A Unification of Fog-Cloud Computing for Data Agitation and Guard Intensification in Industrial Health Care Security

Debarghya Biswas[1], Ankita Tiwari[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India*

KEYWORDS
Fog Cloud Environment, Healthcare Data Security, Data Agitation, Guard Intensification, Cryptographic Approach, Advanced Encryption Standard, Key Validation

ABSTRACT
The development of Fog computing is a decentralized environment in which the data processing, storage and applications are processed between the located server in a cloud environment. By increasing the Internet of things (IoT) and remote storage, the communication in cloud become more sophisticated by processing the data safely and securely. Healthcare data is important which contains medical information and processed centrality in the public environment through IoT, due to increasing security breaches they need to protect depends on the security applicants. All over the centralized data computing are accessed by virtual environment through remote protocol doesn't provide safety in healthcare industry. To resolve this problem, to propose as Unification of fog-cloud computing for data agitation and guard intensification (DA-GI) in Industrial Health Care Security. The Medical Data Health-Care (MDHC) records are stored in Cloud datacenters and the Fog layer based on the guard intensity and the key is provoked for ingress the file. The activity logs are controlled and monitoring from cloud serves sustains the Activity Log, Risk Table and Health Records. To introduce a cryptographic approach based on advanced encryption standards (AES) to protect data and authenticity verification server. The key verification process based on security gateway, Fog cloud server depends on user access rights provided to the user. During the key validation, role of permission to the user s verified and agitate to allow access rights to the verified service access. The proposed system produce high security compared to the other system as well in all security concerns of role, authentication and verification to process data safely.

1. Introduction

In the rapidly evolving landscape of information technology, Fog computing is emerging as a transformative force, particularly in industries requiring stringent data security measures such as healthcare [5]. Unlike traditional cloud computing, which centralizes data processing in remote data centers, Fog computing decentralizes this operation, providing a framework where data processing, storage, and application delivery occur at various levels between the end-user and the cloud. This configuration facilitates immediate data access and processing while enhancing security protocols, which is paramount given the critical need for safeguarding sensitive healthcare data [4].Fog computing, a term popularized by Cisco, describes a system in which data, storage, and applications are distributed across a network, bringing computational capabilities closer to the data source [1]. This decentralization reduces latency and improves the responsiveness of applications, as it allows for data to be processed at the edge of the network, rather than being routed to a centralized cloud server. This characteristic of Fog computing is particularly relevant in healthcare environments, where timely access to data can be a matter of life or death [3]. The advent of the Internet of Things (IoT) has compounded this challenge, as interconnected devices generate an overwhelming amount of sensitive information, further necessitating robust data protection mechanisms [2]. However, the healthcare industry faces a critical vulnerability; the proliferation of security breaches amidst centralized data computing systems often accessed through virtual environments via remote protocols has underscored the urgent need for enhanced security measures. The increasing complexity of cloud architectures necessitates improved mechanisms for data storage and communication. As healthcare operations expand and integrate more sophisticated technologies such as Internet of Things (IoT) devices, electronic health records (EHRs), and telemedicine applications safeguarding patient data becomes critically important [15]. The centralized nature of traditional cloud computing is increasingly regarded as a vulnerability, especially in a public environment where the risk of data breaches and cyberattacks is heightened. The healthcare sector must navigate significant challenges related to data security. Centralized computing environments, which utilize remote protocols for access and communication, often fail to provide the level of safety and protection necessary for handling sensitive medical information. Data breaches have become alarmingly common, leading to increased regulatory scrutiny and the potential for significant financial and reputational damage to healthcare organizations.

Moreover, the dynamics of healthcare data management involve the integration of heterogeneous data

sources, including patient records, medical imaging, and wearable device data. The centralized storage of this sensitive information exacerbates security concerns, as a single breach can lead to extensive exposure of private patient information. Consequently, the healthcare sector is in dire need of solutions that not only secure data but also enable efficient access and processing [10]. Cloud computing security small percentage of the resources allocated to a wide variety of initiatives, innovations, and applications and regulates to protect the IP, data, applications, facilities and related infrastructure of virtualized cloud computing. Implementation of cloud security relies on cloud service or the existing cloud-based security solutions. Implementation of cloud defense system, should be a shared responsibility between the boss and the solution provider of enterprise. 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 Fog computing rises into operation in conjunction with cloud computing to meet the growing demand for IoT-solutions. The Internet of Things incorporation with the cloud is a value-effective business practice. 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. Therefore, this report 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. The contribution of this paper: To improve the security concern in decentralized fog computing to provide healthcare data storage security in server dependable authentication. To design an advanced encryption standard based cryptographic approach to improve the security and validation based on key authentication roles. We focus on server-dependent authentication mechanisms that ensure robust protection of sensitive healthcare information [6]. By leveraging key authentication roles, our approach not only fortifies the data storage process but also facilitates seamless validation of authorized users [8]. We discuss the implications of our findings for improving security protocols in healthcare applications that rely on decentralized fog computing, ultimately contributing to safer and more reliable data management solutions in the medical field [7].

