Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 5, 7721–7730

To Promote Health Data Security in Mobile Cloud Computing By Using the Modular Encryption Protocol

Dr.K.Sai Manoj [1]

[1] *CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, Andhra Pradesh, India.*

Abstract

Cloud computing has greatly increased in recent years as computer capabilities have advanced, due to applications, services, memory, and processing over the Internet. It's employed in a wide range of fields, including medical, agriculture, business, informatics, and many more. It also encourages dynamic resource adaptability and management decoupling at a low cost. Despite the numerous evident advantages of Mobile Cloud Computing (MCC) in medicine, its development is limited by worries about security and privacy. To grasp the full extent and effectiveness of such issues, fast action is required. On a global, regional, and local level, health information security is essential.To make good use of health services, it is necessary to follow the necessary security procedures to avoid security risks and vulnerabilities.As a result, the purpose of this research is to employ the Modular Encryption Standard (MES) to offer requirement-oriented medical data security based on tiered security mechanism modeling. In terms of speed and supplemental qualitative security assuring approaches, the suggested work outperforms existing generally used algorithms for health data security in the MCC environment, according to performance analysis.

Keywords: health data, mobile modular protection, cloud computing,privacy, encryption

I. INTRODUCTION

Innovative changes have enabled progressive solutions to be implemented to improve the nature of humanity. Analysts looking at the future of innovation have gathered and analyzed data on well-being from different sources to gather insight and address well-being-related challenges. As a result, the expansion of integrated medical care technology has the potential to improve productivity and comprehension of results at every level of the medical care system. LTC facilities are an important aspect of the healthcare sector, as they provide care to the population's fastest-growing segment. The use of EHRs in LTC institutions, on the other hand, lags behind other sectors of the health care business [1].These structures can raise personal satisfaction, promote the coordinated effort, improve outcomes, lower costs, and boost the overall effectiveness of e-medical care administrations [2].

[3]Furthermore, Eisenach portrayed e-Health as a tech industry that deals with the Internet's construction, systems management, and health services, all of which greatly benefit the framework's customers and partners. E-wellbeing is a growing field that combines clinical analytics, general health, and Internet-based health services to embrace and promote the overall progress of new technology to address complex issues, reduce costs, and increase understanding [4-6].Models, gadgets, and structures connected with the IoT have grown ubiquitous along these lines. Furthermore, the widespread adoption of IoT has coincided with the advancement of connected communication breakthroughs, such as recording knowledge for medical treatment, business, manufacturing, operational setups, and so on. To enable efficient and secure use of

health data innovations, benefits, and all-encompassing e-[7-8]Health approaches possible, security frameworks must be very efficient and robust. The universality of IoT platforms has fueledIoT innovation, with many designs in mind for usage by healthcare enterprises. Using the Internet of Things to connect devices, devices, apps, and services allows e-Health frameworks to communicate related data using cutting-edge technology [9].When combined as adaptable, versatile, and effective tolerant healthcare service frameworks, IoT and distributed computing are progressive technologies that complement one other's capabilities.

The medical care business has been transformed by distributed computing. Innovation adaptability, smart, energy investment finances, processing, and sharable resources, and faster transmitting are all key benefits of distributed computing. This presentation will go over distributed computing, which has been highlighted as a problem in the medical services business, as well as other cloud-related security and key protection issues. In addition, we'll talk about possible security arrangements. For medical service providers, a coordinated endeavor of data in the cloud raises major security and protection concerns. As a result, major concerns in the adoption of cloud-related innovation programs include attempted security, efficiency, security, and adaptability [7].Mists are collections of virtualized assets such as real-time workers, organized virtual workers, apps, and prospective advantages. To meet the needs of the shopper's end client, figuring assets might be placed in clusters or independently. The uptime is broken down by arrangement. Distributed computing is a technology that is used to deliver and manage applications and data, as well as server availability and end-user configuration (EUC) delivery. Cloud computing enables employees to access and manage their applications and data from any device, at any time, and from any location. [8]

