Revista Argentina de Clínica Psicológica
2024, Vol. XXXIII, N°1, 74-90
DOI: 10.53555/03276716.2024.08

Preserving COVID Related Cardio-Vascular Impairment Records in a Mobile Cloud Infra via Secure Ecosystem

Ms. Anitha Marimuthu[1]*, Dr. Sakthivel Subramaniam[2]

Abstract:
A crucial technique called virtualization, whereby a hypervisor creates several distinct virtual units is used to develop mobile clouds. With the help of the dynamic cloud platform, end-users will carry out complicated functions and organize essential information using smart devices (thin clients)–especially in maintaining health records. A few significant issues are providing secure authentication, validation and integrity of health records via MC services, which are adequate and advanced consent for dynamic data authorizations with block chain.
A thin client makes cloud strategies preferable to telemedicine platforms, especially in tracking risk assessments. Individuals with COVID-19 require specialized cardiac care, emphasizing prompt diagnosis and treatment of heart problems. The Bayesian technique is used in this study to predict the risk of Cardio-Vascular Disease (CVD) with COVID symptoms. Such security ensures risk-free accessibility of CVD records at the end-user point. Three-tier security measures have been provided to the CVD-oriented risk-assessed records in the MC infra. The first tier of security adopts the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms to ensure authentication and validation of the legal data transaction process with SHA-512 for layered authentication. In contrast, the second tier includes progressive security orders and third tier integrated through blockchain technology.
Assessing security is notoriously challenging; often, the only way to do so is to evaluate a system's robustness by observing how well it fares against well-known attacks. Thus, the quantitative analysis deals with various facts and metrics (confidentiality rate, protection index Vs vulnerability index, and protection index Vs attack index) with respect to the resistance rate of the model against a few attacks. The qualitative analysis exhibits the influence of COVID symptoms on CVD and their associated dispersion of data transaction in MC infra (low, moderate, and high). In contrast to a few current models, the suggested model shows the best outcomes, according to multiple analyzes.

Keywords: encryption, cryptosystem, blockchain, security, cloudlet, CVD, COVID, authentication, two-tier security, mobile ecosystem

1. INTRODUCTION

The hashing method and encryption algorithm determine the blockchain's primary strength (Sabeena, 2024). In order to reflect the original data, hashing transforms the block's transaction data into a fixed length value. In addition to blockchain, hashing encryption techniques like MD5, SHA-1, SHA-512, and others can be used in other contexts. In contrast to the original SHA-512 method, which has 80 rounds, this work presents a novel Exchanged SHA-512 algorithm, which is an improved version of SHA-512 with 60 rounds.
Email security, particularly against phishing, spoofing, and distributed denial-of-service (DoS) attacks (Eljim, 2024), is a pressing concern given the essential role email plays in accessing various online accounts and parameters like hash construction, computational efficiency, data integrity, collision resistance, and attack resistance. The results showed its avalanche percentage exceeded the 50% target, reaching 50.08%. Investigates various privacy-preserving techniques (Tungar D.V, 2023) for safely classifying sensitive data using Bouncy Castle's encryption library and machine learning algorithms. The study uses the Bouncy Castle, which offers encryption using the RSA-2048 technique, to encrypt the dataset. The technique improves system speed and privacy protection by utilizing lookup substitution with k-anonymization, which lowers data risks.
Cardiovascular disease is a broad term covering various conditions affecting the heart and its circulatory system (Vetta, 2020). For certain people, the new COVID-19 (Hunter, 2020) virus may harm their cardiovascular system and lead to cardiac complications. Cardiac arrest, autonomic dysfunction, and blood coagulation are just a few of the CVD issues that may result from the virus's ability to trigger inflammation in the entire CVD and circulation arteries. Long-term CVD issues may

[1]*Kingston Engineering College, Vellore, Tamil Nadu, India, Email: anitham.apcse@gmail.com
[2]Sona College of Technology, Salem, Tamil Nadu, India, Email: sakvel75@gmail.com

*Corresponding Author: Ms. Anitha Marimuthu
*Kingston Engineering College, Vellore, Tamil Nadu, India, Email: anitham.apcse@gmail.com

occur even in persons without a history of cardiovascular disease due to the impact of COVID-19, which damages the endothelial cells lining the blood vessels.

There are still no streamlined risk assessment techniques for COVID-19 individuals focused on CVD, and various healthcare practitioners may utilize a variety of instruments or approaches to determine a patient's level of risk. Examining data focusing on CVD risk assessments might assist in pinpointing causes of COVID-19 sequelae such as hospitalization, ICU admittance, or sometimes mortality. The study of COVID-19 patients' medical records with a focus on CVD risk assessment (Rodrigues, 2017) is crucial for advancing the study of the disease and devising more constructive means for detecting and controlling severe instances. Patient records may be efficiently managed on the mobile cloud, allowing on-demand access to information, services, and resources, whatever the volume. Mobile cloud technologies provide more stabilized methods to maintain and retrieve CVD risk assessment records for COVID-19 individuals confidentially and remotely.

The term "mobile cloud computing" describes the practice of using cloud services and resources to facilitate the distribution of mobile software and data. Computing concepts, including shared resources, decentralization, grid, multi-functionality, parallelism, and virtualization, has contributed to MCC's development (“Mobile Cloud Computation: Issues and Challenges,” 2017). Thus, it is a system that combines hardware and software to facilitate the deployment of resources by employing ubiquitous and utility computing. Virtualization is crucial for portable cloud implementation since it allows a hypervisor to create several virtual modules.

Thin clients, like mobile devices and tablets, may access the Mobility Cloud platform, accomplish complicated functions, and store data. However, mobile platforms, battery life, and storage space are always limiting factors (Han et al., 2015). As with cloud computing, the mobile cloud allows individuals to acquire, analyze, and store information across several platforms and systems. MC employs computational rejuvenation strategies, which indicates that computations are performed off-device rather than directly on the mobile unit. As a result, mobile devices with limited capacity may make use of the various kinds of processing power accessible in the cloud infrastructure.

1.1 Significance of Mobile Cloud Computing

Improved security capabilities, expandability, cross-device synchronization, and encrypted storage are just some of the ways in which MCC will ensure the long-term viability of sensitive data. In addition, MCC provides several substantial advantages in the scope of secure data storage (Farrugia, 2016).

Security of sensitive information: Preserve sensitive information on off-site servers, which is an alternative process to storing it locally on the device itself from being abandoned or breached, preventing the potential risk of malfeasance or illegal access.

Information preservation and restoration: Ensure that critical information is not compromised in the case of device malfunction or unexpected massive failure.

Improved security delivers: Features like encrypted data transfer mechanisms, multi-factor authentication, and encrypted communications to their clientele.

Extensibility: Provide a scalable storage capability, which means that the amount of storage space can be readily expanded or lowered depending on the requirements.

Cross-device IPC: Synchronization of data across numerous devices, which could also assist in ensuring that information is updated regularly and is available from any site.

1.2 Architecture of Mobile Cloud

The components that make up mobile cloud architecture (Chondamrongkul & Chondamrongkul, 2017) encompass portable devices, cloud platforms, wireless operators, protection aspects of mobile applications, and virtual mobile data protection.

The two main types of mobile cloud designs are cloudlet architecture and non-Cloudlet architecture (Fernando et al., 2013). In this study, we use cloudlet architecture, a kind of cloud computing that makes use of individual, remotely located servers (labeled "cloudlets") to act as processing and storage nodes for mobile devices. In this way, the mobile device reduces the latency experienced while connecting to distant cloud servers by making use of the cloudlet's computing and storage capabilities.

Figure 1 depicts the generalized architecture of mobile cloud.