Background Study

Cloud computing architecture design is different from the conventional calculation method, such as grid computing [9]. Cloud previous intrusion detection / prevention system developed in the coating (ID is / PS) can not produce the desired level of security and efficiency. The expanding supply for resources of cloud from its users insists on the need for some optimal system for ensuring resource requirement [11]. An active reward framework is planned based on theoretical agreement modeling. The agreement is intended to exploit the base station's anticipated usefulness for the distinguishing trait of security [12]. Next, the problem of assignment of tasks is presented in a two-sided problem, i.e. matching between vehicles and user equipment (ZhenyuZhuo et al., 2019). The vehicle fog computing (VFC) fault-tolerant off-road method vehicle was developed as an optimization problem, running the fog node and using a crosswalk (Zhaolong Ning et al., 2019). IDS can be deployed at various locations, including network boundaries, servers, virtual machines/hypervisors, and clouds smeared in all cloud regions [13]. The IDS method of detection can be based on signatures, anomalies or hybrids. Including soft computing methods such as fuzzy inference, neural system (ANN), support vector machine (SVM), association rules and genetic algorithms (GA), or any combination of these to improve the quality of IDS based on signatures or based on anomalies [14].

IDS log information and execution is a process predefined (Philip Cox et al. 2012), intrusion detection system [16]. These may be entities that encompass the scope of the computer being observed, and may be hardware or software. In cloud computing systems, there are three types of IDS: host-based IDS, network-based IDS, and distributed IDS [17]. Security is the key to a new era of on-demand cloud computing. Researchers have already investigated several intrusion detection technologies in the world of cloud computing to detect intrusions. Most of them provide traditional technical censorship for

identifying abuse and anomalous users (Hongchen Wu et al., 2019). Distributed denial of service (DDoS attack) is a relatively high detection method in the cloud environment. Not only does it seriously harm cloud computing, but it also leads to false and lack of vigilance in establishing DDoS attacks [18]. The concept of Flow Correlation Degree (FCD) is based on asymmetric semi-directional interaction, which has two groups of FCD functions that constitute message statistics (PSD) and semi-directional interaction anomalies (Chen, J et al., 2018.). The Internet provides many information-intensive applications and computing intensives with powerful large-scale computing capabilities [19]. The Internet of Things triggers data, realizes the computing power provided by time-critical applications that calculate fog, and will save the amount of data transferred to the cloud to store data quickly near devices (Chen Xiaowei et al., 2019) [20]. Cloud computing features, such as ubiquitous access, limited computing and the power of multi-tenant IoT devices, the state-of-the-art computing infrastructure in these countries are threatened from severe security and privacy (Virtual Zhang et al., 2019).

The hardware of the FPGA node can be refined to ensure that the minimum delay or low power consumption is added proportionally, thereby providing the maximum mission performance capability (Sendip K. et al., 2018). It is configured to analyze and limit the virus based on the cloud-based healthcare system that it spreads fog [21]. Based on health symptoms, the energy consumption and workload of cloud virtual machines, the decision tree is used to classify the infection level of the user, and the diagnostic alarm is immediately on the user's mobile phone (Luca Cerina et al., 2017). Three main components, multi-level services improve network quality: machine learning, big data and high-performance computers, the prospect of using the cloud and network layer to maximize connection speed [22]. Data storage is used in (Tahamo Hamid et al., 2018) for network traffic routing determination [25]. Secure Deduplication Data Publishing (S-DDD) proposes an IoT scenario for medical treatment using network edge fog servers [23]. Lightweight repetition mechanisms, including Adaptive Blocking Algorithm (ACA), have been proposed to remove redundancy to determine the tangent point between two windows (ATA Ula et al., 2018). In computing-enabled smart cities, a vehicle-based geographic movement model of vehicle computing resources is being developed [24]. As a network platform, the vehicle pushes the limits of the imbalance and complexity of vehicle computing resources which enhances the flexibility of traditional cloud services architecture [26]. To match the resource consumption and globally distribute computer resources, a reward scheme is proposed which influences the choice of vehicle route by resource pricing (FuhongIin et al., 2019 and Wu Yang et al., 2019).

System Model

Developing computing in cloud paradigm is that fog computation extends to the tissue edge required for distributed computing processing. Also, edge registration or cloud, thin grip knobs are ultimately called administrative advantages between gadgets and distributed server farming, promoting the implementation of the system and mechanisms. Fog computing effortlessly serves as the basic level of service for IoT protocol handshakes with cloud computing. Compared to IoT tools, cloud computing servers are super-fast. Fog computing devices provide an intermediary between two distant machines [27]. The fog/computing middle tier allows it to easily move over fog device(s) than software updates can significantly make changes to IoT devices (such as patch Updates, etc.) will make some fixes. Fog Computing provides all edge computing capabilities such as flexibility, interoperability, decentralization, etc. Cloud computing generates scenarios that large IoT installations could not handle flexibly. For example, home automation, for medical and agricultural oriented applications that require low latency while processing data at the network edge [28]. Besides, with 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.