A successfully distributed computing arrangement should provide infrastructure and end users with rearranged or brought together, logical, and secure understanding. Distributed computing, like all advancements, has its own set of characteristics, such as the board, creativity, privacy, and legal concerns. [12-13] Cloud computing has gained a lot of interest in recent times as computing technologies have swiftly advanced, thanks to apps, services, storage, and computation through the Internet. It is widely used in a variety of fields, including medicine, business, agriculture, data [14]technology, and many more. Smart technologies, such as smartphones and tablets, are gradually becoming a necessary part of human existence as an efficient and easy means of communication that is not constrained by space or time. [15]

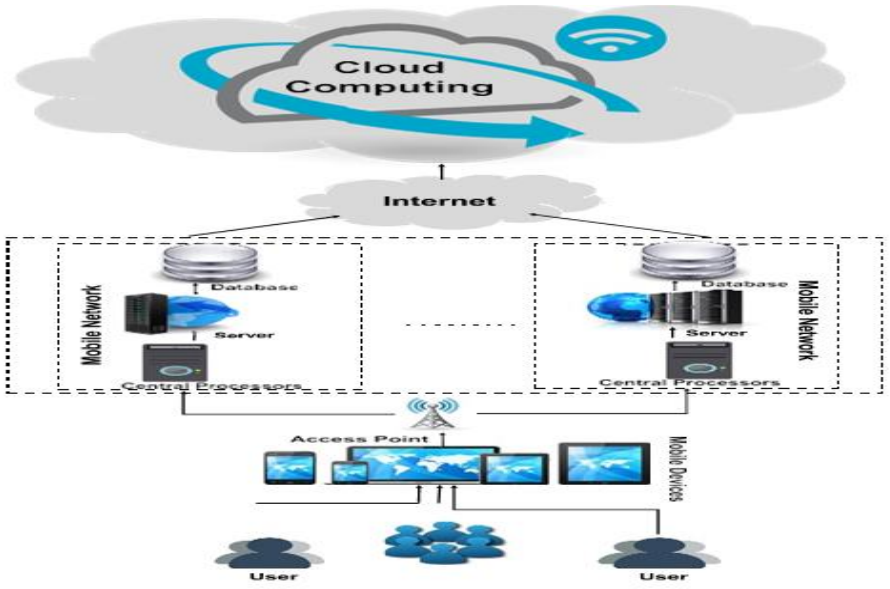

FIGURE 1.*Mobile cloud computing.*

II. THE PROPOSED WORK

This section gives a high-level summary of the planned project. FIGURE 4 depicts the actions that must be taken while using MES to provide HI confidentiality at MCC, whereas FIGURE 2 depicts the overall scenario for HI security utilizing MES at MCC. These safeguards are necessary to protect HI from many types of cloud assaults, including insider and outsider attacks. The goal of this study is to find a solution to the threat's fifth category, as shown in Table 2.The detection and characterization of health records is the first step in this scheme. This classification and identification are based on the necessary level of confidentiality. Most crucially, an entropy-based derived key will be assigned at the MCC client side. Depending on the kind of information saved, the HI owner selects the appropriate key. The key choice is based on the HI classification and identification. The health data would now be decoded using the extender or contractor scheme in the next module.

