g,g)^{\alpha s}\ e(g,g)^{\alpha st}}{\Pi_{i\epsilon I} e(g,g)^{t\alpha\lambda i\omega i}} \tag{7}$$

$$= e(g,g)^{\alpha s} \tag{8}$$

5. Proposed Optimization Framework

Stage 1: Constructed fog centers around three boundaries: Fog cloud passage, information capacity, and fog server. Fog hubs can be addressed as f1, f2...f100.

Stage 2: Fog hubs can hold more than each undertaking in turn, so the culmination time is the time taken for each assignment that runs with the longest execution time. It is feasible to portray the execution time e_t of Task T by the fog hub and defer d with the imperative.

$$e_t = max \sum_{i=1}^{n} c_t\ , i \in N \tag{9}$$

$$e_t\ (t,f) < d$$

where,

e_t - Execution time, c_t - Completion time, t - Time taken, d – Delay, f - Fog nodes

Step 3: Cloud Initialization: First, initialize servers s_1, s_2, s_3, and s_4 for request and response in the cloud platform is done.

Stage 4: Files to be moved in a protected way for the clinical area can be addressed as F1...FN.

Stage 5: For each IoT correspondence

i1: Encrypt F at the shipper side (s) and unscramble F at the recipient side (d).

i2: Frequent review with information base.

i3: Maintain movement log

Stage 5 is rehashed until the reenactment closes.

Stage 6: Monitoring focus keeps up with risk table and wellbeing record.

Cloud computing is easy to target. For this reason, all users and administrators can be judged as potential attackers and strong security measures can be applied to all traffic. It is therefore effective for everyone. This method also supports anomaly-level classification of logs, so it first makes the system administrator analyze the log of the most suspected users. **Fig. 2** depicts the proposed system model. The proposed system can provide an efficient resource allocation, proper response, high QOS economic benefit, and elaborate service efficiently.

Algorithm 1 presents the pseudocode of storing the files securely in the cloud. The input considered for this approach is the file and the resources used are fog and cloud servers. Once the resources are initialized, data from the files are segmented. Each segmented data is encrypted and stored in the corresponding cloud server. To get access to this stored data, the user has to share the private key for decryption. With the private key, the data is decrypted and broadcasted to the user who requested the data access.

Algorithm 1: Secure Storage of Files

Input: File
Output: Storing the Data
Resources: Fog, Cloud Server $C = C_1, C_2, C_3, \ldots, C_n$

```
Initialize the resources
if $data == segmentedData$
    $esegData \leftarrow encrypt(segmentedData)$
    Migrate $esegData$ to $C$
    for $i = 1$ to $n$
        Assign $C_i \leftarrow esegData_i$
        Raise online query for collecting $esegData_i$
        $enewData_i \leftarrow esegData_i$
    End
    $newData \leftarrow decrypt(enewData)$
    Broadcast $newData$ to user
    for $i = 1$ to $n$
        $user_i \leftarrow newData_i$
    End
End
```

Algorithm 2 presents the pseudocode of the estimation of execution time. For every segmented data, the completion time is calculated and accumulated for n size of data. In the meantime, the execution time is recorded on a report for reference.

Algorithm 2: Estimation of Execution Time

Input: Segmented Data $segmentedData$
Output: Report $Report$

```
Assign Index
for $i = 1$ to $n$
    $e_t \leftarrow executionTime(segmentedData_i)$ (Using Equation 1)
    $Report_i \leftarrow report(e_t)$
End
Return $Report$
```

6. Results and Discussions

On multiple platforms like Windows and Linux, CloudSim can run. A system running Windows 7 OS with Intel Pentium Dual core P6000 and clocked at 1.87 GHz along with 8.0 GB of memory and 1 TB of hard disk storage is used for the simulation environment. In the simulator, the application task parameters include File Size, Key Generation, Encryption time, Time taken to upload server, Decryption time, CPU Utilization, and Memory Consumption as presented in **Table 1** and graphically presented in **Fig. 3(a) to 3(b).** In an area, the fog node coordinates are simulated, such as a hospital, and the range of fog nodes from 0 to 100 is limited. The data collected from the fog nodes are Medical Data Health-Care (MDHC) record data.