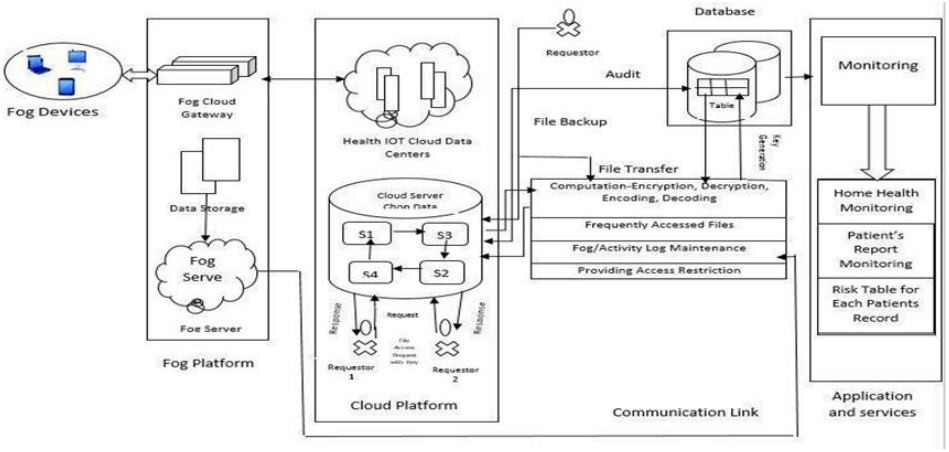


Fig. 2 Architecture of cloud and fog based secure IoT environment

The device are large task share with cloud server the single cloud storage has difficult to process task so it have high latency. Files can be transferred via communication links, so during this process sensors collect critical data and send it to servers to provide connectivity between IoT subsystems and cloud infrastructure [29]. It moves data to the cloud for basic information processing and integration, generating security analysis on health landscape and personality sharing [30]. Additionally, all requests for access to patient data are handled by the Monitoring Center. Authorized users who wish to receive sensor data must submit data requests to the cloud through the Monitoring Center. If the requested data exists in the sensor's data store, the data is returned to the user.

The Proposed DA-GI Framework

To effectively address the security concerns evident in healthcare data management, we propose a framework that leverages the strengths of both fog and cloud computing, termed the Data Agitation and Guard Intensification framework (DA-GI). This dual-layer architecture is specifically designed to fortify security protocols while ensuring robust accessibility and management of MDHC records. The DA-GI framework operates through two main components: Fog Layer: The fog computing layer is positioned closer to the data source such as IoT devices monitoring patients' health metrics thus facilitating immediate data processing and analysis. Sensitive data remains localized within this layer, allowing for effective preliminary filtering and analysis prior to transmission to the cloud. The fog nodes serve as both data processing units and as local security gateways, equipped with algorithms that proactively identify and mitigate potential data **breaches. Cloud Layer**: The cloud component serves as a centralized repository for vast amounts of MDHC records, ensuring scalability and accessible archival storage. Data stored in the cloud is encrypted and managed per strict access controls to prevent unauthorized retrieval. The cloud also hosts advanced security features such as activity monitoring and log management.

2. Security Mechanisms

The DA-GI system introduces a multi-faceted approach to security through the implementation of robust encryption protocols, access control mechanisms, and real-time monitoring:

- **Advanced Encryption Standard (AES)**: Data stored within both the fog and cloud layers is secured using AES encryption, which provides a layer of confidentiality and integrity. This encryption is applied both at rest and in transit, ensuring that data remains secure irrespective of its state.
- **Activity Logs, Risk Tables, and Health Records Management**: The system actively monitors interactions with the MDHC records, maintaining comprehensive activity logs that are analyzed in conjunction with a risk assessment table. This process serves to identify anomalous user behavior and strengthen the overall security posture.

- **Key Verification Process**: Central to the system's security is the sophisticated key verification process. Users are assigned access rights based on role permissions within the security gateway, which screens requests for data access. The verification process during key validation ensures that only users with appropriate credentials can access sensitive information.
- **Role-Based Access Control (RBAC)**: By deploying role-based access control mechanisms, the DA-GI system ensures that permissions are strictly enforced. Users can only access medical data pertinent to their roles, minimizing the potential impact of insider threats and errors.

3. Benefits of the Proposed System

The proposed DA-GI framework offers several advantages over traditional models:

- **Enhanced Security**: By amalgamating fog and cloud architectures, the DA-GI framework provides a more secure environment for healthcare data, effectively mitigating risks associated with centralized data storage.
- **Improved Performance**: The proximity of fog nodes to data sources allows for reduced latency in data processing and retrieval, leading to more timely healthcare interventions and decision-making.
- **Dynamic Adaptability**: The dual-layer system enables real-time monitoring and response to emerging threats or suspicious activity, facilitating proactive risk management.
- **Compliance and Audit Trails**: Comprehensive activity logging and audit trails not only align with regulatory compliance mandates but also bolster trust among patients regarding the confidentiality of their medical records.