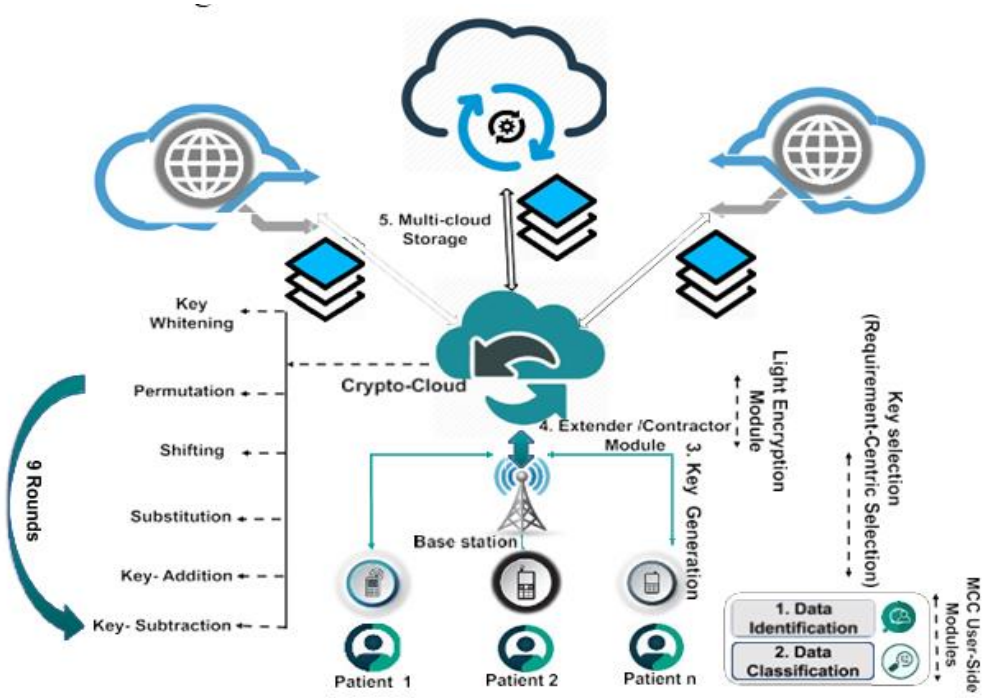

FIGURE 2. *Healthcare monitoring using MES.*

2.1. Security of Health Information (HI)

Along with developments in the healthcare environment, ensuring the security of HI is an ongoing process. As a result of the adoption of new schemes, it is also required to assess HI's security regulations and practises in order to improve the quality and efficacy of HI in practise. Recognizing risks and defending the HI is challenging and time-consuming for small health clinics. This research intends to assist the profession in anticipating those expectations and challenges, conducting effective risk assessments, and developing appropriate security solutions to ensure HI security.

MCC has many advantages in the healthcare field, including

2.1.1 Portability:

The ability to remotely access and analyze patient data in a dispersed and ubiquitous way.

2.1.2 Scalability:

Remote access to patient data is made easier.

2.1.3 Modernization:

MCC lowers the hurdles to healthcare application modernization.

2.1.4 Performance:

MCC can provide speedy access to computing and massive data storage. It facilitates information sharing while also lowering costs.

2.1.5 Collaboration:

It facilitates team-based care and maintains teamwork. MCC, among other options, could be the most effective HI monitoring method. As demonstrated in FIGURE 3, the combination of Healthcare Computing, Mobile Computing, and Cloud Computing is known as HMCC. The categories of medical records are listed in Table 1.

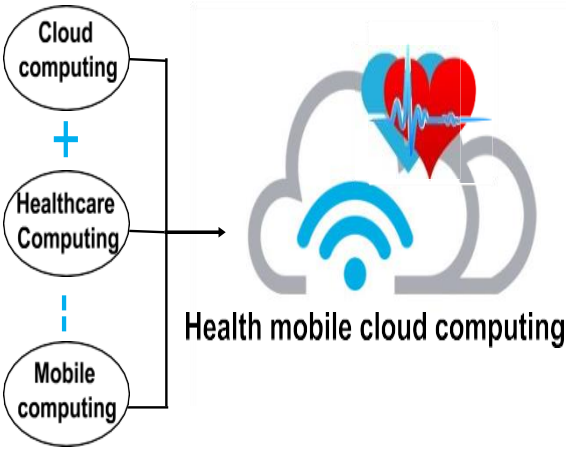

FIGURE 3.*Health mobile cloud computing*

TABLE 1.*Medical records.*

Records	Details
Primary Records	Age, Gender, Marital status, Education, Family situation, Family history of the disease, Economic situation
Lifestyle	Physical Activity, Diet, Smoking, Drinking, and Occupational visits.
Health Disorders	Eye, Foot, Diabetic, Nephropathy, Cerebrovascular, Cardiovascular, and other disorders.
Recall Records	Medications, Accessory evaluations, Signs, symptoms, and cause for referral to a doctor.
Daily review Records	Difficulties like Hypertension and Hypoglycemia.
Examinations	Cerebrovascular, Cardiovascular state, Blood lipids, Blood pressure, Blood glucose control or others.
Diagnosis regimens	Administering drugs, a Lifestyle guide

III. METHODOLOGY

Three significant measures are included in MES. "Identication (IDN)", "Classification (CLF)", and "Securing (SC)" are the three measures. IDN and CLF are carried out by the MCC user. The SC phase is carried out in the Crypto-cloud. Crypto-cloud is a cloud that serves as an intermediate for cryptography operations.

