AN IMPROVED SECURITY FRAMEWORK IN HEALTH CARE USING HYBRID COMPUTING

B. S. Kiruthika Devi[1*], V Vijayakumar[2], G Suseela[3], B. Prabhu Kavin[4], S. Sivaramakrishnan[5], Joel J. P. C. Rodrigues[6]

[1]Research Mentor, Kakinada Area ,CL Educate Ltd., New Delhi 110044, India

[2]Professor, Universidade Federal do Piaui, Brazil

[3]School of Computing, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Tamilnadu, India

[4]Computer Science and Engineering, Sri Ramachandra institute of Higher Education and Research and Technology, Porur, Chennai, Tamilnadu, India

[5]Department of Electronics & Communication Engineering, Dayananda Sagar University, Bangalore, Karnataka, India

[6]Senac Faculty of Ceará, Fortaleza - CE, Brazil

[6]Instituto de Telecomunicações, Covilhã, Portugal

Email: bskiruthikadevi@gmail.com[1]* (corresponding author), viji_06@yahoo.com[2], suseelag@srmist.edu.in[3], prabhukavin@sret.edu.in[4], sivaramkrish.s@gmail.com[5], joeljr@ieee.org[6]

DOI: https://doi.org/10.22452/mjcs.sp2022no1.4

ABSTRACT

Cloud computing is a new category of service that gives each customer access to a large-scale computing network. Since most cloud computing platforms provide services to a large number of people who aren't considered to be trustworthy, various cyber attacks may potentially target them. As a result, a cloud computing system must provide a security monitoring mechanism to protect the Virtual Machine from attacks. In this case, there is a tradeoff between the security level of the security system and its performance. If we need strong security, we'll need more laws or patterns, which means we'll need a lot more computational resources in proportion to the strength of security. As a result of the declining number of resources allocated to customers, we will add a new protection scheme in cloud environments to the VM in this report. Hence, the proposed system Proposed Elliptic curve – Diffie Hellman EC(DH)2 Algorithm is designed and deployed to improve the security in healthcare domain using hybrid computing. The most popular and recent technologies such as cloud computing and fog computing are integrated to explore data movement and stable medical data health-care information. Based on the experimental results, it is inferred that the proposed system offers high security and less operating time while handling the data making its deployment in the healthcare domain.

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

1.0 INTRODUCTION

Cloud computing is a form of computing that focuses on dedicated server or smart device application management and machine learning tools as well. Cloud computing is categorized as public, private, or hybrid depending on the physical location of computer services and who has access to them. Usually, cloud services are introduced based on the needs of the end user. Remote software access and web service-based functionality are supported by SaaS. Another service that is provided as a device is PaaS(Platform as a Service). The computer is subcontracted to purchase and manage its own hardware and software layers instead of a business or data center [1]. Businesses that prefer the simplicity of having their IT infrastructure operated by a cloud provider prefer IaaS. The business will benefit from cloud computing in a variety of ways. It is also easier to access data with the growing number of cloud-enabled devices used in modern business settings (such as smartphones and tablets) [2].

Cloud computing security includes a broad range of programs, technologies, applications, and regulations aimed at safeguarding intellectual property, data, applications, facilities, and related infrastructure in virtualized cloud

computing. Cloud computing is superior in security when compared with legacy computing. It is also cost efficient, controllable, and reliable. Yet it suffers with following security issues such as insider theft, data breaches, data loss, poorly secured APIS, Vendor lock –in, lack of control etc.

Cloud protection is introduced using cloud platforms or existing cloud-based security solutions. The implementation of a cloud protection framework should be a shared endeavor between the company owner and the solutions provider. Cloud security is a must for companies making the transition to the cloud. Security threats have developed and become more complex, and cloud infrastructure is no less fragile than an on-site economy. As a consequence, partnering with a cloud provider that provides best-in-class protection that is tailored for services is important [3].

A computer simulation or replication is referred to as a virtual machine. To run on a computer, a Virtual Machine makes use of Virtualization Software. Both virtualization and the cloud depend on abstract tools to create functional environments. Virtualization, on the other hand, is a technology that allows multiple virtual worlds or dedicated resources to be generated from a single hardware system, while clouds are IT areas that abstract, pool, and begin sharing scalable resources across a system. Self-service power, distributed network scaling, and scalable resource pools are the features that set cloud computing apart from traditional virtualization [4].

Fog is a cloud computing extension that consists of several nodes connected to physical devices directly. Fog computing serves as a conduct between the remote servers and the hardware. This determines what data should be sent to the registry and what data can be processed locally. As a result, Fog is a smart portal that defers data storage, processing ,and analysis to the cloud, allowing for more efficient data storage, processing, and analysis. Fog is a more stable network than the cloud because of its decentralized architecture.

Fog computing can be seen as referring critically to the growing difficulties in accessing information in large cloud systems based data structures[5]. The widely used data encryption algorithm in the literature of secured cloud computing are based on AES (Advanced Encryption Standard), DES (Data Encryption Standard) and RSA (Rivest Shamir Adleman). The AES based security management systems are computationally intensive and hence forth associated cost of encryption is high. The DES based systems are susceptible to brute force attacks. The RSA based security systems are slower as it consumes more time in key generation.