Algorithm

Step 1: define fog nodes f_1, f2...f_n. including stige, server, VM under defined gateway

Step 2: Construct execution task time T, based on the maximum computed time etc. through fog nodes and delay d and constraints.

$$e_t = max \sum_{i=1}^{n} c_t \ , i \in N \qquad (1)$$

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

Step 3: initiate the server computing time on based on the request data through request and response under S1, S2.

Step 4: security apply the crypto policy for all files F_1...F_N.

Step 5: compute for all files generate Id

i_1: Ally All F→Enc(data) to encrypt the data

i_2: Create role authentication policy—K(key)

i_3: verify all the role access control

Step 5: Create Random (key) for all logs

Step 6: verify all the medical records.

Cloud computing is easy to target. In this proposed model to find the cloud gateway, calculate available storage and nodes for this reason, all users key polices 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 system administrator analyze the log of greatest supposed user. Fig. 2 depicts the proposed system model. The projected scheme can provide an efficient resource allocation, proper response, high QOS economically benefit and elaborate service efficiently.

Algorithm 1: Secure Storage of Files

Input: File

Output: Report

1: Resources: Fog, Cloud Server

2: If (data == Segmented) {

3: AES encrypt the data block

4: Migrate to Cloud Server

5: Server selection for each data

6: Connected enquiry for a group of information

7: Key validation used to access and decrypt

8: Broadcast to a data user

9: for (user=1 to n) {

10: collect data for queries

11:}

Algorithm 1 shows the secure storage of data in the cloud which overcomes in preserving the individual's privacy by segmenting the data and storing it in fog and cloud layer based on the security level. Algorithm 2 shows the computation of execution time which is efficient and achieved low latency, fast response time, minimum computation time and CPU utilization.

Algorithm 2: Estimation of Execution Time

Input: Block size data

Output: data aceess

1: Start

2: Assign index

3: For each input data

4: Calculate execution time

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

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

Where

e_t- Execution time

c_t- Completion time

t - Time is taken

d - Delay

f - Fog nodes

5: return report for n input

6: End

7: End

CloudSim works on multiple platforms including Windows and Linux. The simulation environment uses a system running Windows 7 operating system, Intel Pentium Dual-Core P6000, 1.87 GHz, with 8.0 GB memory and 1 TB hard drive storage. In the simulator, application task parameters include file size, key generation, encryption time, upload time to server, decryption time, CPU usage, and memory consumption. In an area simulating fog node coordinate such as a hospital, the range of fog nodes is defined between 0 and 100. Table 1 shows the analysis report of existing system behavior. Table 2 and Figure 3 describe the proposed system analysis report.

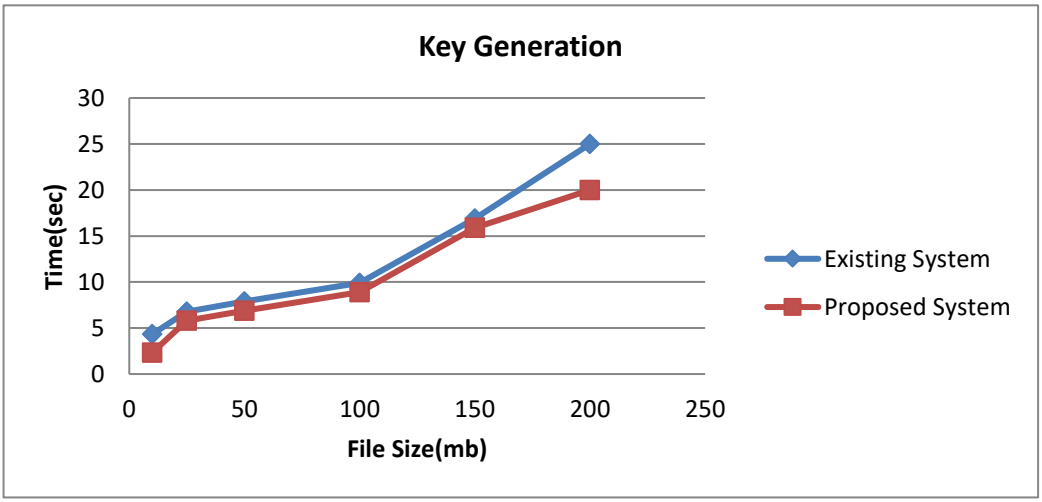
Table 1. Data Analysis Report (Existing Behavior)

File Size (in mb)	Key Generation (in sec)	Encryption (in sec)	Time is taken to upload server (in sec)	Decryption (in sec)	CPU Utilization (in mb)	Memory Consumption (in mb)
10	4.334	4.59	10.8	4.89	14.34	26.9
25	6.789	7.9	14.909	8.899	21.23	34.1
50	7.9	12.008	28.004	10.876	31.19	39.89
100	9.902	22.099	69.892	19.789	51.1	59.37
150	16.906	45.021	79.012	35.038	69.33	70.2
200	25.003	69.091	88.201	49.934	78.567	79.09