3.1. Identification

The amount of confidentiality of HI determines the need for safeguarding HI, which is determined by IDN and CLF characterization. The IDN of Health Records is determined by the mentioned prerequisites of the MCC client. It usually consists of two broad classes, with sub-classifications in between. Confidential HI (which needs extensive security) and accessible HI (which does not).

3.2. Classification

In HI, classification determines the level of secrecy depending on the record's type. It helps determine which HI should be protected, lowering security costs as a result. Dependent on the extent of sensitivity, these two groupings are divided into five unique sub-categories. The five different sub-categories are listed below. The safeguarding measure consists of five distinct types of keys for the 5 sub-classifications listed below.

1) Non-sensitive data

Open Data, such as doctor's/hours specialists of accessibility and clinics, etc.

2) Sensitive data

Information that isn't as sensitive, such as the patient's name, gender, and so onInformation that is moderately sensitive, such as the general practitioners or medical centres to which the patient has been referred, the dates and times of patient-doctor consultations, and so on.Extremely sensitive information, such as patient diagnostic results, etc.

3.3. Securing

The securing metric is made up of the remaining cryptographic methods. These operations would take place in the crypto-cloud. This step consists of nine rounds totaling ten keys. The modular interaction that underpins the entire process of HI storage and cloud access is depicted in FIGURES 6 and 7. We'll go over the MES decryption and encryption technique in the next section.

3.4. Modular interaction

The patient is connected to the smart gadgets via three modules on the user side. At the second layer, the securing measure, which is made up of eight sub-measures, is used to connect connected devices to the crypto cloud. Finally, FIGURE 4 depicts the crypto-cloud to multi-cloud link. FIGURE 5 illustrates the modular interface for gaining access to confidential health information.

3.5. Mathematical model

Table 2 shows the notations that were utilized in the developed model.