Trying different things with huge scope structures includes the accessibility of registering assets for use in a recreation climate. The performance of the existing system is evaluated. At first, the key generation and the encryption time followed by the uploading time between the client and cloud for the data file were measured. The results of each calculation over 10 various tests were averaged. The timely execution of the proposed plan in all exhibition measurements are outperformed than the customary plan. The absolute CPU usage season of the proposed plan for performing Fog and Cloud procedures on the document and the ideal opportunity for the client to arrange on working the server are lower than the ordinary strategy. The performance of the proposed encryption technique is compared with the existing methods such as Chosen Ciphertext Attack-secure Attribute Based Encryption (CCA-secure ABE) [24], Ciphertext Policy-ABE (CP-ABE) [25], CP-Attribute Based Signature (CP-ABS) [26], and Block based Sharing Scheme (BSS) [27]. Different sizes of input files are passed through these three models to evaluate their performances in terms of time taken for execution in key generation, data encryption, data decryption, uploading server, and CPU utilization. It is evident from than the existing models. This proves the robustness of the proposed model of being able to process any file size efficiently.

Table 1. Data Analysis Report (Existing and Proposed System)

Key Generation			
File Size (MB)	**(CCA-secure ABE) [24] *(ms)***	**(CP-ABE) [25] *(ms)***	***Proposed System (ms)***
10	966.214	1008.756	822.540
20	1810.813	2038.108	1521.956
30	2778.602	3026.403	2447.180
40	3602.651	4014.653	3272.739
50	4570.352	5064.466	4138.420
60	5497.040	6032.255	5043.982
Data Encryption			
File Size (MB)	**(CP-ABS) [26] *(ms)***	**(CP-ABE) [25] *(ms)***	***Proposed System (ms)***
10	96.716	102.09	66.269
20	291.940	284.776	148.657
30	349.254	354.627	274.03
40	401.194	417.313	361.791
50	497.910	442.388	444.179

<table>
<tr><th colspan="4">Data Decryption</th></tr>
<tr><th><i>File Size (MB)</i></th><th>(CP-ABS) [26] <i>(ms)</i></th><th>(CP-ABE) [25] <i>(ms)</i></th><th><i>Proposed System (ms)</i></th></tr>
<tr><td>10</td><td>120.166</td><td>63.739</td><td>87.564</td></tr>
<tr><td>20</td><td>178.892</td><td>61.025</td><td>137.51</td></tr>
<tr><td>30</td><td>198.747</td><td>58.308</td><td>166.143</td></tr>
<tr><td>40</td><td>280.044</td><td>63.115</td><td>226.12</td></tr>
<tr><td>50</td><td>378.892</td><td>57.888</td><td>336.259</td></tr>
<tr><th colspan="4">Time taken for upload server</th></tr>
<tr><th><i>File Size (MB)</i></th><th colspan="2">Block based Sharing Scheme (BSS) [27]</th><th><i>Proposed System (ms)</i></th></tr>
<tr><td>1</td><td colspan="2">247.140</td><td>188.554</td></tr>
<tr><td>1.5</td><td colspan="2">494.651</td><td>381.981</td></tr>
<tr><td>2</td><td colspan="2">597.932</td><td>561.881</td></tr>
<tr><td>2.5</td><td colspan="2">705.721</td><td>660.665</td></tr>
<tr><td>3</td><td colspan="2">799.993</td><td>786.486</td></tr>
<tr><td>3.5</td><td colspan="2">903.279</td><td>835.688</td></tr>
<tr><td>4</td><td colspan="2">1002.058</td><td>961.499</td></tr>
<tr><td>4.5</td><td colspan="2">1091.828</td><td>997.175</td></tr>
<tr><td>5</td><td colspan="2">1393.423</td><td>1190.607</td></tr>
<tr><th colspan="4">CPU Utilization (Percentage)</th></tr>
<tr><th><i>File Size (MB)</i></th><th colspan="2">Block based Sharing Scheme (BSS) [27]</th><th><i>Proposed System (ms)</i></th></tr>
<tr><td>1</td><td colspan="2">1.529</td><td>0.198</td></tr>
<tr><td>1.5</td><td colspan="2">2.510</td><td>1.469</td></tr>
<tr><td>2</td><td colspan="2">2.971</td><td>2.768</td></tr>
<tr><td>2.5</td><td colspan="2">3.981</td><td>2.998</td></tr>
<tr><td>3</td><td colspan="2">5.108</td><td>4.095</td></tr>
<tr><td>3.5</td><td colspan="2">5.858</td><td>5.019</td></tr>
<tr><td>4</td><td colspan="2">6.984</td><td>5.479</td></tr>
<tr><td>4.5</td><td colspan="2">7.502</td><td>5.998</td></tr>
<tr><td>5</td><td colspan="2">8.455</td><td>7.876</td></tr>
</table>

Experimenting with large-scale structures involves the availability of computing resources for use in a simulation environment. We evaluated the implemented performance of the existing system. At first, we measure the key generation and encryption time followed by the uploading time between the client and cloud for the data file. We average the results of each and every calculation over 10 various tests. The time performance of the proposed design in all performance metrics is outperformed than conventional design. The total CPU utilization time of the proposed design for performing Fog and Cloud operations on the file and the time for the client to coordinate on operating the server are lower than the conventional method.