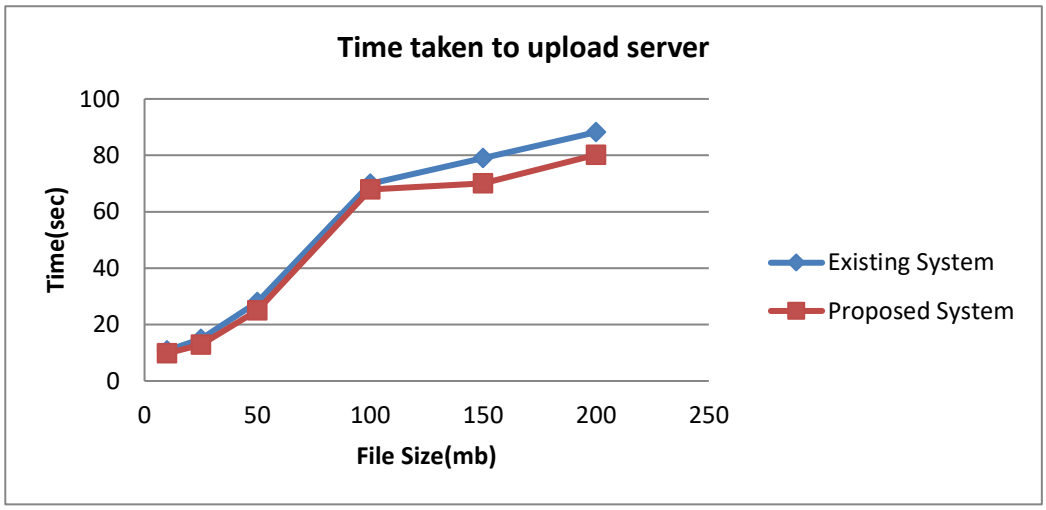
Table 2. Data Analysis Report (Proposed Behavior)

File Size (in mb)	Key Generation (in sec)	Encryption (in sec)	Time taken to upload server (in sec)	Decryption (in sec)	CPU Utilization (in mb)	Memory Consumption (in mb)
10	2.334	3.59	9.8	3.89	12.34	22.9
25	5.789	6.9	12.909	7.899	19.23	29.1
50	6.9	11.04	25.004	9.876	27.19	32.89
100	8.902	19.099	67.892	16.789	48.1	56.37
150	15.906	39.021	70.012	29.038	59.33	64.2
200	20.003	62.091	80.201	45.934	69.567	71.09

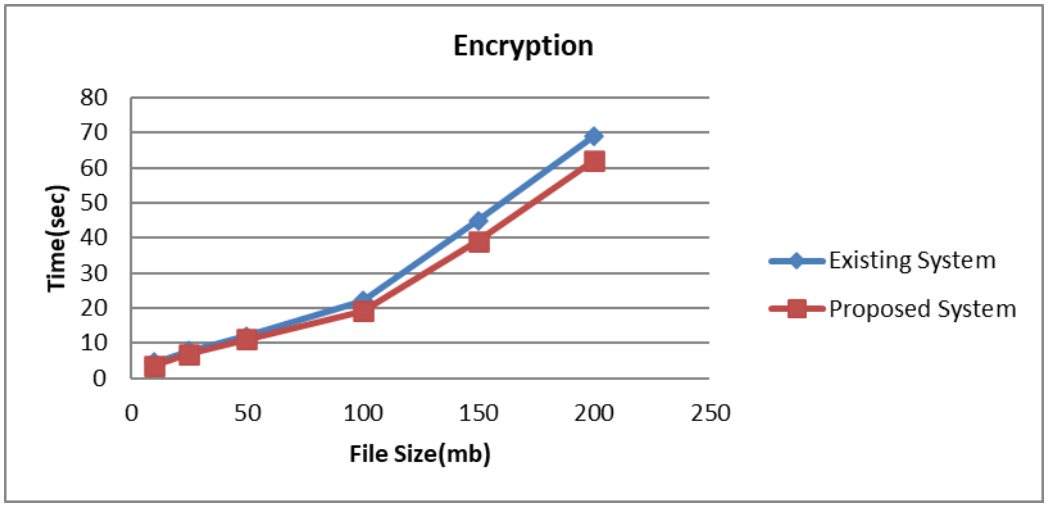
Large-scale configuration tests involve using available computing resources in a simulation environment. We evaluated the processing efficiency of the existing system. First, we measure key generation, encryption time, and then data file upload time between the client and the cloud. We averaged the results from each of the 10 different experiments. The transient performance of the proposed design outperforms the conventional design in all performance metrics. The proposed design performs fog and cloud operations on files with lower total CPU utilization time and client-side integration time with the task server than traditional approaches.