As a result, a detailed discussion of security solutions could improve this work. The security aspects of data security are addressed in personal computers and information analysis in the cloud. This work makes a contribution by presenting various data encryption algorithms in hybrid computing for rigid health care systems. As previously stated, this research differs from other recent security methods. It provides as much detail as previous works. Section II reviews the background and related works in the literature. Section III justifies the necessity for hybrid computing in health care applications. Section IV describes the proposed system model and encryption algorithm. Section V discusses the simulation results and performance analysis with existing security methods followed by conclusion in Section VI.

2.0 RELATED WORK

Since cloud computing design architecture varies from conventional computing methods such as grid computing, the implementation of previously established Intrusion Detection / Prevention Systems (ID / PS) in cloud computing cannot achieve the desired level of safety and performance. The growing demand for cloud services from its users necessitates the creation of an optimal framework for securing resource requirements, as intruders can manipulate cloud resources and damage the information stored there. Centered on theoretical contract modeling, an active compensation system is proposed. The agreement seeks to optimize the base station's anticipated utility for each type of vehicle's distinguishing feature. The problem of task assignment is then viewed as a two-sided problem, i.e. vehicle and user equipment matching [6]. By using traveling and pedestrian crosswalks as fog nodes, the VFC (Vehicular Fog Computing) enabled offloading system is built-up as an optimized solution. The delineation is validated by a real-world taxi trajectory based reliability assessment. The research concerns and problems that exist in VFC-enabled traffic management are reviewed and addressed [7].

The IDS can be deployed in the cloud at a number of sites, including network borders, servers, virtual machines (VMs), and hypervisors, as well as across all cloud regions. The detection approach used by IDS to alarm and alert are categorized as1. signature-based, 2. anomaly-based, or 3. hybrid. To boost signature-based or abnormally-based IDS accuracy, soft computational methods such as Support Vector Machines (SVM), Fuzzy Reasoning, Convolutional Neural Systems (RNN), Association rules, and Genetic and Evolutionary Algorithms or as a hybrid combination of all of these are used.IDS are intrusion detection systems that log information and carry out

predefined procedures. These can be hardware or software, and they can contain whole machine entities that have been observed. There are three types of IDS in cloud computing systems: host-based IDS, network-based IDS, and distributed IDS. Safety is crucial in this modern age of on-demand cloud computing. The cloud computing environment, has rich literature in intrusion detection system to detect invasions. The majority of them include a study of conventional strategies for detecting anomalies and detecting misuse [8].

The investigative portion can be retained outside the VM on a hypervisor and this technique is called as Virtual Machine Introspection (VMI). VMI techniques are very useful in detecting various stealth attacks that focus users and kernel based processes or tasks executing on VMs. Hypervisor Introspection (HVI) techniques maintain the hypervisor's protection and mitigate forthcoming attacks on virtual machines (VMs) running over them from a suspicious compromised hypervisor. Introspection techniques analyze the hypervisor by employing integrated hardware-assisted and virtualization-enabled technologies. The primary aim is to conduct a thorough literature review of various possible cloud environment Intrusion Detection techniques, as well as an evaluation of their ability to detect attacks.

A risk model and taxonomy attack are provided to elucidate the vulnerabilities in the cloud. Researchers will be able to release and immerse themselves in cloud-based Intrusion Detection approaches as a result of this work [9]. DDoS attacks have caused substantially vandalized cloud computing, also rate of failures of current DDoS attack detection approaches are comparatively large in cloud environments. The improved Random Forest (RF) developed using genetic algorithm based on the Flow Correlation Degree (FCD) function is proposed in this paper as a tool for spotting DDoS attacks. The FCD definition is based on asymmetric and semi-directivity interaction characteristics, and it uses the Bi -tuple FCD function of Packet Statistical Degree (PSD) and Semi Directivity Interaction Anomaly (SDIA) to describe the characteristics of typical flow and attack flow. Then, using sequences, an FCD-based genetic algorithm optimizes the RF's two key decision tree parameters: maximum number of decision trees for each decision tree and maximum depth [10].

As a whole, the Internet of Things (IoT) along with cloud-based fog computing principles provide computational facilities for a wide variety of knowledge and computing intensive applications. Fog computing conveniences can provide computing resources close to IoT devices where evidence is generated, allowing for high bandwidth processing for real time and time bounded critical applications while reducing the amount of data sent to the cloud for storage [11]. Because of more advanced data mining technology, cloud computing systems may be able to provide large-scale cloud storage and computing services for inexpensive long-term storage or data-intensive analytics. These cutting-edge computing facilities, however, still faces significant security and privacy threats due to their inherent built-in properties, such as cloud computing's omnipresent access and multitenancy capabilities or IoT devices' limited computing capacities [12].