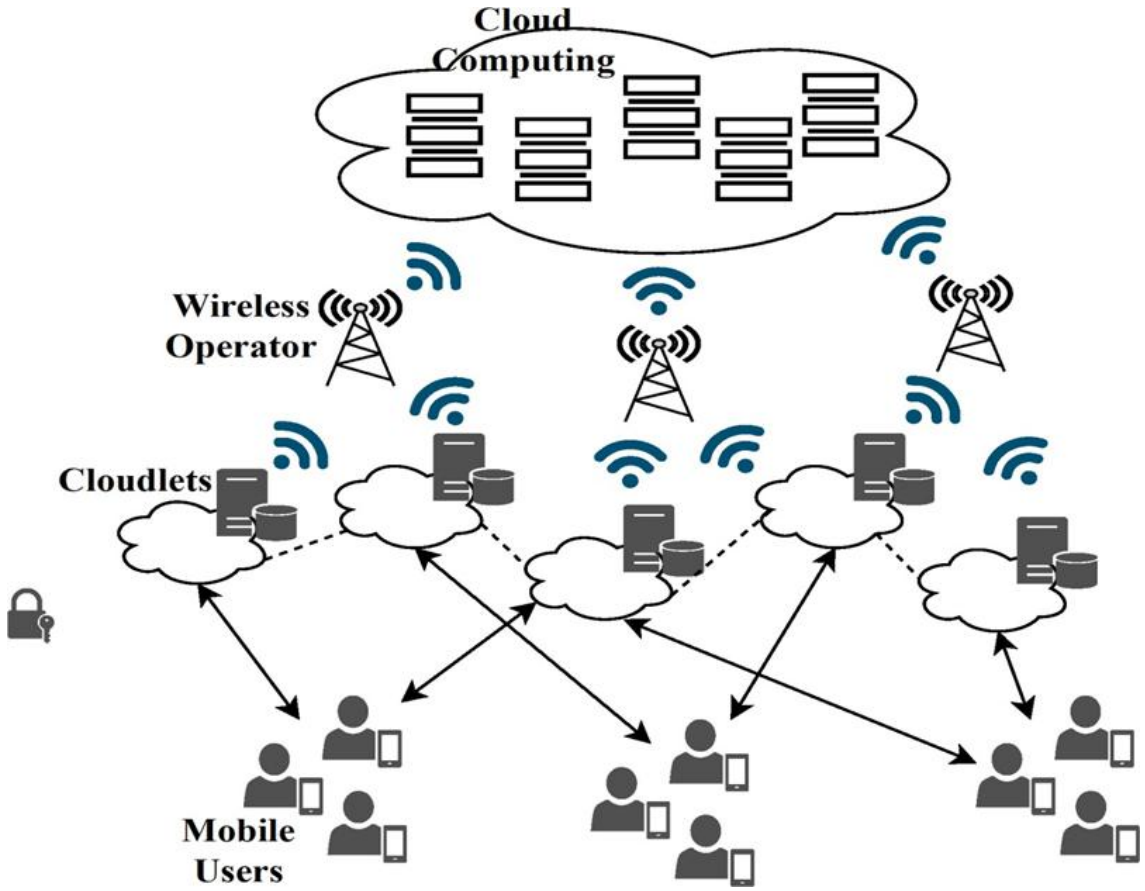


Figure 1. Mobile Cloud Architecture

Vital elements of cloudlet mobile architecture are (Sobh & Khalil, 2022):

Portable Devices: Runs apps and services while interacting with the cloudlet. This takes some of the processing and storage load off of the device.

Cloudlet Platform: The cloudlet is a compact cloud infrastructure that can be plugged into a mobile device to give it additional storage and processing power.

Virtual Infra: The virtualization consists of external cloud servers that the cloudlet can connect to access more data to store and manage.

Wireless Operators: The mobile network bridges the gap in communication between the mobile units, the cloudlet, and the cloud's backend infrastructure.

Protection aspects of mobile applications: Mobile apps are computer programmes that may be integrated into a mobile device and operate locally, communicating with a cloud-based server so the client can access digital sites. Several different frameworks and programming languages can be employed to create such apps.

Virtual mobile data protection: The mobile cloud's security is crucial since it prevents malicious users from accessing sensitive data. Examples include authentication programmes, encryption software, and security systems restricting who may enter specific confidential data sectors.

Together, they provide a computing platform that is accessible virtually everywhere and on all virtual machines interconnected with numerous mobile devices, is highly scalable, and allows for the distribution of mobile apps and services.

1.3 Problem Identification

Establishing a secure work context for storing records of cardiovascular impairment due to COVID in mobile cloud architecture necessitates carefully considering numerous aspects. Maintaining the confidentiality and security of patient information is of paramount importance. However, mobile cloud architecture may introduce other cyber security vulnerabilities (Raghunath et al., 2022), necessitating extra precautions to protect the data's privacy, security, and accessibility. Compliance with all applicable rules and regulations, such as those pertaining to data protection and privacy, is crucial to ensuring the preservation and use of sensitive healthcare information within the ecosystem.

Consequently, it is crucial to check that all information obtained is accurate and reliable. Creating a safe environment may be costly, particularly when stringent safety measures and regulatory conformity must be complied with. Also, consideration should be given to the costs associated with preserving and enhancing the infrastructure. Finally, there is a need to enlighten both

healthcare providers and patients on the value of data sharing to advance medical science and improve patient care.

1.4 Problem Definition

Records of COVID-related cardiovascular impairment can be stored securely in a mobile cloud environment. This could offer a scalable and versatile computing environment for storing and retrieving medical records while also protecting the privacy of patients' sensitive information. There are many critical aspects involved in creating a safe environment for storing records of cardiovascular dysfunction due to COVID in a mobile cloud infrastructure:

- Assessing potential risks: Data privacy and security hazards are only two instances of risks that should be considered during a risk assessment of the mobile cloud architecture.
- Implementation of security measures: In order to reduce the impact of the threats identified by the risk assessment, proper security measures must be put in place. Access restrictions, encryption, and data backup and restoration are all possibilities.
- Employing encrypted storage: To ensure the safety of private data, it is essential to encrypt stored files and implement strict access restrictions. Security features, notably multi-encryption, encrypted transmission, and other safeguards, are among those commonly provided by cloud providers for their clients' information.
- Secure Data Transactions: Data transfers between mobile devices and the cloud infrastructure should be encrypted using encrypted communication techniques.
- Adherence to the Standard Regulatory: Any healthcare information kept in the mobile cloud environment must adhere to all applicable privacy and security policies. Proper data management policies and collaboration with a cloud-based service provider authorized to comply with healthcare regulations are essential for ensuring compliance.

Thus, we use a two-level security model, with AES ,DES and SHA-512 cryptosystems providing the first level of security and blockchain-based explicabilities providing the second level ensure the safety and privacy of sensitive information and also to prevent unwanted access and verify the integrity of COVID- related cardiovascular impairment reports stored in a mobile cloud environment.

Blockchain comprises a distributed ledger which contains a decentralized and immutable record of transactions. A blockchain-based system may be utilized to build a confidential and immutable database of COVID-related cardiovascular impairment records. This could aid in preserving the data for future use and preventing tampering.

The combination of these technologies has the potential to provide a reliable and safe system for safeguarding and storing documents relating to COVID-related cardiovascular dysfunction in an environment that is hosted in the cloud.

1.5 Scope and Motivation

Enhancing clinical outcomes, fostering research, and offering improved healthcare services depend on establishing a safe ecosystem for storing records of COVID-related cardiovascular dysfunction. Quality therapeutic outcomes can be expected as a result of earlier diagnosis of COVID-related cardiovascular abnormalities, facilitated by a secure setting for achieving such a goal. An early diagnosis aids in prompt intervention and avoiding problems. This study can potentially inform the design of improved therapeutic and preventative strategies. With mobile cloud architecture, physicians and other medical staff may access the information from any device at anytime. The privacy and confidentiality of patient data may be protected in a safe environment by shielding it from illegal access and cyber warfare.

1.6 Objectives

The objectives for establishing a secure ecosystem for preserving COVID-related cardiovascular impairment records in a mobile cloud infrastructure are:

- To preserve the COVID-related cardiovascular impairment records access to healthcare professionals and researchers for future reference.
- To develop a risk assessment model to identify potential threats and vulnerabilities this includes risks related to data privacy and security.
- To make the data accessible to healthcare professionals from anywhere at any time for better healthcare services to improve patient outcomes.
- To protect the data from unauthorized access and cyber threats, ensuring the privacy and confidentiality of patient information.
- To establish an ecosystem that is interoperable with different healthcare systems and platforms, ensuring that data can be shared and accessed by authorized parties.
- To provide complete study for research purposes to study the long-term impact of COVID on the cardiovascular system with the development of new treatment approaches and preventive measures.

The layout of the research work is delineated in the following manner. Section 2 highlights few recent and most relevant security approaches carried out in MC infra. Section 3 elaborates the inclusion datasets and BRAM model for risk assessment. Section 4 delineates the core methodology of the proposed model. Section

5 discussions both quantitative and qualitative assessments on implemented proposed model against various attacks. Section 6 summarizes the entire thematic process of the research work with possible future enhancements.

2. RELATED WORK

Hashing algorithm for security defined by S. Jenifa Sabeena et al. (2024) proposed an Exchanged Secure Hashing Algorithm (ESHA-512) which introduces a novel Exchanged SHA-512 algorithm is an improved version of SHA-512 with takes lesser number rounds as 60 where in traditional SHA-512 it is 80 rounds, it improves the strength as well as reduces the overall computation of the algorithm considerably and also also increases encryption data size per second than the SHA-512 algorithm.