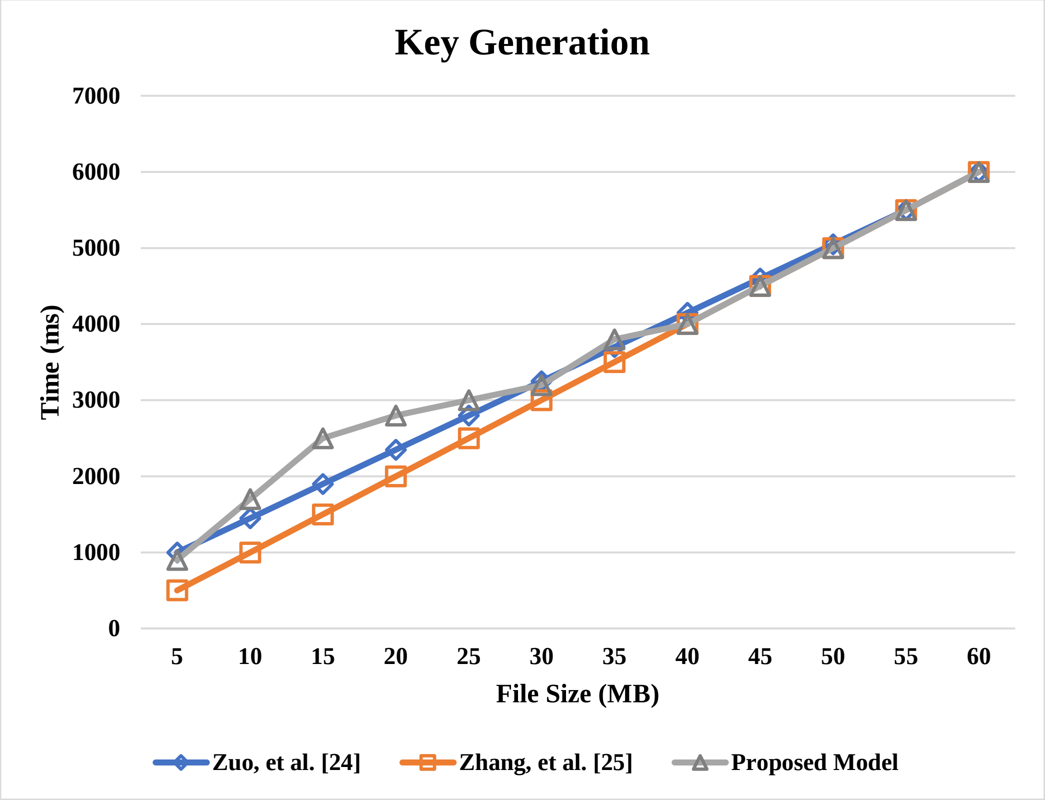

Fig. 3 (a)