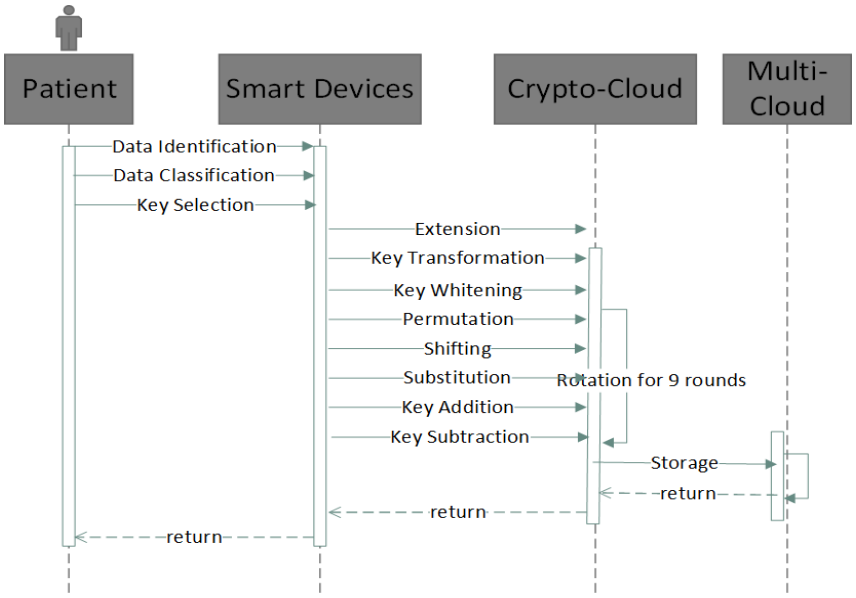

FIGURE 4*.HI storage at cloud using MES.*

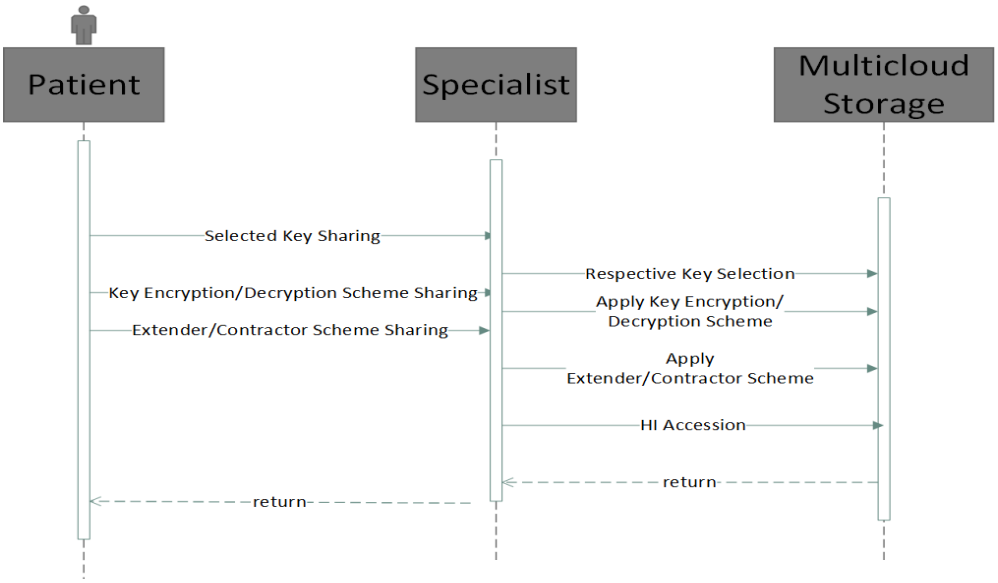

Fig 5.*HI storage sharing using MES.*

Table 2.*Notationsused.*

PT	Plaintext
K	Key
Ext	Extension
Cn	Contraction
LEPT	
Exp	
DExp	
Pr	r^{th}
Sr	Substitution for r^{th} *round*
K_L^r	
K_R^r	r^{th}
fXfY	Fx

3.5.1. HI sharing at MCC using MES

As shown in FIGURE 9, the steps for distributing HI utilizing MCC are as follows.

1) After a health inspection, take a picture of yourself. The HIR is delivered to the patient through a mobile device.
2) Data transfer from mobile devices to the cloud, as well as data transfer from medical to the cloud.
3) The sharing system specifies the accessibility to HI in the case of therapy.
4) The doctor uses the cloud to obtain the patient's medical information.
5) The doctor makes a diagnosis and makes any necessary referrals.

3.6. Examining the patient

The HealthCare Center provides HIR to the patient (HCC). The HCC and cloud do the authentication process.