Email Security defined by Sean Eljim S et al. (2024) proposed a Modification of SHA-512 using Bcrypt and salt for secure email hashing which provides Email security, particularly against phishing, spoofing, and distributed denial-of-service (DoS) attacks, is a pressing concern given the essential role email plays in accessing various online accounts. It introduced a modified SHA-512 algorithm, implementing additional security layers including randomly generated salt and the Bcrypt algorithm which evaluated on parameters like hash construction, computational efficiency, data integrity, collision resistance, and attack resistance. The results showed its avalanche percentage exceeded the 50% target, reaching 50.08%

Secure Classification of sensitive data defined by Tungar D. V. et al. (2023). Proposed an Evaluation of Privacy-Preserving Techniques: Bouncy Castle Encryption and Machine Learning Algorithms for Secure Classification of Sensitive Data. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 429 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2976

Access Control mechanism defined by Abdul et al. (2022) proposed an Enhancing Security of Mobile Cloud Computing by Trust- and Role-Based Access Control which provides a mechanism mitigating the malicious actions caused by authenticated users. The performance results indicate that the system's efficiency increases compared to trust and role-based access control mechanisms (detects and mitigates malicious users from the MCC environment).

Security measure gathered from Arumugam et al. (2021) proposed a secure data sharing for mobile cloud computing using RSA which provides consumers a number of points of interest, similar to storage limits, reliability, scalability and access to real-time information. As a result, it is expanding steadily and is undoubtedly organized into a daily day-to-day life. The amount of security provided for data protection is therefore directly proportional to the data value.

Mobile Cloud Architecture designed with the reference Zkik et al. (2019) proposed a Secure Mobile Multi Cloud Architecture for Authentication and Data Storage which provides an authentication and confidentiality scheme based on homomorphic encryption, and also a recovery mechanism to secure access for mobile users to the remote multi cloud servers. Also provide an implementation of our framework to demonstrate its robustness and efficiency, and a security analysis. Performance results a recovery mechanism to ensure the high availability and to prevent our network from distributing denial of services attacks.

Encryption and Decryption technique estimated with the help of Nasiraee and Ashouri 2018 proposed a Dependable and Robust Attribute-Based Encryption in Mobile Cloud Computing which introduce and address the problem to more dependability and robustness of whole networks when DoS attacks are present. Finally with discussion on different aspects of the proposal we show its profitability. Results with efficient source authentication for fast verification of outsourced encryption especially for resource constrained devices to thwart DoS attacks. Also with a simple mechanism, it discards the replayed packets.

Parameswari and Vani (2018) proposed a Mobile Cloud-Privacy and Data Security in Healthcare Environment Using Cloudsim Simulator is a mobile cloud- based healthcare system that provides a high level of privacy and data security for protecting patient data from unauthorized access. Performance results that the system can provide high performance in terms of response time and resource utilization with the CloudSim simulator.

Storage Security supported by Suganya and Shalinie (2018) proposed a Provable dynamic auditing in mobile cloud computing for secure storage of e-health data. Using Provable Dynamic Data Auditing Protocol (PD-DAP) involves a trusted Third-Party Auditor (TPA) who is in charge of blockless verification of data without retrieving the private health data. The usage of bilinear pairing and Merkle Hash Trees guarantees blockless verification by TPA. Also, the proposed PD-DAP supports secure dynamic operations by the mobile user with the help of TPA. Hence, it saves the mobile user's computational resource, thereby achieving cost-effectiveness to gain trust in the Cloud Storage Server (CSS). From the above related work, it is seen that the huge storage space is used for data access with less security and many of the researchers used only single encryption and decryption algorithms. In the present research proposes less data storage consumption techniques with more than one data encryption and decryption algorithms such as AES and DES using two-tier security measures.

It is evident that the widespread use of mobile cloud infrastructures in recent years has revolutionized the distribution of healthcare services. However, the

security of healthcare data in mobile cloud systems has received little attention from researchers. Adherence to laws governing the confidentiality and security of medical records is a significant obstacle. In addition, the specific difficulties of mobile cloud settings, such as data mobility, resource limits, and network heterogeneity, call for security solutions up to the task. There is also a need for thorough risk assessment approaches to spot and eliminate vulnerabilities in mobile cloud settings. Protecting sensitive healthcare information stored in mobile cloud environments requires filling these knowledge gaps.

3. METHODOLOGY

3.1 Dataset

Essential data samples are derived from the open source research platform, namely, the "open science framework" for investigating the proposed risk assessment model in collaboration with other existing researches. Table 2 represents a wide range of datasets related to COVID-19 affected CVD patient samples on this platform are considered with appropriate clinical and demographic data.

Table 2. Clinical and Demographic characteristics of COVID-19 related CVIs

Characteristics		Overall (N = 1000)	Samples of COVID-19 prevailing CVD patients (N = 500)	Records of COVID-19 recovered CVD patients (N = 500)
Age (Mean ± SD)		38.9±15.7	37.72±15.4	37.72±15.4
Male		534 (53.4)	264 (49.44)	270 (50.56)
Female		466 (46.6)	236 (50.64)	230 (49.36)
CVD Complications due to COVID-19	Acute Cardiac Injury	154 (15.4)	89 (57.8)	65 (42.2)
	Acute Coronary Events	218 (21.8)	111 (50.92)	107 (49.08)
	Left Ventricular Systolic Dysfunction	108 (10.8)	52 (48.14)	56 (51.86)
	Heart Failure	94 (9.4)	46 (48.94)	48 (51.06)
	Arrhythmia	113 (11.3)	51 (45.13)	62 (54.87)
	Myocarditis	87 (8.7)	44 (50.58)	43 (49.42)
	Hypoxic Injury	52 (5.2)	22 (42.31)	30 (57.69)
	Ischemic Injury	35 (3.5)	15 (42.86)	20 (57.14)
	Epicardial Coronary Artery	67 (6.7)	35 (52.24)	32 (47.76)
	Mortality	43 (4.3)	24 (55.81)	19 (44.19)
	Cytokine Storm	29 (2.9)	16 (55.17)	13 (44.83)

3.2 Risk Assessment Model

In this study, we applied Bayesian risk assessment model to assess the risk of CVD in individuals who have COVID-19 symptoms or have been diagnosed with COVID-19 (G, 2020). Mostly, a modern BRAM for CVD with COVID symptoms involves collecting patient data, identifying risk factors, probabilistic modeling, sensitivity analysis, and risk communication.

CVD is a condition that affects the heart and blood vessels and can lead to serious health consequences, including heart attacks, strokes, and heart failure. Figure 2 represents the key steps involved in a modern BRAM for CVD with COVID symptoms.

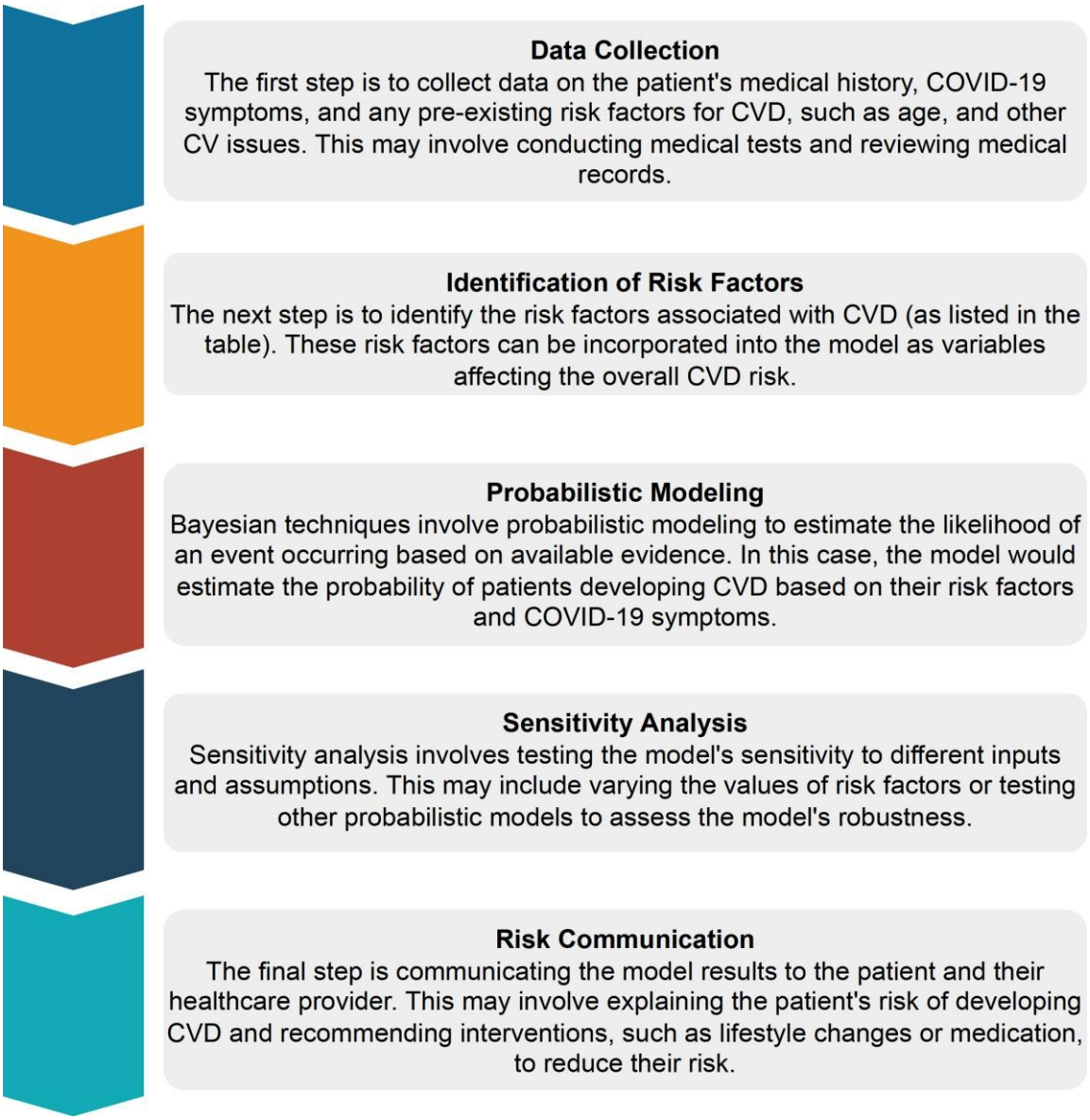


Figure 2. Procedures of BRAM

A mathematical representation of the BRAM for estimating the risk of cardiovascular disease (CVD) in individuals with COVID-19 symptoms is as follows:

Z_i - vector of significant factors (persistence & recovery)

μ_j - disease severity, duration of hospital stay, and therapy

$P(Z_i)$ - probability distribution of population

P(hypertension) - population-at-large incidence of hypertension

The model then applies Bayes' theorem to the updated data, μ_j, to produce a new prior probability distribution:

$$\mathbb{P}\left((Z_i|\mu_j)\right) = \mathbb{P}(Z_i|\mu_j) \times \left[\mathbb{P}(Z_i)/\mathbb{P}(\mu_j)\right] \quad (1)$$

where, $P(\mu_j|Z_i)$ is the likelihood of observing the required data μ_j given Z_i, $P(Z_i|\mu_j)$ is the posterior probability distribution after observing μ_j,

$P(Z_i)$ is the prior probability distribution, and $P(\mu_j)$ is the marginal probability of μ_j.

After determining the posterior probability distribution $P(Z_i|\mu_j)$,, the model generates a probability distribution for the patient's risk of getting CVD, $P(CVD|Z_i,\mu_j)$. It is possible to accomplish so by using a suitable function, $F(Z_i)$, which transfers values of Z_i to the chance of CVD, which can be expressed as,

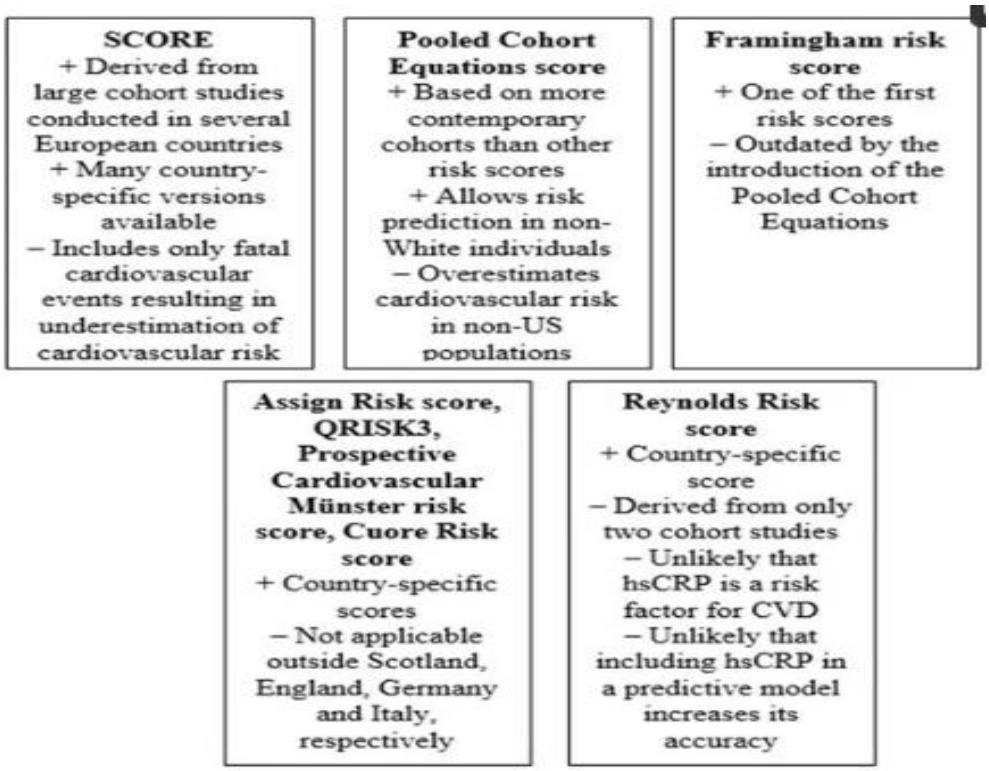
$$\mathbb{P}(\boldsymbol{CVD}|Z_i,\mu_j) = \boldsymbol{F}(Z_i) \quad (2)$$

Finally, the probability distribution can be used to inform clinical decision-making, such as whether to initiate preventive interventions or monitor the patient more closely for CVD with the accuracy of the Bayesian Risk Assessment model depends on the quality of the data and ensuring generalizability.

One risk assessment tool that calculates the 10-year risk of cardiovascular disease (CVD) death is the Systematic Coronary Risk Evaluation (SCORE) model. Age, sex, systolic blood pressure (SBP), total cholesterol

(TC), and smoking status are among the variables that form the basis of the model. There are variations of the SCORE model for low-, high, and very-high-risk nations. These are the risk categories:
Low: 0–4%
Moderate: 5–9%
High: more than 10%

More recent prevalence data can be used to recalibrate the SCORE model at the national level. However, based on the disease's prevalence in the population, the model may exaggerate or underestimate the risk of CVD.
Twelve cohort studies from Europe were used to create the SCORE model. In 2016, the SCORE algorithm was approved for use in the European Society of Cardiology Guidelines. The ESC online offers Heart Score, an electronic version of the SCORE model.



4. SECURE ECOSYSTEM

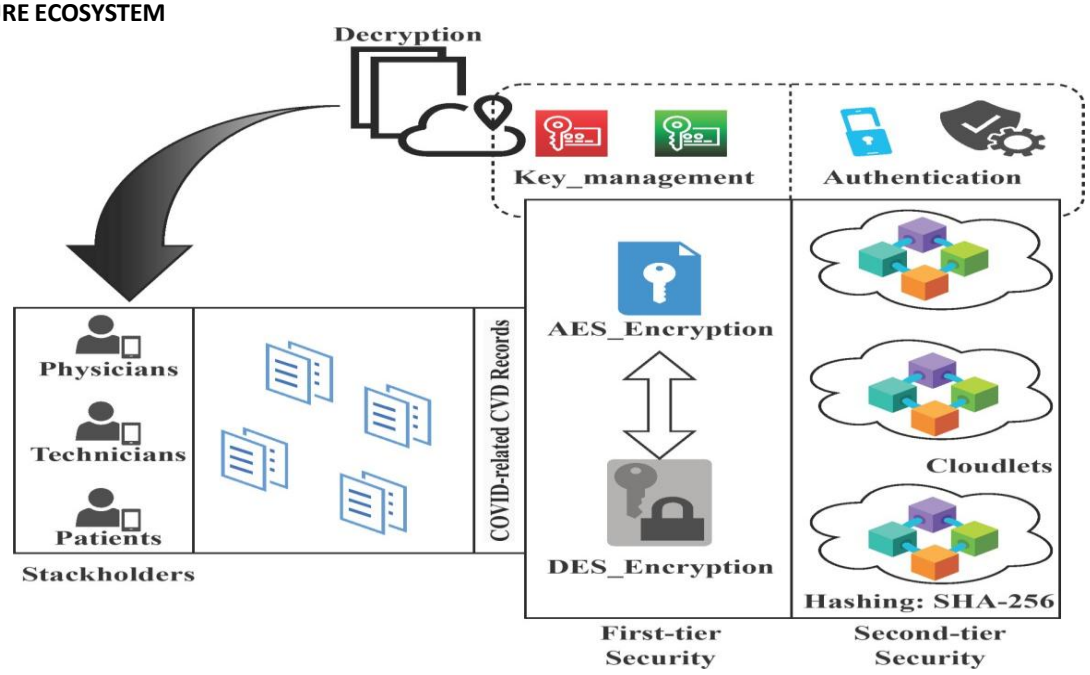


Figure 3. System Architecture

A cybersecurity ecosystem is a safety network that consists of equipment, tools, regulations, and people

who collaborate to safeguard our computers and internet data. It seeks to provide a robust infrastructure in which all elements collaborate harmoniously to detect, stop, lessen, and address various cyberthreats.

Key components of a cybersecurity ecosystem include networks, computers, servers, mobile devices, and the software that runs on them.

Security Tools: specialized software, such as intrusion detection and prevention systems, firewalls, antivirus programs, and encryption tools, that guard these devices.