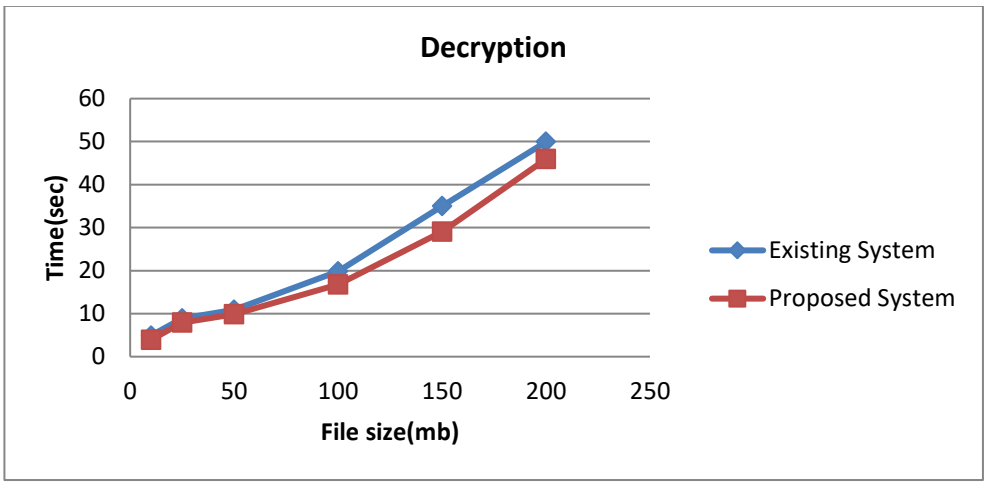
(a) Key Generation



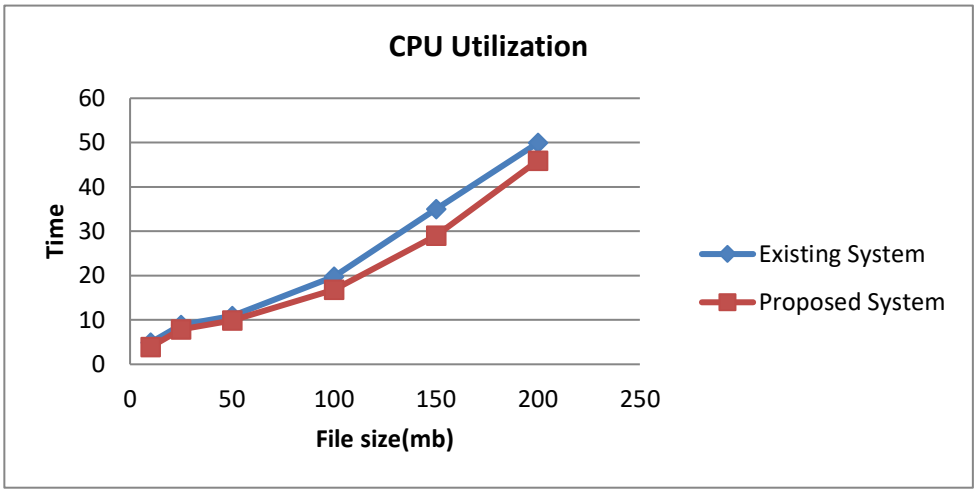
(b) Encryption



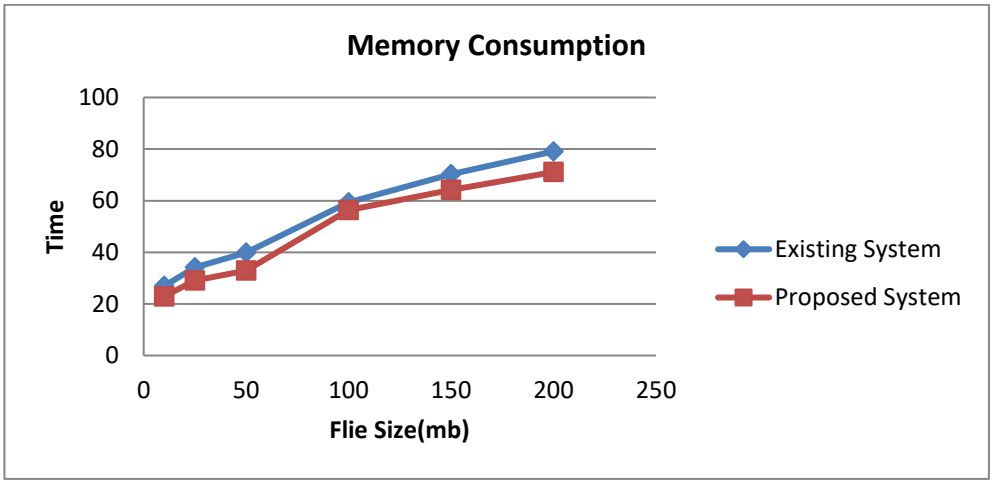
(c) Time taken to Upload server



(d) Decryption



(e) CPU Utilization



(f) Memory Consumption

Fig. 3 Performance of Data Analysis

Nonetheless, we consider that the time of cryptographic activities is nothing more than traditional methods in all cases of file upload/download operations. Also, the transmission time is always lower than the existing design, regardless of the file size. Note that operations for uploading and downloading are asymmetric and use various times to complete the operations. We also mention that when the size of the actual data file content increases the output overhead of the proposed system becomes less important. However, it was on par with the other algorithms when 100 or more tasks were submitted. In this work, it is important to note that the two layers are modeled throughout different environments during testing. The administrator did not directly transfer tasks/data from the terminal layer to the fog layer. This can be considered in future work.