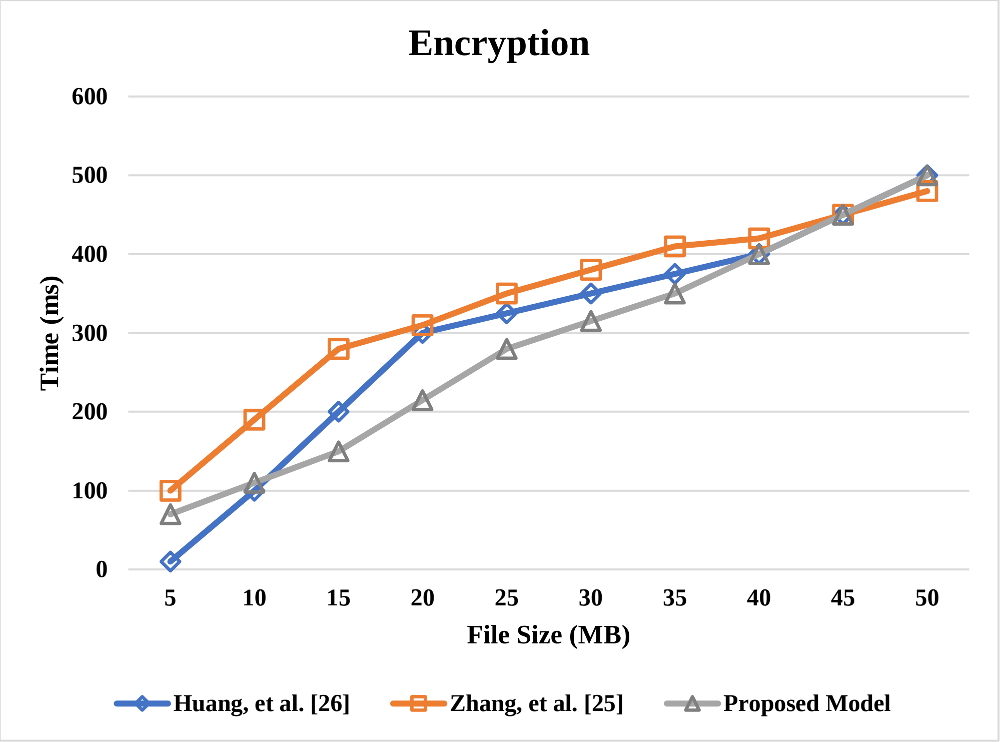
Encryption
Time (ms)
0
100
200
300
400
500
600
5
10
15
20
25
30
35
40
45
50
File Size (MB)
Huang, et al. [26]
Zhang, et al. [25]
Proposed Model

Fig. 3 (b)

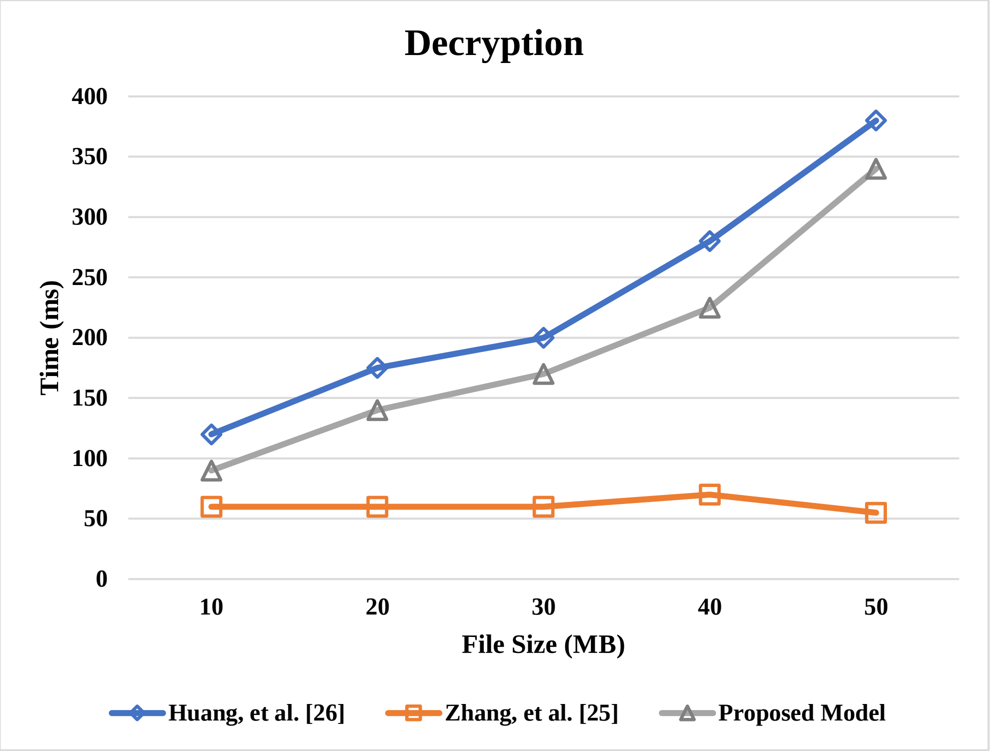
Decryption
Time (ms)
0
50
100
150
200
250
300
350
400
10
20
30
40
50
File Size (MB)
Huang, et al. [26]
Zhang, et al. [25]
Proposed Model

Fig. 3 (c)