Rules and Procedures: Policies for handling and preserving cybersecurity in a company, including those pertaining to data backup and recovery, incident response, passwords, and access.

People: All consumers, cybersecurity experts, and IT professionals who use the gadgets.

Standards: Groups and regulations, such as NIST and GDPR, that provide the benchmarks for cybersecurity procedures.

Threat intelligence is the gathering, evaluating, and disseminating of data regarding current and possible dangers.

Partners are outside companies that offer a range of cybersecurity services, solutions, or parts that work with the ecosystem of a business.

4.1 Hybridized Cryptosystem

4.1.1 Implementation of First-tier Security

A hybridized method involves encrypting the AES key via DES and then using AES for the majority of the data. Combining the robust ciphering capabilities of AES with the time-tested and widely used DES technique culminates in obtaining an optimal solution.

AES is used to encrypt the data using a significant key, and then DES is used to encrypt the AES key. When many algorithms are used to encrypt the same data, it becomes far more difficult for an intruder to decode the data, even if they penetrate the encryption of one algorithm. The first tier security system is delineated in the following steps.

Table 3. Procedural steps of First-tier Security

Encryption	Step_1: Generate a random AES key, $\hbar_1$, and can be utilized to encrypt the sensitive CVD information, $\mathbb{D}$. The computation of encryption process (ciphertext) of AES can be represented as: $¢ = a_{aes}(\%, k_1)$ **(3)** Step_2: Generate a random DES key, $\hbar_2$, and use it to encrypt $\hbar_1$ using DES. The encryption operation can be represented as: $\boldsymbol{\kappa} = a_{des}(k_1, k_2)$ **(4)** Step_3: Store both the ¢ and κ securely.
Decryption	Step_4: To decrypt the $\mathbb{D}$, retrieve the κ and decrypt it using DES to obtain $\hbar_1$. The initial decryption process is represented as: $k_1 = \boldsymbol{d}_{des}(\boldsymbol{\kappa}, k_2)$ **(5)** Step_5: Use $\hbar_1$ to decrypt the ¢ using AES to obtain the original data. The decryption operation can be expressed as: $\% = \boldsymbol{d}_{aes}(¢, k_1)$ **(6)**

4.1.2 Implementation of Second-tier Security

With the integration to the first-tier security, the second-tier utilizes blockchain technology to ensure the security of COVID-related CV impairment records in a mobile cloud infra. Table 4 represents the operational processes of second tier security measures along with first-tier.

Table 4. Operational Processes of Second Tier Security Measures

Step_1: To encrypt the data, both equation (3) and (4) are utilized,

$¢ = a(\%, k_1) \oplus \boldsymbol{\kappa} = a_{des}(k_1, k_2)$ **(7)**

Step_2: Compute the hash of the *(ℏ)* using a secure hash function *f(ℏ)* such as SHA-256.

$(\hbar)_¢ = \boldsymbol{SHA-2}(¢)$ **(8)**

Step_3: Store both the κ and the $(\hbar)_¢$ securely in an appropriate *block$_i$* of the blockchain.

Step_4: To retrieve the original data, derive the κ and the $(\hbar)_¢$ from each *block$_i$*.

Step_5: For decryption both equation (5) and (6) are utilized.

$k_1 = \boldsymbol{d}(\boldsymbol{\kappa}, k_2) \oplus \% = \boldsymbol{d}_{aes}(¢, k_1)$ **(9)**

Step_6: Compute the $\hbar$ of the decrypted data using SHA-256.

$\hbar_{\%} = \boldsymbol{SHA-256}(\%)$ **(10)**

Step_7: Compare the computed $\hbar_{\%}$ with the $(\hbar)_¢$ retrieved from the blockchain. If they match, the data has not been tampered with.

The computation process from Tables 3 and 4 defines the steps required to encrypt and decrypt data using the hybrid security process with AES and DES along with blockchain procedures (de-Melo-Diogo et al., 2022). The encryption and decryption part of both AES and DES functions are assumed to be already defined and can be implemented using standard cryptographic libraries or algorithms (Rismayani & Susanto, 2020). It also defines the steps required to hash the outcome of the hybridized security process using AES and DES and store it in a blockchain after hashing.

4.1.3 Implementation of Third-tier Security

A variation of SHA-256, SHA-512 uses eight 64-bit words to provide a 512-bit message digest with a 1024-bit block length. If necessary, the message is first padded to a length of 1024 bits. It is then parsed into 1024-bit message blocks denoted by MB(1), MB(2),…, and MB(N). One by one, each communication block is processed. Hash(0) is the initial predetermined hash value used to start the hashing process. The formula for further hashing values is
hash(i) = hash(i−1) + CFMB (i)(hash(i−1)).

where the Cryptographic Hash (CF) of the i-thmerkle branch is usually represented by CFMB(i). A Merkle Branch (MB) in a merkle tree or hash tree is a collection of node hash values that run from a leaf node to the tree's root. The concatenation operation is represented by +, and the CF of this MB is a hash value that captures the branch's integrity.

4.1.4 Key management and Authentication

Data confidentiality and integrity are ensured by using key management and authentication in a hybrid security paradigm that employs both the AES and DES encryption
algorithms along with blockchain technology. We provide a potential mathematical approach for handling keys and authentication for a hybridized security paradigm.
Key generation: A master key is generated using a secure random number generator. This master key is used to generate sub-keys for both AES and DES encryption techniques.

Let M_K be the master key, and let *f(KDF)* be the key derivation function used to generate subkeys for AES and DES.

$$M_K = random()\ AES\_key = f(KDF)\ (M_K, "AES")\ DES\_key = f(KDF)\ (M_K, "DES") \quad (11)$$

Sub-key generation: The M_K is passed through a *f(KDF)* to generate sub-keys for both AES and DES. The *f(KDF)* is typically a secure one-way function that takes the M_K and produces a set of unique and unpredictable subkeys. One most popular *f(KDF)* is HKDF, which takes the M_K, an optional salt-value ϕ, and an optional context string Ֆ to produce two sub-keys: one for AES and one for DES.

$$HKDF(M_K, \boldsymbol{\phi}, \boldsymbol{Ֆ}) = (M_K\_AES, M_K\_DES) \quad (12)$$

where K_AES = HMAC(M_K, "AES" || $\boldsymbol{\phi}$ || $\boldsymbol{Ֆ}$) and K_DES = HMAC(M_K, "AES" || $\boldsymbol{\phi}$ || $\boldsymbol{Ֆ}$)

Encryption and decryption: AES and DES are used in combination to encrypt and decrypt data. AES is used for the bulk of the data while DES is used for key exchange and initialization vector (ψ) generation.

For encryption: Let „Ƭ‟ be the original data, ¢ be the ciphertext information, a_k be the AES sub-key, and d_k be the DES sub-key.

$$\psi = a[\boldsymbol{rand}(), \boldsymbol{d_k}];\ ¢ = a_{\boldsymbol{aes}}(Ƭ, \boldsymbol{a_k}, \psi) \quad (13)$$

For decryption: Let ¢ be the ciphertext message, „Ƭ‟ be the original data, a_k be the AES sub-key, and d_k be the DES sub-key.

$$\psi = \boldsymbol{d}[¢[:\boldsymbol{8}], \boldsymbol{d_k}];\ Ƭ = \boldsymbol{d_{aes}}(\boldsymbol{a_k}, \psi) \quad (14)$$

Authentication: Authentication is performed using MAC algorithm such as HMAC. The MAC is calculated over the ¢ along with a secret key shared between the patients and stakeholders. This ensures that the data has not been tampered with during transmission.

For HMAC: Let R be the real data, S_K be the secret key shared between the sender and receiver, and $\hbar$ be the hash function used in the HMAC algorithm (Kumar et al., 2011).

$$\boldsymbol{G_{tag}} = \hbar[\boldsymbol{S_K} \oplus \boldsymbol{O_{pad}} || \hbar(\boldsymbol{S_K} \oplus \boldsymbol{I_{pad}} || \boldsymbol{R})] \quad (15)$$

where, outer_padding (O_{pad}) and inner padding (I_{pad}) are constants which are specified as:
O_{pad} = 0x5c5c5c. . .5c5c5c //64 times
I_{pad} = 0x363636. . .363636 //64 times

Computation: To compute a MAC (Θ) over a ¢ using HMAC with a S_K, the following equation is employed:

$$\boldsymbol{\Theta} = \boldsymbol{H}(\boldsymbol{S_K}, ¢) \quad (16)$$

Verification: To verify a received *Θ''* outcome over a computed ¢″, the following equation is applied:

$$\boldsymbol{\Theta}'' = \boldsymbol{H}(\boldsymbol{S_K}, ¢'') \quad (17)$$

IF *Θ = = Θ''*:

 # Authentication successful
ELSE: ***# Authentication failed***

Overall, this in-depth equation-based working mechanism ensures that the data is encrypted securely using both AES and DES, with key management and authentication measures in place to protect the data stored in the blockchain. But it is also essential to ensure the transaction authentication over mobile cloud, which accomplishes the primary objective of the security ecosystem.