5 Security Concern

A large-capacity cloud masquerading attack on the network. In addition, mimicking man-in-the-middle attacks is a shared authentication protocol, which is a very important security issue whether the attacker tries to serve and mimic end users or fog. To secure data transmission, the key validation proves the security by accessing the cloud servers. To provide a secure cloud, the public key infrastructure must have the keys (encryption and decryption) of the fog and cloud servers it generates to ensure secure communication between the fog and cloud servers. All fog systems will hold their own private keys and other confidential information together so that adversaries cannot access this information. Like a fog device, private key privacy must be maintained by the cloud server. All these private keys are very important, because, it should be pointed out that all these keys should be a secure communication group

session key. If the adversary gets all these keys inexplicably, and then uses the protocol definition, he can get all the communications exchanged through the fragile stream by setting the older session key. Another important parameter of confidentiality with the session key in this regard. For subsequent data exchange, the session key must be obtained using the mutual authentication protocol of the session key encrypted by the data exchanged between the entities. The data integrity concept proof message is basically obtained from the sender by the receiver-end to send the same message. It has been operated by some researchers and is striving to achieve high integrity rights. The problem with open research on the cloud computing fog model is our greatest ability, still high credibility and the complexity of success. The Intrusion Detection System (IDS) is also essential for protecting the security of cloud servers, as it provides security against internal attacks, denial of service attacks, port scan attacks and flood attacks. Malicious users can send beneficiaries of irrelevant information during communication, and DoS and DDoS attack attacks performed by flood recipients that can generate data. Therefore, it is very necessary and important for fog equipment to introduce IDS technology to track and identify destructive activities through log file evaluation, user information, access control strategies, etc. There are also several available algorithms for building IDS, but there is no quality efficiency.

2. Conclusion and future scope

As the healthcare industry continues to evolve within the digital landscape, the imperative for securing sensitive medical data has never been more pronounced. The proposed Unification of Fog-Cloud Computing for Data Agitation and Guard Intensification (DA-GI) system presents a forward-thinking solution, capable of addressing prevalent security threats while enhancing the overall efficiency of healthcare data management. By leveraging the strengths of fog and cloud architectures, implementing robust encryption protocols, and sustaining rigorous access controls, the DA-GI system aims to establish a reliable framework for safeguarding Medical Data Health-Care records and fostering greater trust in the healthcare sector's digital transformation. As technology continues to advance, the ongoing development and refinement of such security solutions will be vital in protecting patient data in an increasingly interconnected world.

Reference

[1] Prosper Chemouil, Pan Hui, et al, Special Issue on Artificial Intelligence and Machine Learning for Networking and Communications, IEEE Journal on Selected Areas in Communications. 37 (6) (2019) 1185-1191.
[2] Murk, AsadWaqar Malik, Imran Mahmood et al, Big Data in Motion: A Vehicle Assisted Urban Computing Framework for Smart Cities, Special Section on Urban Computing and Well-being in Smart Cities: Services, Applications, Policymaking Considerations. 7 (2019) 55951-55965.
[3] Cong Wang, Chow, Kui Ren and Wenjing Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers. 62 (2) (2011) 362-375.
[4] Fei Zhang, Guangming Liu, Xiaoming Fu and RaminYahyapour, A survey on virtual machine migration: challenges, techniques, and open issues, IEEE Communications Surveys & Tutorials. 20 (2) (2018) 1206-1243.
[5] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21
[6] ZhenyuZhuo, Pengju Liu, Junhao Feng, Yan Zhang, ShahidMumtaz& Jonathan rodriguez, Computation Resource Allocation and Task Assignment Optimization in Vehicular Fog Computing: A Contract Matching Approach. IEEE transactions on vehicular technology. 68 (4) (2019) 3113-3125.
[7] Zhaolong Ning, Jun Huang, and Xiaojie Wang, Vehicular Fog Computing: Enabling Real-Time Traffic Management for Smart Cities. IEEE Wireless Communications. 26 (1) (2019) 87-93.
[8] Intrusio Detection in a Cloud Computing Environment. Available at: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment (2012).
[9] Hongchen Wu, Mingyang Li, and Huaxiang Zhang, Enabling Smart Anonymity Scheme for Security Collaborative Enhancement in Location-Based Services. IEEE Translations and content mining. 7 (2019) 50031-50040.
[10] Sonya, A., & Kavitha, G. (2022). A Data Integrity and Security Approach for Health Care Data in Cloud Environment. Journal of Internet Services and Information Security, 12(4), 246-256.
[11] PreetiMishra, Emmanuel S.Pilli, VijayVaradharajan and UdayaTupakula, Intrusion detection techniques in a cloud environment: A survey. Journal of Network and Computer Applications. 77 (2017) 18-47.
[12] Cheng, J., Li, M., Tang, X., Sheng, V.S., Liu, Y., and Guo, W., Flow correlation degree optimization driven random forest for detecting DDoS attacks in cloud computing. Journal of Security and Communication Networks. ID 6459326