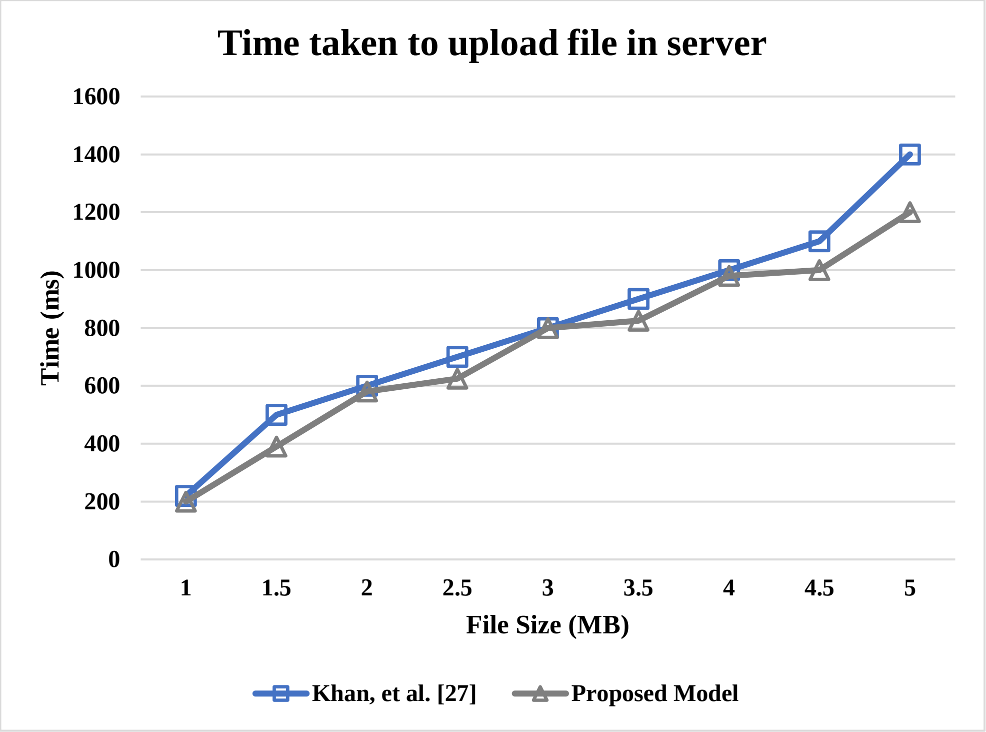

Fig. 3 (d)

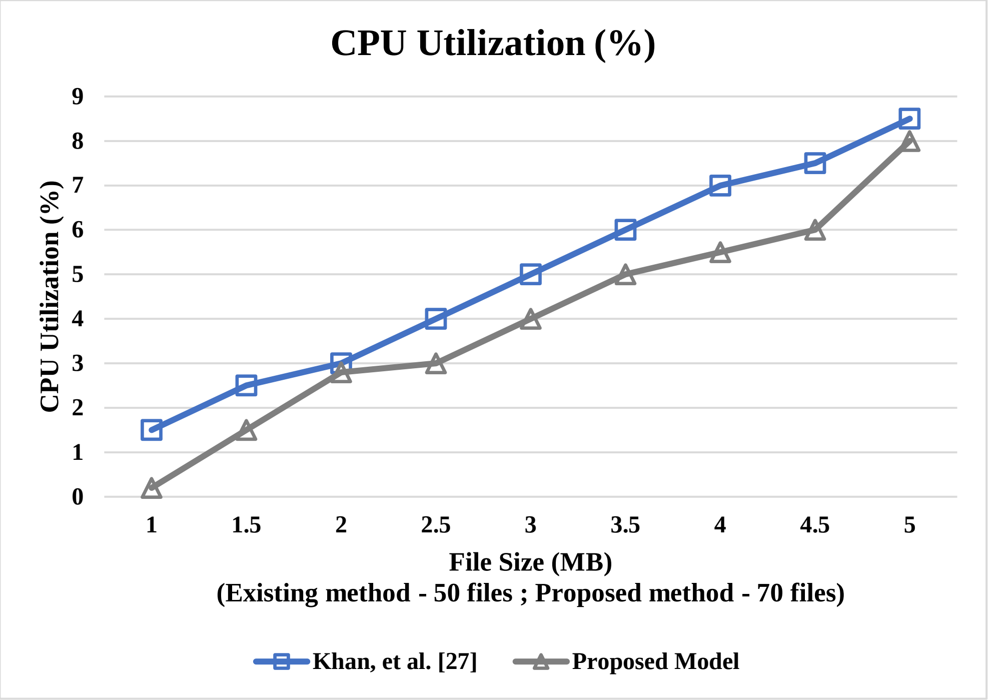

Fig. 3 (e)

Fig. 3. Various performances of Fog and Cloud Operations (a) Key Generation (b) Encryption (c) Decryption (d) Time taken for upload server (e) CPU utilization

Regardless we consider that the hour of cryptographic exercises is just conventional techniques in all instances of record transfer/download activities. Likewise, the transmission time is dependably lower than the existing system, no matter what the record size. Note that activities for transferring and downloading are awry and utilize different times to finish the tasks. It is notable that, when the size of the actual data file content increases the output overhead of the proposed system becomes less important. In any case, it was comparable to different calculations when 100 or more assignments were submitted. In this work, it is vital to take note that the two layers are displayed all through various conditions during testing. The administrator didn't move errands/information straightforwardly from the terminal layer to the fog layer. This could be considered in future work.