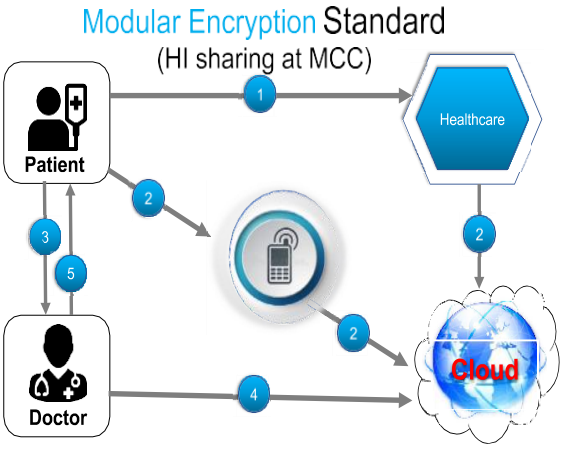

Fig. 6.*HI sharing at cloud using MES.*

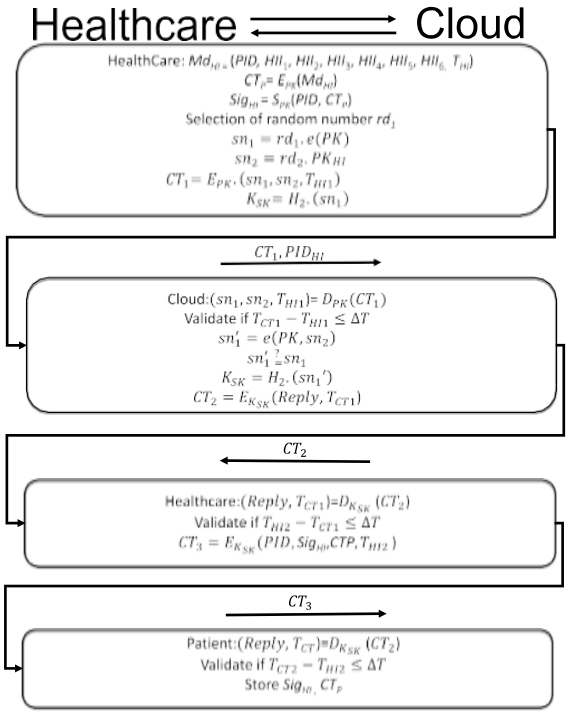

FIGURE 7.*Patient examination.*

IV. EXPERIMENTS AND RESULTS

In the MCC context, this section covers the MES analysis from many angles. The following specifications were used to implement MES in the cloud. The results of our proposed work's performance evaluation are shown in this part. We looked at the performance testing aspects of MES on their own and in comparison to other common encrypting block ciphers. The environmental configuration for the suggested scheme performance evaluation is shown in Table 3.

TABLE 3.*Setup for experiments.*

Setup	Description
System	64-bit OS, X-64 based Processor
OS	Windows 10
Processor	Intel(R) Core(TM) i7-7500U CPU @ 2.70 GHz 2.90GHz
Platform	Visual C++ (Visual Studio Community 2017)

4.1. Modularity Check

Table 5 shows the module-based processing use of MES with varied input sizes. In addition, the MES's module-based runtime is as follows. The elapsed time of MES encryption is calculated. The time it takes the cryptographic technique to convert real data to cipher-text is called enciphering time. The encryption time aids in _guring the throughput for any technique. It controls the encryption rate. The lower the power consumption, the greater the throughput. Varying results were obtained by employing different quantities of inputs, as indicated below. The graphs below demonstrate the superiority of the suggested work over alternative methods.

Table 4.*Processor utilisation rate.*

	Modular-Analysis	Time (1KB sec)	Time (2KBs sec)	Time (3KBs sec)
1	**Key-Transformation**	0.0620079	0.00341145	0.00275324
2	**Key-Whitening**	0.000007030	0.000019749	0.000001057
3	**Rounds**	0.000371302	0.000035610	0.000025030
4	**Key-Encryption**	0.000394236	0.000004572	0.000003534

Table 5.*Analyses based on different processors.*

Processor Categories	MES Elapsed Time
Intel(R) Core(TM) M-5Y10c CPU @ 0.80GHz 1.00 GHz	0.0542858(sec)
Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz 1.90 GHz	0.515033(sec)
Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz	0.330330(sec)

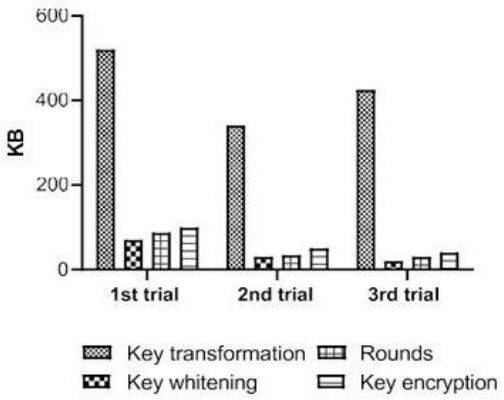

Fig. 8.*MES modular analysis.*

4.2. Memory utilization

The most important parameter in performance assessment is memory consumption.The graphs below show how much memory MES, Blow sh, RC6 DES, RC5, AES, and 3DES use.