4.1.5 Transaction Authentication

The complete details of the utilized transaction authentication process are delineated in a step-by-step manner in the table 5.

Table 5. Procedures of Transaction Authentication

Input: $\mathbb{D}$
1: $\hbar_{\%} = SHA - 256(\%)$ *//Compute the hash of the data using a secure cryptographic hash function*
2: $t_i(\%) = \{\hbar_{\%}, \%\}$ *//Create a transaction with the HashedData as a metadata field*
3: Broadcast the t_i to the network.
4: The t_i is validated by MC nodes, n_i and added to the $block_i$ in blockchain.
5: Compute the $\hbar$ of the t_i by $f(\hbar) \rightarrow t_i(\mathbb{D})$ using the same hash function utilized in step 2.
6: Add the computed $\hbar[t_i]$ to the $block_i$ as the transaction_ID, and store the transaction metadata.
7: $B_m \leftarrow \{block_1, block_2, \cdots, block_n\}$ *//Add the block to the blockchain, and create a new block for subsequent transactions*
8: update $\{block_1, block_2, \cdots, block_n\} \rightarrow n_i$

The above algorithm defines the steps required to store the hash data for transactions in a blockchain using a secure cryptographic hash function, SHA-256. The algorithm includes the creation of a transaction with the Hashed Data as a metadata field, broadcasting the transaction to the network, and adding the computed Hashed Transaction to the blockchain as the transaction identifier.

5. Performance Evaluation

Performance evaluation is crucial to validating any proposed system, including a secure ecosystem for preserving COVID-related CV impairment records in a mobile cloud infra. This is because performance evaluation allows for measuring various performance metrics and indicators, such as confidentiality rate and other comparisons like vulnerability index Vs Protection index and protection index Vs attack index.

In the case of a secure ecosystem for preserving COVID-related cardio-vascular impairment records in a mobile cloud infrastructure, performance evaluation is particularly important due to the sensitive nature of the data being stored and transmitted. Any delays or inefficiencies in the system's performance could result in significant consequences, such as compromised patient data, delayed treatment, or even loss of life.

Moreover, performance evaluation helps to identify potential bottlenecks, weaknesses, and areas for improvement in the system, which can be addressed before the system is deployed in a real-world setting. This can help to ensure that the system functions optimally, securely, and reliably, even under stressful conditions. The evaluation metrics are elaborated to understand yielded performance from the proposed system. Moreover, the outcomes are compared with a few existing models to maximize the research view.

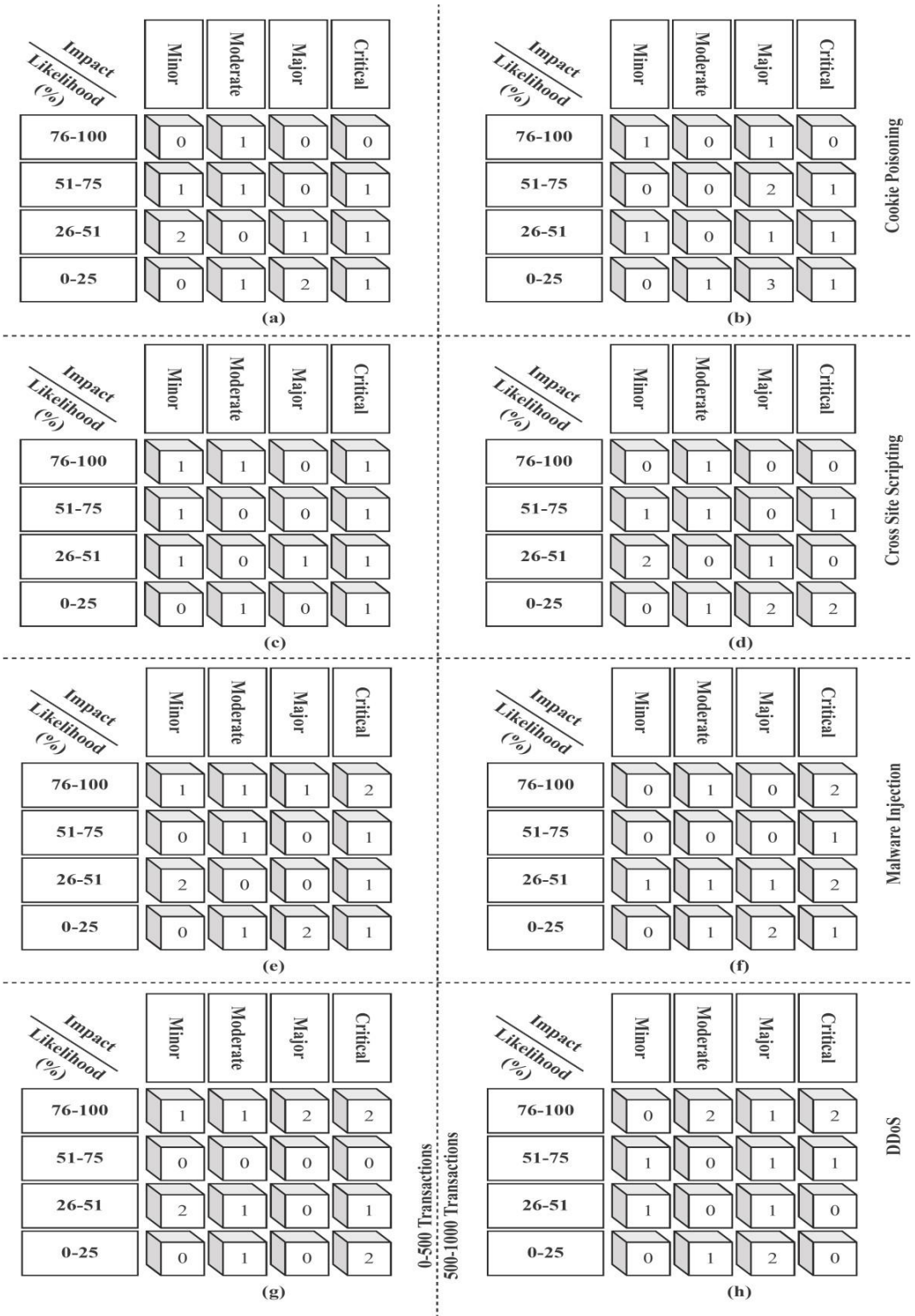


Figure 4. Risk Matrix

The proposed ecosystem is compared with the existing methodology to check the performance. Few recent research work from Sabeena et al. (2024), Eljim et al. (2024), Tungar D.V (2023), Abdul et al. (2022), Arumugam et al. (2021), and Zkik et al. (2019) are considered for the comparative evaluation with suggested model.

The BRAM-based risk matrix is obtained with specific outcomes against various attacks and represented is represented from figure 4(a) to 4(h). The matrix uses a Bayesian network to model the likelihood of an attack occurring and the potential impact of the attack. The matrix then assigns a risk score to each attack based on the likelihood and impact, which can be used to prioritize resources and efforts for mitigating the risks. The outcome is analyzed based on four risk probability

terms, namely, minor, moderate, major, and critical. Each risk matrix represents the risk probability of all four attacks in two scenarios, i) 0-500 transactions and ii) 500-1000 transactions. In the matrix resultants, it is noted that the risk score is high as the transaction increases. Categorization of risk probability based on four probability terms makes precise implications regarding the proposed model which organizes for better understanding and prioritize their security risks, and allocate resources and efforts to mitigate those risks in a more effective and efficient manner.

5.1 Confidentiality rate

The confidentiality rate of a proposed cryptosystem can be calculated using the same equation for entropy or randomness. The higher the entropy or randomness, the more secure and confidential the cryptosystem is considered to be.

Here is the equation to calculate the confidentiality rate of a proposed cryptosystem:

$$\varepsilon = -\sum[\mathbb{p}(k) \cdot \mathbf{log_2}\ \mathbb{p}(k)]$$

where, ε denotes entropy or randomness of the proposed cryptosystem, $\mathbb{p}(k)$ probability of a keys being used in the cryptosystem.

The confidentiality rate of the proposed cryptosystem can be calculated by determining the entropy or randomness of the *ƙ's* used in the system. The *ε* value can be used to assess the level of confidentiality in a system, as a system with high *ε* is more difficult to predict or guess. This involves calculating the probability of each possible *ƙ* being used and applied in the above equation.

Most security models aim to achieve good confidentiality rates because maintaining confidentiality is a fundamental aspect of security. From the figure 5, it is notable that the proposed secure ecosystem manages to surpass the existing models in achieving required confidential rate via high *ε* value. Such a high value implies that the suggested model possess high complexity in breaching the secured data. All the models are evaluated for varied data size. It is also noted, as the size of the data increases the *ε* value gradually decreases, which specifies the intricacy process of the security process. The average *ε* value of the proposed model is 0.804 whereas for other models, it is recorded as 0.734. High entropy values mean that there is greater randomness in the data. This makes it more difficult for an attacker to predict the value of the data, increasing the security of the data. Random keys are important for the security of the system because they make it more difficult for an attacker to guess the key and gain access to the encrypted data. The working mechanism of Adbul et al. (2022) performed poorly then the other models, since it involves in the misconfiguration of access control policies which has resulted in unintended consequences, such as denying legitimate access or granting authorized access. This requires careful management and monitoring to ensure that access control policies are properly configured.