Fog-Empowered anomaly detection is a modern anomaly detection technique that uses a strong hyper ellipsoidal clustering algorithm to take advantage of the Fog computing platform [13]. Based on the configuration of the Field Programmable Gate Array (FPGA) [14], an edge node is proposed. The hardware of an FPGA node can be reconfigured to provide maximum task efficiency, minimal delay, or the ability to scale the number of connected devices with minimal power consumption [15]. This virus can be monitored and avoided using a cloud-based, fog-based healthcare system. A decision tree is initially used to assess the user's infection category based on their health concerns and clinical alerts [16].

Using dynamically built atomic safety elements; it is proposed to create a security provisioning template for medical devices in fog environments. For security purposes, calculating the processor clock cycles from the running of the software on the occupant computing platform will check the atomic elements' reliability [17]. A fog-assisted information sharing platform for health big data is proposed to be lightweight while still protecting privacy. Fog computing, in particular, is incorporated into the e-healthcare framework to reprocess existing health data and boost personal data processing efficiency [18].

With three main components and several levels, the network service quality has improved: Big Data, Machine Learning, and High-Performance Computing Computers are used to forecast network traffic, which is then passed on to cloud and network layers in order to optimize link rates, data storage, and route decisions[19].Using network edge Fog servers, a Secure De-duplicated Data Dissemination (S-DDD) scheme for healthcare IoT is proposed. To eliminate redundancy and define the cut-point between two windows, a lightweight de-duplication mechanism based on the Adaptive Chunking Algorithm (ACA) is also proposed [20].A vehicle-based geographic migration model of the vehicle computing resource is being developed for fog computing-enabled smart cities. The vehicle pushes the boundaries of the disparity and sophistication of vehicle computing resources as a network platform, improving the

versatility of conventional cloud services architecture. To balance resource use and spread machine resources internationally, an incentive scheme is proposed that uses resource pricing to control vehicle route choice [21, 22]. However, certain strategies are only useful in such cases. Initiatives and work to integrate such critical innovations are still in their infancy. By integrating IoT, fog computing, and AI, this article aims to find a convergence way to address the existing limitations [23].

In summary, the related work addresses the security system that need to be deployed within the cloud computing environment. The fog computing is also the most emerging area and the focus is given on the functionality of the computing facilities. But, the focus on the data security using cryptographic algorithms is inevitable in the hybrid computing. By addressing the security, users are provided with high quality of services in health care infrastructure without any delay or processing overhead. The proposed system provides improved security for health care domain using hybrid computing. But doing so, the resources are energy invested is saved and the users are provided with best effort solutions.

3.0 NEED FOR HYBRID COMPUTING IN HEALTH CARE

The cloud is facing various challenges in operating critical/sensitive data, particularly health care data. The issues experienced are data transmission, delay and unavailability of services [26]. In health care domain, even minimum delay can lead to causalities. For addressing these issues, the recent technology called the fog computing is embedded between IoT and cloud network. Based on the situation, fog and cloud computing are used interchangeably. For emergency conditions, the sensed information is processed through fog computing and aids in successful data transfer with minimal delay. By using this hybrid computing, the performance of the infrastructure is enhanced manifolds. The jitter, delay and cost involved in operating the nodes are reduced at the greater extent. Further, application delivers its services with high availability and consistency.

4.0 PROPOSED HYBRID MODEL

Fog computing is a distributed computing model that stretches to the edge of an organization's processes. Haze figuring, also known as Edge Registration or Hazing, enables process activity, processing, and system management between end devices and distributed server farms. Knowledge can be prepared much more effectively when working with these administrations at the edge of the system that make up the Internet of Things (IoT) than if it had to be sent to the cloud for processing. Waste of money, lack of proper response, increased expenditure, and a lack of QOS are all disadvantages of the current system.

In cloud computing, a multi-level intrusion detection framework is a platform for implementing active IDS. By applying differential level of protection based on the degree of anomaly to users, the multi-level IDS approach leads to the most effective use of resources. By deploying multi-level IDS and handling anomaly level use rlogs per community, the proposed approach improves cloud computing system resource availability and addresses potential threats [24].Fog devices do a lot of computing, storage, local communication, and backbone routing on the internet. This connects the system's sensors to the cloud server.

Usually, this functionality is built into a gateway system that links all sensors and manages cloud connectivity. The gateway system must have reliable data storage and processing power in order to handle multi-sensor data. IoT technologies are used in a fog-assisted data model to provide healthcare as a cloud service. As devices and software handle private information and present healthcare data, the IoT healthcare domain may be a target for an intruder.

To achieve corresponding services, the emphasis is on confidentiality, honesty, authentication, availability, durability, and fault tolerance. Since files can be transmitted over a communication link, sensors are constantly collecting important data and sending it to a private server to connect the IoT device to cloud storage during this process. It performs simple data processing and aggregation, resulting in consistent signals that can be sent to subscribing entities for notification or to transfer the data to the cloud for further review and personality sharing through healthcare.