(2018) 1-14.
[13] Xiaowei Chen, Songtao Tang, Jiu Wu, et al, IDISC: A New Approach to IoT-Data-Intensive Service Components Deployment in Edge-Cloud-Hybrid System. Special Section on Data Mining for the Internet of Things. 7 (2019) 59172-59184.
[14] Xuyun Zhang, Yuan Yuan, Zhili Zhou, Shancang Li, Lianyong Qi and Deepak Puthal, Intrusion Detection and Prevention in Cloud, Fog and Internet of Things. Security and Communication Networks. ID 4529757 (2019) 1-4.
[15] Mohamed, K.N.R., Nijaguna, G.S., Pushpa, Dayanand, L.N., Naga, R.M., & Zameer, AA. (2024). A Comprehensive Approach to a Hybrid Blockchain Framework for Multimedia Data Processing and Analysis in IoT-Healthcare. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 94-108. https://doi.org/10.58346/JOWUA.2024.I2.007
[16] LingjuanLyu, JiongJin, SutharsanRajasegarar, Fog-Empowered Anomaly Detection in IoT Using Hyperellipsoidal Clustering. Journal of IEEE Internet of things. 4 (5) (2017) 1174-1184.
[17] RehmatUllah, Muhammad Atif Ur Rehman and ByungSeo Kim, Design and Implementation of an Open-Source Framework and Prototype for Named Data Networking-Based Edge Cloud Computing System. IEEE Translations and content mining. 7 (2019) 57741-57759.
[18] Luca Cerina, Sara Notargiacomo, Matteo Greco and Luca Paccani, A Fog-Computing architecture for Preventive Healthcare and Assisted Living in Smart Ambients. IEEE Access (2017).
[19] Sandeep K.Sood and Isha Mahajan, A Fog-Based Healthcare Framework for Chikungunya. IEEE Internet of Things Journal. 5 (2) (2018) 794-801.
[20] Junaid Chaudhry, KashifSaleem, Rafiqul Islam and Ali Selamat, AZSPM: Autonomic Zero-Knowledge Security Provisioning Model for Medical Control Systems in Fog Computing Environments. IEEE 42nd Conference on Local Computer Networks Workshops. (2017) 121-127.
[21] Wenjuan Tang, Kuan Zhang, Ju Ren, Yaoxue Zhang, and Xuemin Shen, Lightweight and Privacy-preserving Fog-assisted Information Sharing Scheme for Health Big Data. IEEE Access (2017).
[22] Thaha Muhammed, Rashid Mehmood, AiiadAlbeshri and IyadKatib, UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities. Special Section on Big Data Learning and Discovery, IEEE Access. 6 (2018) 322528-322585.
[23] Ata Ullah, IqraSehr, Muhammad Akbar and Huansheng Ning, Fog Assisted Secure De-Duplicated Data Dissemination in Smart Healthcare IoT. IEEE International Conference on Smart Internet of Things. (2018) 166-171.
[24] FuhongIin, Yutong Zhou, Ilsun You et al, Content Recommendation Algorithm for Intelligent Navigator in Fog Computing Based IoT Environment. Special Section on Collaboration for the Internet of Things, IEEE Access. 7 (2019) 53677-53686.
[25] Wu Yang, Siyi Liao, Jianhua Li, Jun Wu, and Zhitao Guan, Fog Enabled Vehicle as a Service for Computing Geographical Migration in Smart Cities. Special section on emerging technologies on the vehicle to everything (v2x). 7 (2019) 8726-8736.
[26] JongGwanAn, Wenbin Li et al., EiF: Toward an Elastic IoT Fog Framework for AI Services. IEEE Communications Magazine. 57 (5) (2019) 28-33.
[27] ProsantaGope, Jemin Lee, Ruei-Hau Hsu, and Tony Q.S.Quek, Anonymous Communications for Secure Device-to-Device-Aided Fog Computing. IEEE Consumer Electronics Magazine. 8 (3) (2019)10-16.
[28] Vaishnavi, S., Sethukarasi, T. SybilWatch: a novel approach to detect Sybil attack in IoT based smart health care. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02189-3
[29] Karthigaiveni, M., Indrani, B. An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card. J Ambient Intell Human Comput (2019). https://doi.org/10.1007/s12652-019-01513-w
[30] Sheng Zhou, Zhiyuan Jiang and ZhishengNiu, Exploiting Moving Intelligence: Delay-Optimized Computation Offloading in Vehicular Fog Networks. IEEE Communication Magazine. 57 (2019) 49-53.