6.1 System security

A. Authentication

As a rule, the fog server empowers the end client with apparatuses. Accordingly, the fog server must initially confirm the end client's personality and afterward securely disperse assets. Validation components are one of the significant security administration issues and it's expected in cloud fog processing innovation. To get to any administrations, the end-user(s) or device(s) should be confirmed to the collector end (like the server). Validation assumes a vital part as fog gadgets can give assets after just end-client verification and accordingly, all end-client and fog gadgets should be confirmed by the cloud server before supporting admittance to assets. Yet in addition, shared validation is similarly significant because of the huge volume of organizations and the cloud disguise assault. It is additionally critical security worries in the common validation convention that copy man-in-the-center assault, which the aggressor attempts to emulate as either end client or fog serves. Assuming that the assailant some way or another plays out this assault, the authentic substance (end client, fog server) will profit from having the first message. Along these lines, protecting such a sort of attack is profoundly attractive.

B. Key Management

Key administration is one more significant thought which is vital for secure information transmission among cloud and fog servers. There must be a public key framework that produces key (encryption, decoding) for the fog and cloud server to guarantee secure correspondence between the fog and cloud server. All fog frameworks will hold their own private key alongside other classified data so the adversary can't get to the data. Like fog gadgets, the private key protection should be kept up with by the cloud server as well. Every one of those private keys is indispensable, because, it ought to be referenced that every one of these keys should set meeting key for secure correspondence. If the rival in some way or another gets every one of these keys, utilizing the convention definition, he can get every one of the correspondences traded through a weak stream by setting the more established meeting keys. Another significant contention connects with the classification of meeting keys in this specific circumstance. For ensuing information trade, the meeting key should be gotten in the common confirmation convention utilizing the meeting keys that is traded between the substances to scramble the information. It is best security concern and challenge work for the aggressor not to deliver legitimate meeting key from the convention's public data. It is likewise fundamental that assuming the past meeting key is uncovered somehow or another the aggressor shouldn't assess the substantial meeting key. Key administration accordingly is likewise a significant thought in the worldview of fog cloud computing.

C. Data Confidentiality

The information respectability idea demonstrates that the message acquires a similar message from which the source sent by the beneficiary end. It is likewise one of the essential qualities in cloud-fog it is important to register the model. End-client information is generally recovered either from the fog or cloud server. While the fog or cloud server conveys important information, the legitimacy of the information should be given. Similarly, the security ought to be kept up with to send information to either the fog framework or the cloud server. To give the respectability property, one of the current cryptography techniques called hash work (Example: SHA-1, SHA-2, MD5, and so forth) is utilized. It has been worked on by a few scientists and is attempting to accomplish high-integrity rights. Open research problems for the cloud-fog computing model are high ability, high credibility, and high complexity.

D. Data Storage

Information capacity in one or the other server or cloud in plaintext structure is an extremely basic issue, yet to store information securely it is as yet being dealt with by scientists. The important information in our cloud-fog processing model is put away in fog gadgets (as often as possible utilized information) and in cloud servers. All fog and cloud servers hold data set for information capacity. The information is put away in fog data set for later use in the system of fog processing. In any case, the trouble is the way the fog gadgets put away information will give security. It is known to all enemies that they have high usefulness or that they have utilized raised standard strategies to break the framework. On the other hand, a few agents were recommended to store the information in a scrambled mode so they wouldn't have the option to unscramble the information after getting the put away information. The fog gadgets need to hold a key for encryption and unscrambling thusly. Similarly, as with fog apparatuses, there are similar types of issues in cloud computing. Overall, quite well the protected stockpiling of information with proficient results of the calculation stays an open test for established researchers.