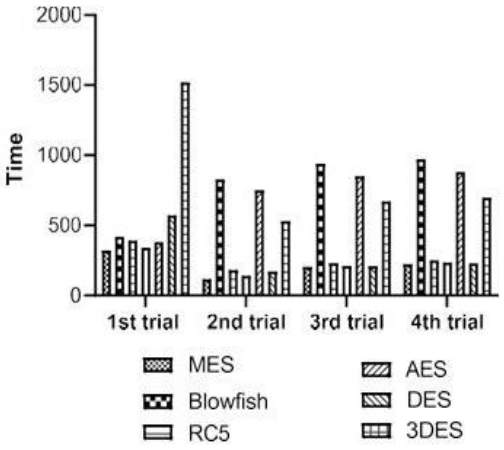

FIGURE 9. *Processor utilization rate.*

The memory usage of various methods is depicted in FIGURE 15. With the help of the "Visual studio analysis tab," this analysis was completed. The MES diagnostic session lasted 12.12 seconds, with memory usage measured in kilobytes. While it took 16.123 seconds for AES, 11.23 seconds for Blow sh, 14.12 seconds for RC5, 11.23 seconds for RC6, 16.234 seconds for DES, and 22.12 seconds for 3DES, with memory usage in kilobytes.

4.3. Rate of key-data collation for a single round

Except for the KW stage, each key updates the data twice per round. Key subtraction and key addition, in addition to KW, are key subsuming measures, thus it's 18 times key subsuming with information rather than 9 times (for nine levels). FIGURE 12 compares DES, IDEA, RC5, 3DES, RC6, Blow sh, AES, IDEA, 3DES, MES, and DES in terms of single round key subsuming, with MES performing the transition twice in each round compared to DES, IDEA, RC5, RC6, 3DES, Blow fish, and AES.

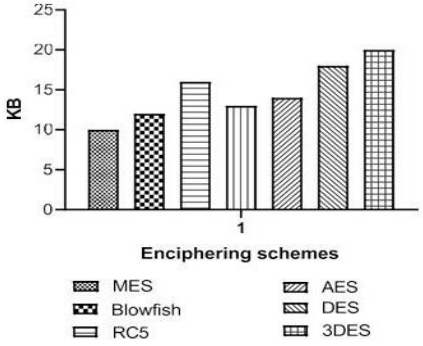

FIGURE 10.*Memory utilization.*

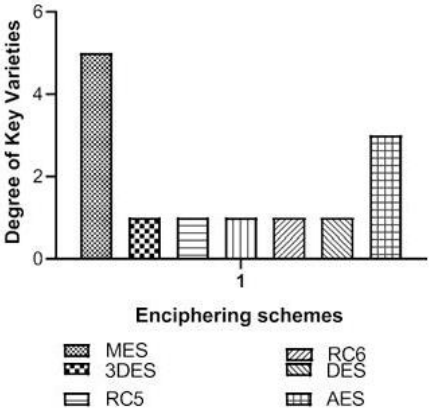

FIGURE 11.*Degree of key varieties.*

4.4. Complications in time and space, and also analysis of results

MES uses fixed block sizes, like 3DES, DES, AES, and other cryptographic algorithms. It has an O(1) temporal complexity and is unaffected by the size of the input. MES has an O spatial complexity (n). The designed Methods 1 and 2 can identify these outcomes. Moreover, the above studies showed that MES outshines other frequently used methods in terms of low processor and memory usage, the highest extent of key variances, and the highest data collection rate, implying that MES is a better choice for mobile devices due to its low storage and processor usage. The created technique can provide acceptable results in the MCC situation due to the additional distinct quantitative security guaranteeing procedures stated in Table 6.

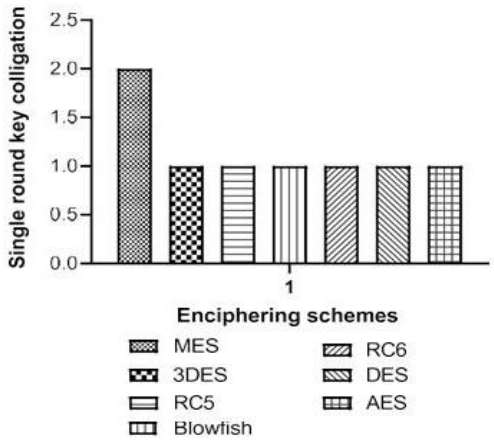

Fig. 12.*Key-data colligation rate.*

V. CONCLUSION

Despite the potential answers given by MCC in health record surveillance, many roadblocks prevent MCC from realizing its full potential. The use of MCC in healthcare is hampered by many issues, the most significant of which are security and privacy concerns. One of the significant research gaps is this. As a result, this study employs MES, a layered, modular, data-centric cryptography solution that employs secure HI sharing and retention techniques. In the MCC environment, the results show that this method beats other commonly utilised methods.