In the data center, tasks such as sorting, storing, and analyzing patient health data obtained from the IoT subsystem are performed. In application, data-driven patient evaluation and intervention takes place. A doctor, an emergency management service, a medical testing facility, and health practitioners are all present. At the control center, a significant number of individuals are involved in clinical observation, patient diagnosis, and intervention processes [26][27][29]. Furthermore, the control center manages all requests for patient data access. Registered users who

want sensor data must use the surveillance center to send a data proposal to the cloud. When the requested data is available in the sensor's data storage, the data will be returned to the user.

Key findings of the proposed system

- An enhanced security mechanism is proposed for healthcare using hybrid computing.
- The execution time is less compared to the existing algorithms and this hybrid computing provides high availability of services.
- The hybrid computing is more suitable for health care applications and provide services without any processing delay and jitter.

4.1 HYBRID ALGORITHM

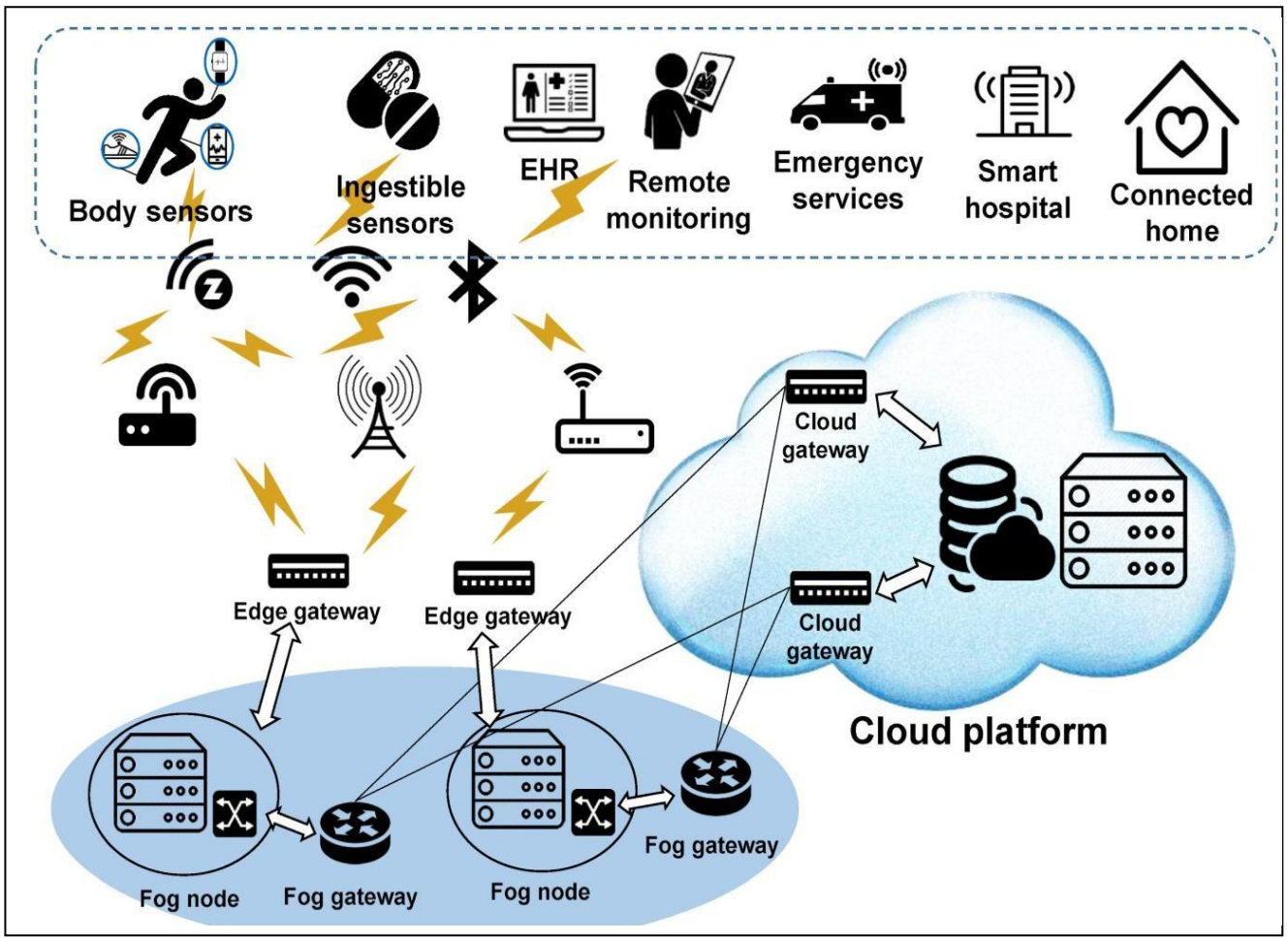

Fig. 1: Architecture of cloud and fog based secure IoT environment

Step1: Fog cloud gateway, data storage, and fog server are the three parameters that built fog focuses on. A total of 100 fog nodes are formed.