E. Intrusion Detection System (IDS)

IDS is additionally imperatively significant as cloud server security insurance gives protection from insider assault, forswearing of-administration assault, port checking assault and flood assault. Noxious clients can send unimportant data to the recipient during correspondence and can create a surge of information for the beneficiary to execute a DoS or DDoS assault. Thusly, sending IDS strategies on fog gadgets to recognize problematic action is extremely essential and significant by following and assessing log records, client data, access control approaches, and so on There are likewise a few laid out IDS calculations accessible not or quality proficient. In any case, growing new and compelling calculations for IDS is as yet testing work. Like fog gadgets, could likewise be important at the cloud server. On the opposite side, Intrusion Prevention System (IPS) is additionally vital on the fog and cloud server as it is as yet open review difficulties to plan a proficient calculation.

From the outcome and approval, it is seen that the proposed technique uses less capacity size quicker than expected. In the present cloud computing climate, wellbeing cloud safeguards the individual touchy data for a very long time, for example, clinical examination, health care coverage organizations, clinical information investigation, and so on at the point when any approved individual access these fogs, delivered information shouldn't think twice about person's protection and it ought to stay valuable also. The information should be delivered so that any singular character can't be uncovered. Algorithm 1 shows the safe stockpiling of information in the cloud which defeats saving the singular's protection by sectioning the information and putting it away in the fog and cloud layer in light of the security level. Algorithm 2 shows the calculation of execution time which is productive and accomplished low inactivity, quick reaction time, least calculation time, and CPU use.

F. Qualitative Comparison

The qualitative differences between the proposed security model and the existing security models CP-ABS and CP-ABE in terms of key length flexibility, time consumption for key generation, time taken for encryption, time taken for decryption, and security level against brute force attacks are given in **Table 2**.

Table 2. Qualitative Comparison

Specification	**CP-ABS [26]**	**CP-ABE [25]**	**Proposed secure-ABE**
Key length flexibility	Yes	Yes	Yes
Time consumption for key generation	Less	Less	Less
Time consumption for encryption	Less	High	Very less
Time consumption for decryption	Very high	Very less	High
Security against brute force attacks	Less secure	Less secure	Highly secure

7. Conclusion

The emergence of IoT devices is crucial in the external environment, and this will be vital because of the predominant utilization of fog figuring as a structure supporting innovation. With the rushed development of IoT and cloud computing, cloud-based IoT applications and patterns are becoming clear in the medical care area. The issue is the joining of cloud-based IoT and Fog processing into the medical services framework in the following ten years. In this paper, cloud and fog processing approaches were joined to survey information development and safe data about clinical medical care. A scope of overwhelming open examination issues is analyzed, for example, access control, information security, area assurance, protection saving rethought information mining, and the tremendous volume of computational repercussion that quite extraordinarily impedes asset-compelled clients from their wide-going applications.

References

[1] T. L. Duc, R. G. Leiva, P. Casari, and P. O. Ostberg, “Machine learning methods for reliable resource provisioning in edge-cloud computing: A survey,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1-39, 2019. Article (CrossRef Link)

[2] P. Chemouil, P. Hui, W. Kellerer, Y. Li, R. Stadler, D. Tao, and Y. Zhang, “Special issue on artificial intelligence and machine learning for networking and communications,” *IEEE Journal on Selected Areas in Communications*, vol.37, no. 6, pp. 1185-1191, 2019. Article (CrossRef Link)

[3] A. W. Malik, I. Mahmood, N. Ahmed, and Z. Anwar, “Big data in motion: A vehicle-assisted urban computing framework for smart cities,” *IEEE Access*, vol. 7, pp. 55951-55965, 2019. Article (CrossRef Link)

[4] T. Alam, "Internet of things: A secure cloud-based manet mobility model," *International Journal of Network Security*, vol. 22, no. 3, pp. 516-522, 2020. Article (CrossRef Link)

[5] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE transactions on computers*, vol. 62, no. 2, pp. 362-375, 2013. Article (CrossRef Link)

[6] D. Tank, A. Aggarwal, and N. Chaubey, "Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison," *International Journal of Information Technology*, vol. 14, pp. 847-862, 2022. Article (CrossRef Link)

[7] F. Zhang, G. Liu, X. Fu and R. Yahyapour, "A survey on virtual machine migration: Challenges, techniques, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 20, no.2, pp. 1206-1243, 2018. Article (CrossRef Link)

[8] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI," *Big Data and Cognitive Computing*, vol. 4, no. 28, 2020. Article (CrossRef Link)

[9] D. Shehada, A. Gawanmeh, C. Y. Yeun, and M. J. Zemerly, "Fog-based distributed trust and reputation management system for internet of things," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8637-8646, 2022. Article (CrossRef Link)