REFERENCES

1. Almaiah, Mohammed Amin, and Ahmad Al-Khasawneh. "Investigating the main determinants of mobile cloud computing adoption in university campus." Education and Information Technologies 25.4 (2020): 3087-3107.
2. Aliyu, Ahmed, et al. "Mobile cloud computing: taxonomy and challenges." Journal of Computer Networks and Communications 2020 (2020).
3. Li, Haifeng, et al. "A secure and lightweight fine-grained data sharing scheme for mobile cloud computing." Sensors 20.17 (2020): 4720.
4. Shamshirband, Shahab, et al. "Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues." Journal of Information Security and Applications 55 (2020): 102582.
5. AAlmusaylim, Zahrah, and N. Z. Jhanjhi. "Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing." Wireless Personal Communications 111.1 (2020): 541-564.
6. Lo'ai, A. Tawalbeh, et al. "Mobile cloud computing model and big data analysis for healthcare applications." IEEE Access 4 (2016): 6171-6180.
7. Xu, Xiaolong, et al. "Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing." Multimedia Tools and Applications 79.15 (2020): 9819-9844.
8. Aceto, Giuseppe, Valerio Persico, and Antonio Pescapé. "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0." Journal of Industrial Information Integration 18 (2020): 100129.
9. Youssef, Ahmed E. "A framework for secure healthcare systems based on big data analytics in mobile cloud

computing environments." Int J Ambient SystAppl 2.2 (2014): 1-11.
10. Stergiou, Christos L., et al. "Secure machine learning scenario from big data in cloud computing via internet of things network." Handbook of computer networks and cyber security. Springer, Cham, 2020. 525-554.
11. Raj, Jennifer S. "A novel encryption and decryption of data using mobile cloud computing platform." IRO Journal on Sustainable Wireless Systems 2.3 (2021): 118-122.
12. Nanda, Sarmistha, Chhabi Rani Panigrahi, and BibudhenduPati. "Emergency management systems using mobile cloud computing: A survey." International Journal of Communication Systems (2020): e4619.
13. Abuarqoub, Abdelrahman. "D-FAP: dual-factor authentication protocol for mobile cloud connected devices." Journal of Sensor and Actuator Networks 9.1 (2019): 1.
14. Altowaijri, Saleh M. "An architecture to improve the security of cloud computing in the healthcare sector." Smart Infrastructure and Applications. Springer, Cham, 2020. 249-266.
15. Sun, Lanfang, et al. "Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application." IEEE Access 8 (2020): 101079-101092.

AUTHORS DETAILS

Dr. SAI MANOJ KUDARAVALLI, is a Founder and CEO in Innogeecks™ Technologies, Vijayawada and also acting as a CEO for the Amrita Sai Institute of Science and Technology since 2014, and he played vital key role in Fidelity Investments as a Senior Business Analyst for 4.4 years in Business Analytics & Research and worked as Project Engineer in Wipro Technologies for 1.5 years, He got more than 10 years of experiences in financial services, IT services and education domain. He was awarded Doctor of Science in the merit level.

He was completed Bachelor of Technology in Mechanical Engineering from Amritha University, Coimatore. He is completed Master of Technology in Information Technology from IIIT- Bangalore. He holds Doctor of Philosophy (PhD) in Cloud computing arena from Kanpur University, India.

He was certified in Microsoft Certified Technology Specialist (MCTS) from Microsoft Corporation, and Certified Ethical Hacker v9 (CEH), and “Paul Harris Fellow” recognition by Rotary International. He is Published more than 10 research papers in various reputed International and national research journals/conferences/ Magazines. He attended 4 national level workshops and participated 3 international workshops; He is also a charted Engineer (Computer Science) from IEI. He is active member of IEEE, ACM, IEI, SHRM, NEN – Bangalore Chapter, HR Sangham – Chennai, CCICI (Cloud Computing), Rotary International Services. He is acting as a reviewer for the High Standard Journals such as Springer, IE, Scopus etc.