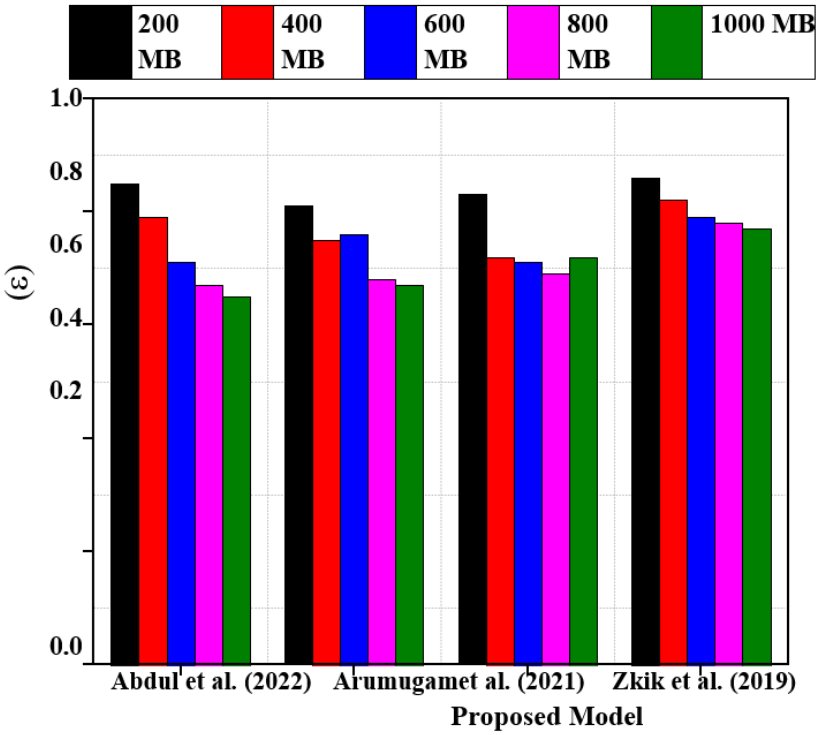


Figure 5. Analysis of Confidentiality Rate

5.2 Vulnerability Index

Assessing vulnerability of a cryptosystem involves examining multiple factors that contribute to the susceptibility of the system to attacks or exploits. Some common factors that are often considered in vulnerability assessments of cryptosystems include: Resistance to Attacks (r), Key Management (k_M), Strength of Encryption (e_s), External Dependencies (þ). The VI of the proposed model is validated by assigning different a weight score (*w*) on the scale of 0 to1 to each of the vital factors.

$$\boldsymbol{VI} = [(\boldsymbol{r} \times \boldsymbol{w}_r) + (\boldsymbol{k_M} \times \boldsymbol{w}_{k_M}) + (a_s \times \boldsymbol{w}_{a_S}) + (þ \times \boldsymbol{w}_þ)]$$

The degree to which the encryption algorithm used in the system can withstand attacks from malicious actors. The effectiveness of the system's key management practices, such as key generation, storage, distribution, and revocation. The system's vulnerability to attacks from outside sources, like operating systems, network infrastructure, or other software components. Similarly, the attack index may also take into account the potential attacker's resources, such as computing power, available time, and knowledge of the system. The proposed model is validated against user-level security model which is poses a significant risk at application level. Thus rare type of attacks like Cookie Poisoning, Cross Site Scripting, Malware Injection, DDoS are considered for validating both attack and protection index (Singh, 2018).

In general, a higher protection index and a lower vulnerability index are desired. The protection index refers to the strength and effectiveness of the security measures implemented to prevent cookie poisoning, malware injection, cross site scripting and DDoS attacks. This can include measures such as using implementing secure encryption algorithms, and using access control mechanisms (e.g., two-level security) to limit access to sensitive data and systems. Figure 6(a), 6(b), 6(c), and 6(d) represents the protection index of all the considered models against the vulnerability index for four different attacks, respectively. In all the outcomes, it is observed that the proposed model succeeds in attaining the reasonable protection index against possible vulnerable index. For cookie poisoning and cross site scripting, the protection index of the suggested model is maintained at above 0.927 whereas for malware injection and DDoS, is it maintained at above 0.946. Thus, the result implies that the likelihood and severity of such attacks are minimized. Moreover, the proposed model excelled all other existing model, since the average protection index of all other models is 0.892.

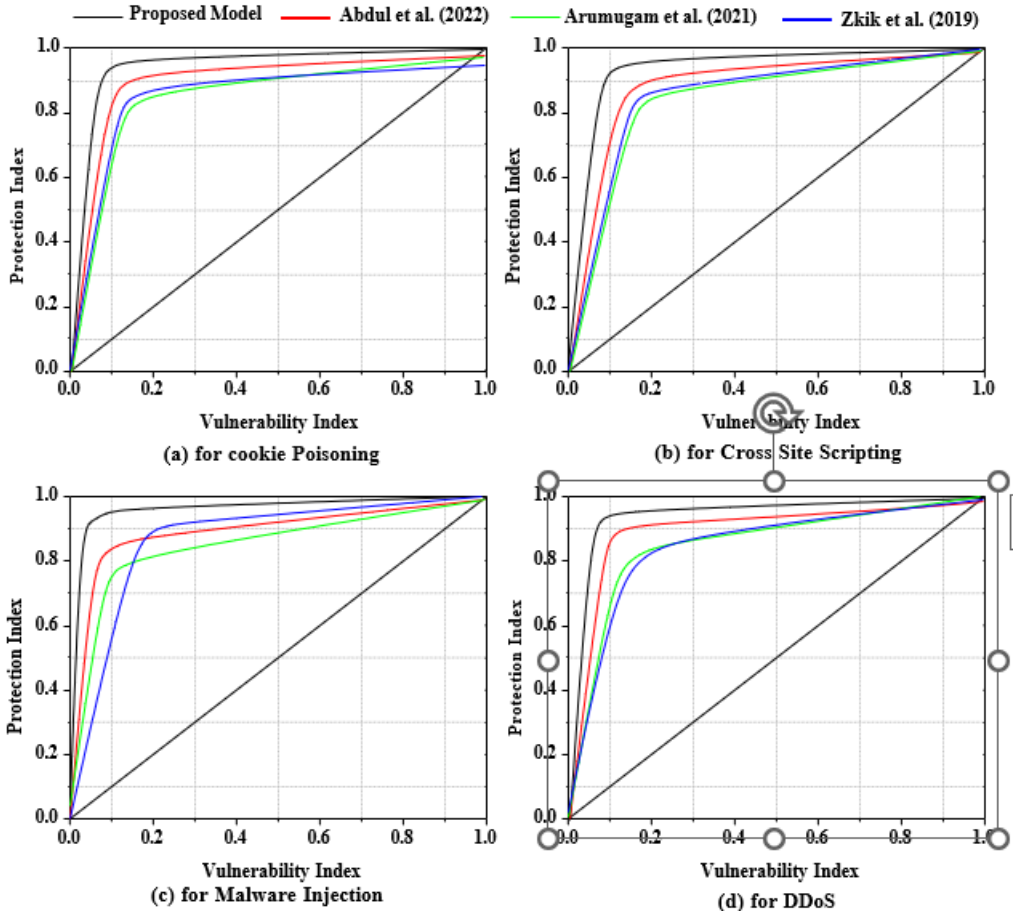


Figure 6. Protection Index Vs Vulnerability Index against Various Attacks

The optimal protection index and attack index of various cyber attacks can vary depending on multiple factors, including the nature of the attack, the target system, and the attacker's skill level. Other than cookie poisoning, the suggested model attained optimal protection index (0.78±0.11) against cross-site scripting, malware injection, and DDoS attacks, which is represented in figure 7. For cookie poisoning, the average protection index of 0.58 is achieved, which is due to utilization of cookies stored in an insecure format, and dynamic vulnerable web applications. Since the proposed model implements best security practices, it attained an optimal protection index against various cyber attacks in mobile cloud infrastructure.

However, it is important to note that the threat landscape is constantly evolving, and attackers are continually developing new and more sophisticated attack techniques. Therefore, it is crucial to stay up to date with the latest security trends and best practices and regularly assess and test systems to identify and remediate vulnerabilities before attackers can exploit them.