[10] R. Anandan, S. Gopalakrishnan, S. Pal, and Zaman, N. (Eds.), *Industrial Internet of Things (IIoT): Intelligent Analytics for Predictive Maintenance*, John Wiley & Sons, Scrivener, 2022

[11] B. Afzal, M. Umair, G. A. Shah and E. Ahmed, "Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges," *Future Generation Computer Systems*, vol. 92, pp.718-731, 2019. Article (CrossRef Link)

[12] D. W. Chadwick, W. Fan, G. Costantino, R. De Lemos, F. Di Cerbo, I. Herwono, and X. S. Wang, "A cloud-edge based data security architecture for sharing and analysing cyber threat information," *Future Generation Computer Systems*, vol. 102, pp. 710-722, 2020. Article (CrossRef Link)

[13] S. Kunal, A. Saha, and R. Amin, "An overview of cloud-fog computing: Architectures, applications with security challenges," *Security and Privacy*, vol. 2, no. 4, 2019. Article (CrossRef Link)

[14] A. Kishor, C. Chakraborty, and W. Jeberson, "A novel fog computing approach for minimization of latency in healthcare using machine learning," *Int J Interact Multimed Artif Intell*, vol. 6, no. 7, 2020. Article (CrossRef Link)

[15] A. Kaur, and S. K. Sood, "Cloud-fog assisted energy efficient architectural paradigm for disaster evacuation," *Information Systems.*, vol. 107, p. 101732, 2021. Article (CrossRef Link)

[16] J. Sun, X. Wang, S. Wang, and L. Ren, "A searchable personal health records framework with fine-grained access control in cloud-fog computing," *Plos One*, vol. 13, no. 11, e0207543, 2018. Article (CrossRef Link)

[17] J. B. Awotunde, A. K. Bhoi, and P. Barsocchi, "Hybrid cloud/fog environment for healthcare: An exploratory study, opportunities, challenges, and future prospects," in *Hybrid Artificial Intelligence and IoT in Healthcare*, 2021, pp. 1-20. Article (CrossRef Link)

[18] R. M. Abdelmoneem, A. Benslimane, E. Shaaban, S. Abdelhamid and S. Ghoneim, "A cloud-fog based architecture for IoT applications dedicated to healthcare," in *Proc. of ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1-6, 2019. Article (CrossRef Link)

[19] R. Mahmud, F. L. Koch, and R. Buyya, "Cloud-fog interoperability in IoT-enabled healthcare solutions," in *Proc. of the 19th international conference on distributed computing and networking*, pp. 1-10, 2018. Article (CrossRef Link)

[20] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289-330, 2019. Article (CrossRef Link)

[21] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of things," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1-16, 2020. Article (CrossRef Link)

[22] P. Gope, J. Lee, R. H. Hsu, and T.Q. Quek, "Anonymous Communications for Secure Device-to-Device-Aided Fog Computing: Architecture, Challenges, and Solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 10-16, 2019. Article (CrossRef Link)

[23] P. D. Singh, G. Dhiman, and R. Sharma, "Internet of Things for sustaining a smart and secure healthcare system," *Sustainable Computing: Informatics and Systems*, vol. 33, p. 100622, 2022. Article (CrossRef Link)

[24] C. Zuo, J, Shao, G. Wei, M. Xie, and M. Ji, "CCA-secure ABE with outsourced decryption for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 730-738, 2018. Article (CrossRef Link)

[25] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 753-762, 2018. Article (CrossRef Link)

[26] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941-12950, 2017. Article (CrossRef Link)

[27] A. N. Khan, M. L. Kiah, M. Ali, S. A. Madani, and S. Shamshirband, "BSS: block-based sharing scheme for secure data storage services in mobile cloud environment," *The Journal of Supercomputing*, vol .70, no. 2, pp. 946-976, 2014. Article (CrossRef Link)

L. Arulmozhiselvan received the Ph.D. Degree in Information Science and technology from Anna university, CEG Campus, Chennai, India, in 2023. Currently, he is working as an Assistant Professor in Meenakshi Sundararajan Engineering College, Chennai, India. His area of interest is cloud computing, fog computing, security, cloud security.

E. Uma received the Ph.D. Degree in in Information Science and technology from Anna university, CEG Campus, Chennai, India, in 2014. Currently, she is working as an Associate Professor in the department of Information Science and technology at Anna university, CEG Campus, Chennai, India. Her area of interest are Network Security and Forensics Block Chain, Machine & Deep Learning, Cloud Computing, Internet of Things (IoT), Service Oriented Architecture, Semantic Web and .Net Framework Development.