Step 2: Since fog nodes can hold several tasks at once, the completion time is the time it takes for the longest-running task to complete. The fog node and delay d can be used to define the execution time t and delay d of a task T as in Equation 1:

$$t = \max \sum t, i \epsilon N, t(T,F) < d, \quad x=1 \qquad (1)$$

Step 3: Cloud Initialization: First, initialize servers for request and response in cloud platform is done.

Step 4: Initialize servers for request and response in the cloud platform during cloud initialization. F may be used to describe files that need to be moved in a safe manner for the medical field.

Step 5: For every IoT communication, Encrypt F at the sender (s) and decrypt (d) at the recipient. Database audits are conducted on a regular basis. Keep a record of your activities.

Step 6: Step 5 is repeated until the simulation is complete.

Step 7: Monitoring center maintains risk table and health record.

The proposed Elliptic Curve, Diffie-Hellman EC(DH)2 technique provides enhanced security of health records stored in cloud server [30]. The elliptic curve cryptography (ECC) is used initially for encryption and Diffie-Hellman method is applied twice for improving the security level of the data. The main objective of using EC (DH)2 is to share the dynamic key among the cloud clients. ECDH helps in user authentication in a secure way as the key plays a vital role in the secure transmission.

Hence, in the proposed system, elliptic curve cryptography is coupled with Diffie-Hellman method. Once the base point is generated, the keys are generated for authentic users. ECC is a method of encryption which converts the given data into unknown data for data protection. A secret is key is utilized by the data owner to encrypt the data intended to protect. The ECC algorithm is better in comparison with RSA and the major incentives in choosing ECC are low processing overhead, resource saving and fast computing capability.

Step 1 Do the key exchange process using Diffie-Hellman

Step 2 Select the elliptic curve using the following equation,

$$y^2 = x^3 + ax + b \qquad (2)$$

Step 3 Find the base point E = (X1, Y1) such that mE = O.

Step 4 Select the private keys for users A & B $m_A < m$, $m_B < m$.

Step 5 Evaluate the public keys using the following equations

$$PK_A = m_{AB}, \qquad (3)$$

$$PK_B = m_{BE}. \qquad (4)$$

Step 6 Select the shared key using the following equation

$$SK = m_A PK_B, \qquad (5)$$

$$SK = m_B PK_A. \qquad (6)$$

Cloud computing is a straightforward target to reach. As a consequence, all users and administrators can be considered possible attackers, and all traffic can be subjected to strict security measures. As a consequence, it is advantageous to all. This approach also supports anomaly-level log classification, so system administrators must first review the log of the most suspicious user. The proposed device model is shown in Figure 1.

5.0 RESULTS AND DISCUSSIONS

The proposed system will efficiently distribute resources, react appropriately, provide high QOS at a low cost, and provide elaborate service. Cloud Sim can run on a number of platforms, including Windows and Linux. File Size,

Key Generation, Encryption time, Time to Upload Server, Decryption time, CPU Usage, and Memory Consumption are among the device task parameters in the simulator. The coordinates of fog nodes in an environment, such as a hospital, are simulated, and the range of fog nodes in 0 to 100 is reduced. The research summary of current device activity is shown in Table 1. The proposed system's study report is shown in Table 2 and Figure2-5.

The availability of computational resources for use in a simulation environment is needed when experimenting with large-scale structures. We assessed the current system's implemented performance. We begin by testing key generation, encryption time, and data file uploading time between client and cloud. Over the course of ten different experiments, we combine the results of each measurement. The proposed design outperforms the traditional design in all output metrics in terms of time.

The proposed design's total Processor utilization time for conducting Fog and Cloud operations on the file, as well as the time for the client to coordinate server activity, are both less than traditional method. The existing systems used RSA algorithm. The recent work on modified RSA public key security system proposed by Kumar et al [31] has been considered for comparison and performance analysis of the proposed Hybrid model. The proposed system provides lesser processing time when compared to the existing system. From Table 1 it is been observed that the proposed EE(DH)2 security system out performs the existing system [32].

Table 1: Data analysis report

Parameters	**File Size (in mb)**	**Existing system**	**Proposed system**
Key Generation (in secs)	25	4.334	2.334
	50	7.9	6.9
	75	9.902	8.902
Encryption (in secs)	25	4.59	3.59
	50	12.08	11.04
	75	22.09	19.09
Uploading (in secs)	25	10.8	9.8
	50	28.004	25.004
	75	69.892	67.892
Decryption (in secs)	25	8.899	7.899
	50	10.876	9.876
	75	19.789	16.789

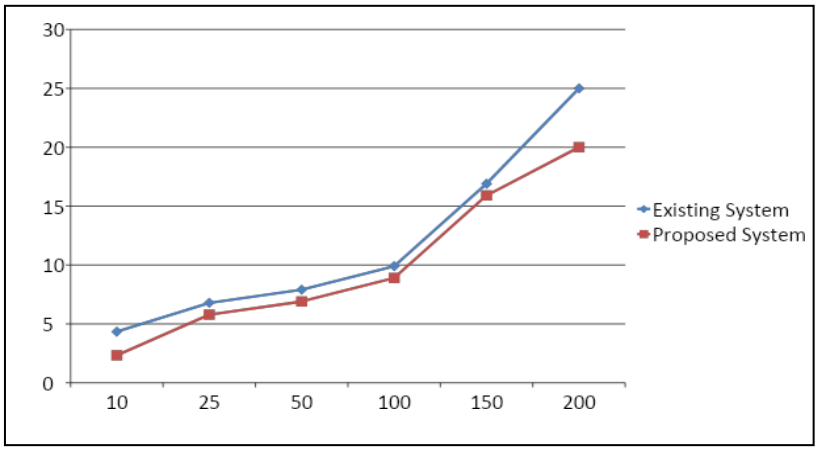

Fig. 2: Key Generation Time: RSA Vs Proposed EC(DH)^2

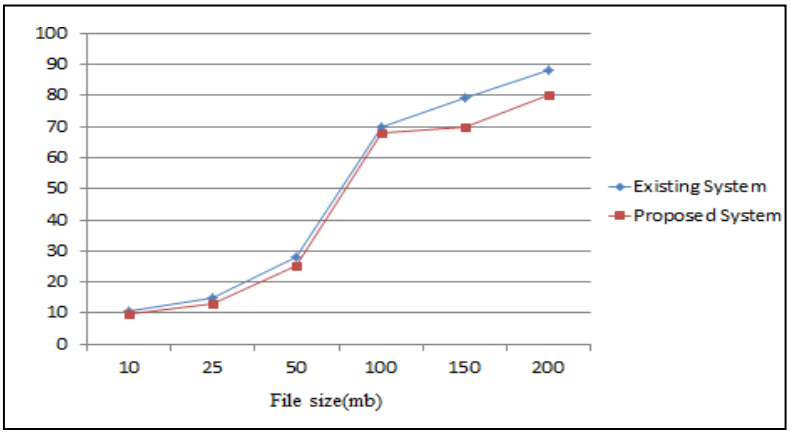

Fig. 3: Encryption Time : RSA Vs Proposed EC(DH)^2

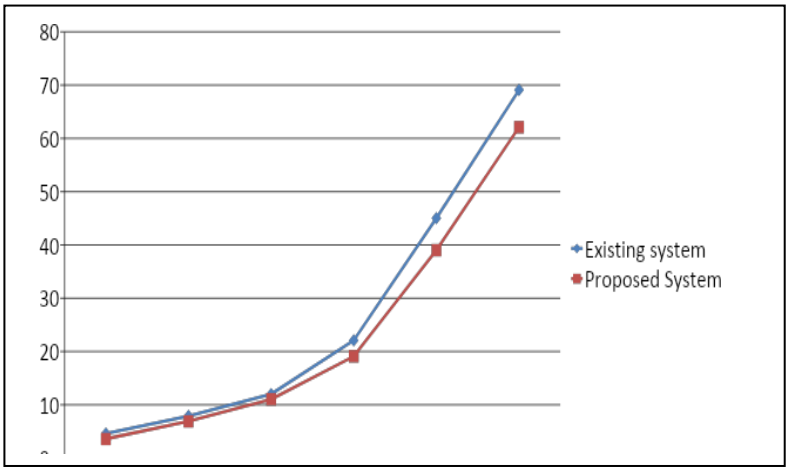

Fig. 4: Uploading Time: RSA Vs Proposed EC(DH)^2

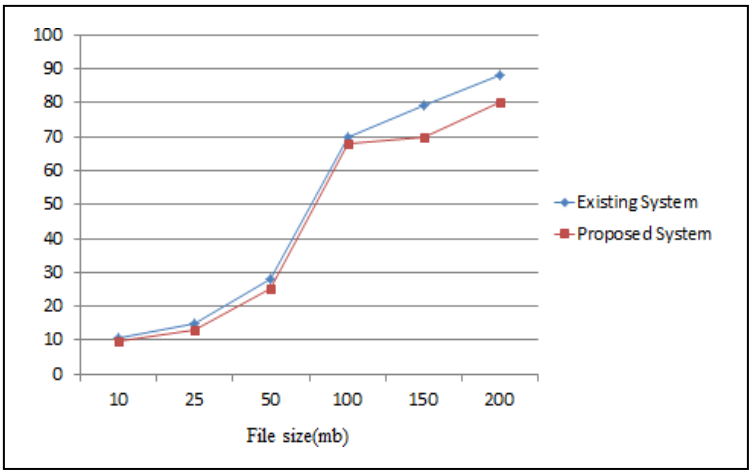

Fig. 5: Decryption Time: RSA Vs Proposed EC(DH)[2]

Nonetheless, we believe that in all cases of file upload / download operations, the time spent on cryptographic activities is no more than that spent on traditional methods. In addition, regardless of file size, transmission time is often faster than current design. It's worth noting that the uploading and downloading operations are asymmetric and take different amounts of time to complete. We also mention that as the size of the actual data file content grows larger, the proposed system's output overhead becomes less significant. When 50 or more tasks were submitted, it was on par with the other algorithms. It's worth noting that the two layers are modeled in different environments during testing in this study. The tasks/data were not moved directly from the terminal layer to the fog layer by the administrator. This may be considered in future study.

Figure 6 shows the execution time of the proposed algorithm against the other traditional algorithms such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard) used in existing systems. It is inferred from the figure that, proposed algorithm provides lesser time in comparison with other algorithms for different file sizes. Thus, enhanced security is achieved in the hybrid computing with less execution time and high security.

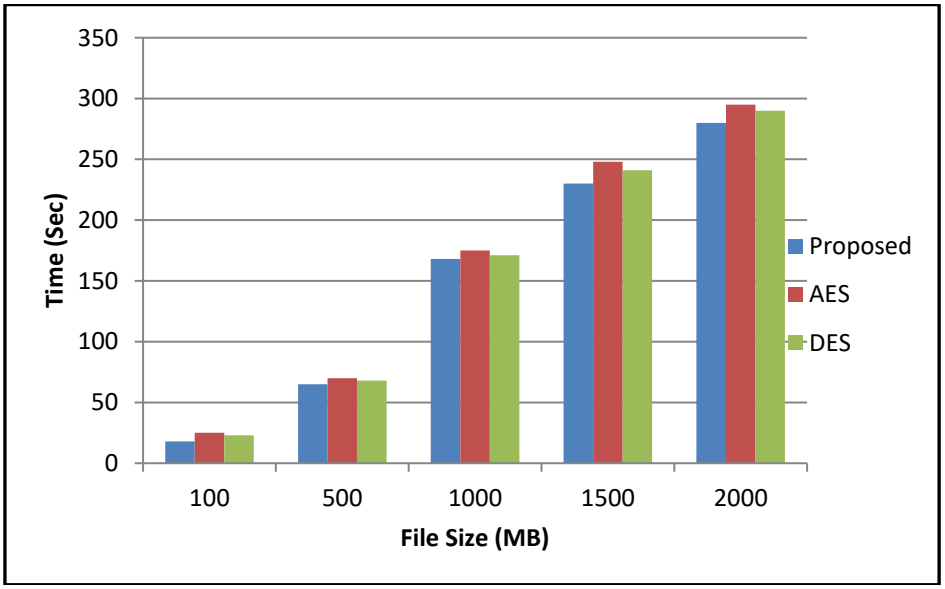

Fig. 6: Execution time against the existing algorithms

6.0 CONCLUSION

Cloud-based IoT applications and trends are evolving in the healthcare domain, due to the growth of IoT and cloud computing. The issue is how to integrate cloud-based IoT and fog computing into the healthcare system in the coming decade. In this communication, cloud and fog computing techniques were combined to examine data movement and secure medical healthcare information. The proposed EC(DH)2 algorithm provides enhanced security and the execution time is less when compared to the existing methods. Thus the experimental results prove that the cryptographic methods are most suitable in hybrid computing and its application in health care domain is inevitable. In future the proposed system will be tested with parallel computing environment to reduce the work load at the cloud server. The proposed system paves way for future energy saving solutions in hybris computing for health care.

6.0 ACKNOWLEDGEMENT

This work is partially funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the Project UIDB/50008/2020; and by Brazilian National Council for Scientific and Technological Development - CNPq, via Grant No. 313036/2020-9.

REFERENCES

[1] P. Chemouil et al., "Special Issue on Artificial Intelligence and Machine Learning for Networking and Communications", *IEEE Journal on Selected Areas in Communications*, Vol. 37, No.6, 2019, pp. 1185-1191.

[2] A. W. Malik et al., "Big Data in Motion: A Vehicle-Assisted Urban Computing Framework for Smart Cities", *IEEE Access*, Vol.7, 2019, pp. 55951-55965.

[3] C. Wang et al., "Privacy-preserving Public Auditing for Secure Cloud Storage", *IEEE Transactions on Computers, Vol.* 62, No.2 , 2011, pp. 362-375.

[4] F. Zhang et al., "A Survey on Virtual Machine Migration: Challenges, Techniques, and Open Issues*", IEEE Communications Surveys & Tutorials*, Vol. 20, No.2, 2018, pp. 1206-1243.

[5] S. Zhou et al., "Exploiting Moving Intelligence: Delay-optimized Computation Offloading in Vehicular Fog Networks", *IEEE Communications Magazine*, Vol. 57, No.5, 2019, pp. 49-55.

[6] Z. Zhou et al., "Computation Resource Allocation and Task Assignment Optimization in Vehicular Fog Computing: A Contract-Matching Approach", *IEEE Transactions on Vehicular Technology* , Vol.68, No.4, 2019, pp. 3113-3125.

[7] Z. Ning, et al., "Vehicular Fog Computing: Enabling Real-time Traffic Management for Smart Cities*", IEEE Wireless Communication*, Vol. 26, No. 1, 2019, pp. 87-93.

[8] P. Cox., "Intrusion Detection in a Cloud Computing Environment", 2012.

[9] H. Wu et.al., "Enabling Smart Anonymity Scheme for Security Collaborative Enhancement in Location-Based Services", *IEEE Access*, Vol. 7, 2019, pp. 50031-50040.

[10] P. Mishra, Preeti et al. "Intrusion Detection Techniques in Cloud Environment: A Survey*", Journal of Network and Computer Applications*, Vol. 77, 2017, pp. 18-47.

[11] J. Cheng et al., "Flow Correlation Degree Optimization Driven Random Forest For Detecting DDoS Attacks in Cloud Computing", *Security and Communication Networks*, 2018.

[12] X. Chen et al., "iDiSC: A New Approach to IoT-Data-Intensive Service Components Deployment in Edge-Cloud-Hybrid System", *IEEE Access*, Vol. 7, 2019, pp. 59172-59184.

[13] X. Zhang et al., "Intrusion Detection And Prevention in Cloud, Fog, and Internet of Things", 2019.

[14] L. Lyu et al., "Fog-empowered Anomaly Detection in IoT using Hyperellipsoidal Clustering", *IEEE Internet of Things Journal*, Vol. 4, No.5, 2017, pp. 1174-1184.

[15] R. Ullah et.al., "Design and Implementation of an Open Source Framework and Prototype for Named Data Networking-Based Edge Cloud Computing System", *IEEE Access*, Vol. 7, 2019, pp. 57741-57759.

[16] L. Cerina et al., "A Fog-Computing Architecture for Preventive Healthcare and Assisted Living in Smart Ambient", *Proceedings of the Third IEEE International Forum on Research and Technologies for Society and Industry*, IEEE, 2017, pp.1-6.

[17] S.K. Sood and I.Mahajan, "A fog-based healthcare framework for chikungunya", *IEEE Internet of Things Journal*, Vol. 5, No.2, 2017, pp. 794-801.

[18] J. Chaudhry et al., "AZSPM: Autonomic Zero-Knowledge Security Provisioning Model for Medical Control Systems in Fog Computing Environments", *Proceedings of the IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, 2017, pp. 121-127.

[19] W. Tang et al., "Lightweight and Privacy-Preserving Fog-Assisted Information Sharing Scheme for Health Big Data", *Proceedings of the IEEE Global Communications Conference*, 2017, pp.1-6.

[20] T. Muhammed et al., "UbeHealth: A Personalized Ubiquitous Cloud And Edge-Enabled Networked Healthcare System for Smart Cities", *IEEE Access*, Vol. 6, 2018, pp. 32258-32285.

[21] A. Ullah, Ata et al., "FoG Assisted Secure De-Duplicated Data Dissemination in Smart Healthcare IoT", *Proceedings of the IEEE international conference on smart internet of things*, 2018, pp. 166-171.

[22] F. Lin et al., "Content Recommendation Algorithm for Intelligent Navigator in Fog Computing Based IoT Environment", *IEEE Access*, Vol. 7, 2019, pp. 53677-53686.

[23] S. Liao et al., "Fog-enabled Vehicle as a Service for Computing Geographical Migration in Smart Cities", *IEEE Access*, Vol. 7 , 2019, pp. 8726-8736.

[24] J. An et al., "EiF: Toward an Elastic IoT Fog Framework for AI Services", *IEEE Communications Magazine* Vol, 57, No.5, 2019, pp. 28-33.

[25] P Gope et al., "Anonymous Communications for Secure Device-To-Device-Aided Fog Computing: Architecture, Challenges, and Solutions", *IEEE Consumer Electronics Magazine*, Vol. 8, No.3, 2019, pp. 10-16.

[26] A. Kumari et al., "Fog Computing for Healthcare 4.0 Environment: Opportunities and Challenges", *Computers & Electrical Engineering*, 72, 2018, pp. 1-13.

[27] A. Alamer., "Security and privacy-awareness in a Software-Defined Fog Computing Network for the Internet Of Things", *Optical Switching and Networking*, 2021, 100616.

[28] G. Fersi.., "Fog Computing and Internet of Things in One Building Block: A Survey and an Overview of Interacting Technologies", *Cluster Computing* ,2021, pp. 1-31.

[29] S.A et al., "Transmission of Secure Sensitive Health Care Information Using Hybrid Encryption in Cloud Computing", *International Journal of Advanced Science and Technology*, Vol.28, No.15, pp.344 - 354.

[30] B.P. Kavin and S. Ganapathy., "EC (DH) 2: An Effective Secured Data Storage Mechanism for Cloud Based IoT Applications using Elliptic Curve and Diffie-Hellman", *International Journal of Internet Technology and Secured Transactions*, Vol. 10, No.5, 2020, pp. 601-617.

[31] Y.K. Kumar R. M. Shafi., "An Efficient and Secure Data Storage in Cloud Computing using Modified RSA Public Key Cryptosystem", *International Journal of Electrical and Computer Engineering*, Vol.10, No.1, 2020, pp. 530.

[32] B.P Kavin et al., "An enhanced security framework for secured data storage and communications in cloud using ECC access control and LDSA", *Wireless Personal Communication*, Vol. 115, No.2 , 2020, pp. 1107-1135.