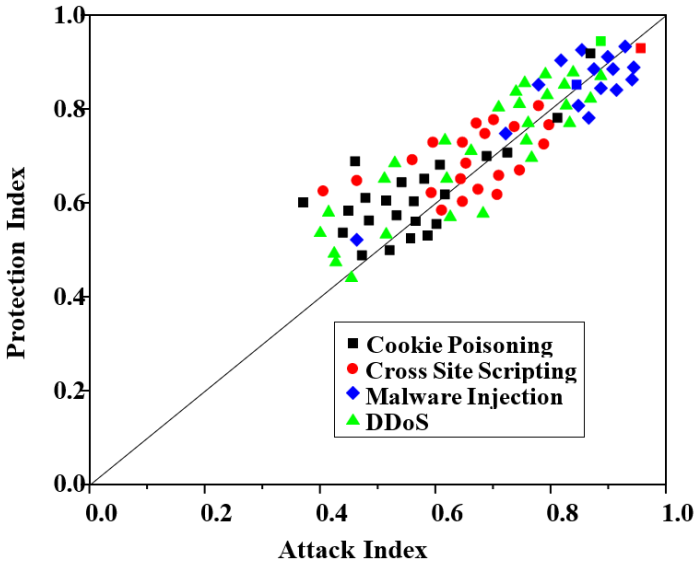


Figure 7. Protection Index Vs Vulnerability Index against Various Attacks

6. CONCLUSION AND FUTURE WORK

In this research work, a secure ecosystem is established for preserving COVID-related cardiovascular impairment records in a mobile cloud infrastructure with block chain technology. This can help ensure that patient data is protected and that researchers and healthcare providers have access to the data they need to better understand the impact of COVID-19 on cardiovascular health. In this investigation, the risk of CVD associated with COVID symptoms is predicted using the Bayesian method. With a well-thought-out MC strategic strategy and cutting-edge security measures, we can keep all of the relevant data safe and sound. These safety measures ensure that the end user may access CVD data without any kind of danger. The risk-assessed records in the MC infra that pertain to CVD have been given three layers of protection. In order to authenticate and validate the lawful data transaction process, the first layer of security uses the DES ,AES and SHA-512 algorithms. On the other hand, the second level features progressive security orders and blockchain-based integrity.

The suggested MC ecosystem is compared to three current security techniques to provide light on the fundamental findings and inquiries. The study of results shows how the two-tier security approach and the authentication of data transfers in MC infra affected the outcome.

In the future, we plan to utilize artificial intelligence and machine learning algorithms, which makes the system to identify patterns and trends in the data that may be difficult for humans to detect. These algorithms can help healthcare providers and researchers to better understand the impact of COVID-19 on cardiovascular health and develop more effective treatments.

REFERENCES

1. S. Jenifa Sabeena, & S. Antelin Vijila. (2024). Exchanged Secure Hashing Algorithm (ESHA-512) For Blockchain Technology. Journal of Computational Analysis and Applications (JoCAAA), 33(07), 476–486. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1084
2. Sean Eljim S et al. (2024). Modification of SHA-512 using Bcrypt and salt for secure email hashing. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 33, No. 1, January 2024, pp. 398~404. ISSN: 2502-4752, DOI:

10.11591/ijeecs.v33.i1.pp398-404
3. D. V. , T. ., & D. V., P. . (2023). Evaluation of Privacy-Preserving Techniques: Bouncy Castle Encryption and Machine Learning Algorithms for Secure Classification of Sensitive Data. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(7s), 429 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2976
4. Abdul, A. M., Mohammad, A. A. K., Venkat Reddy, P., Nuthakki, P., Kancharla, R., Joshi, R., & Kannaiya Raja, N. (2022). Enhancing Security of Mobile Cloud Computing by Trust- and Role-Based Access Control. Scientific Programming, 2022, 1–10. https://doi.org/10.1155/2022/9995023
5. Arumugam, M., Deepa, S., Arun, G., Sathishkumar, P., & Jeevanantham, K. (2021). Secure data sharing for mobile cloud computing using RSA. IOP Conference Series: Materials Science and Engineering, 1055(1), 012108. https://doi.org/10.1088/1757-899x/1055/1/012108
6. Chondamrongkul, N., & Chondamrongkul, P. (2017). Secure Mobile Cloud Architecture for Healthcare Application. International Journal of Future Computer and Communication, 6(3), 76–80. https://doi.org/10.18178/ijfcc.2017.6.3.493
7. de-Melo-Diogo, M., Tavares, J., & Nunes Luís, Â. (2022). Data Security in Clinical Trials Using Blockchain Technology. Research Anthology on Convergence of Blockchain, Internet of Things, and Security, 607–625. https://doi.org/10.4018/978-1-6684-7132-6.ch034
8. Farrugia, S. (2016). Mobile Cloud Computing Techniques for Extending Computation and Resources in Mobile Devices. 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). https://doi.org/10.1109/mobilecloud.2016.26
9. Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29(1), 84–106. https://doi.org/10.1016/j.future.2012.05.023
10. G, P. (2020). Extending the Range of COVID-19 Risk Factors in a Bayesian Network Model for Personalised Risk Assessment. Epidemiology International Journal, 4(6). https://doi.org/10.23880/eij-16000170
11. Han, Q., Liang, S., & Zhang, H. (2015). Mobile cloud sensing, big data, and 5G networks make an intelligent and smart world. IEEE Network, 29(2), 40–45. https://doi.org/10.1109/MNET.2015.7064901
12. Hunter, P. (2020). The spread of the COVID -19 coronavirus. EMBO Reports, 1. https://doi.org/10.15252/embr.202050334
13. Kumar, M., Avasthi, A., & Gaurav, G. (2011). Advancing the Cryptographic Hash-Based Message Authentication Code. International Journal of Engineering and Technology, 3(3), 269–273. https://doi.org/10.7763/ijet.2011.v3.236
14. M, S., & Shalinie S, M. (2018). Provable dynamic auditing in mobile cloud computing for secure storage of ehealth data. Biomedical Research. https://doi.org/10.4066/biomedicalresearch.29-17-824
15. Mobile Cloud Computation: Issues and Challenges. (2017). International Journal of Recent Trends in Engineering and Research, 3(4), 388–396. https://doi.org/10.23883/ijrter.2017.3162.n9xny
16. Nasiraee, H., & Ashouri-Talouki, M. (2018). Dependable and Robust Attribute-Based Encryption in Mobile Cloud Computing. Electrical Engineering (ICEE), Iranian Conference On. https://doi.org/10.1109/icee.2018.8472519
17. Parameswari, R., & Vani, K. (2018). Mobile Cloud-Privacy and Data Security in Healthcare Environment Using Cloudsim Simulator. International Journal of Engineering & Technology, 7(3.27), 220. https://doi.org/10.14419/ijet.v7i3.27.17880
18. Raghunath, K. M. K., Kumar, V. V., Venkatesan, M., Singh, K. K., Mahesh, T. R., & Singh, A. (2022). XGBoost Regression Classifier (XRC) Model for Cyber Attack Detection and Classification Using Inception V4. Journal of Web Engineering. https://doi.org/10.13052/jwe1540-9589.21413
19. Rismayani, & Susanto, C. (2020). Using AES and DES Cryptography for System Development File Submission Security Mobile-Based. 2020 8th International Conference on Cyber and IT Service Management (CITSM). https://doi.org/10.1109/citsm50537.2020.9268805
20. Rodrigues, A. M. (2017). Perception of Patients about Cardiovascular Disease (CVD) and Effect of Communication by Physician and the Assisting Registered Nurse to Enhance Assessment of Risk and Bridge a Gap of Accurate Perception of their Risk of CVD. TEXILA INTERNATIONAL JOURNAL of NURSING, 3(2), 167–174. https://doi.org/10.21522/tijnr.2015.03.02.art016
21. Singh, H. P. (2018). Survey of new attack models on Cloud Infrastructure. International Journal of Engineering and Computer Science, 7(03), 23742–23752. https://doi.org/10.18535/ijecs/v7i3.15
22. Sobh, T. S., & Khalil, A. H. (2022). Securing Hybrid Architecture of Cloudlet Computing in 5G Networks Enabling IoT and Mobile Wireless Devices. Recent Advances in Computer Science and Communications, 15. https://doi.org/10.2174/2666255815666220513100

0257

Author
M. Anitha (Anitha Marimuthu) is a Computer Science and Engineering Assistant Professor at Kingston Engineering College, Vellore, Tamilnadu. She has about 18 years of teaching experience in educational field. She has 5 years of research experience in the field of Mobile Cloud Computing and Block Chain. She completed his B.E Degree in Computer Science and Engineering with First class from Bharathidasan University, Trichy and M.E Degree in Computer Science and Engineering with First class from Anna University, Chennai.
Mailid: anitham.apcse@gmail.com

Co-Author
Dr Sakthivel S (Sakthivel Subramaniam) is a Computer Science and Engineering Professor at Sona College of Technology, Salem, Tamil Nadu, India. He obtained his M.E. and PhD from Anna University, Chennai, Tamil Nadu, India. His research interests include Pattern Recognition, Image Processing, Biometric Systems, Cryptography and Network Security and Computation complexity Problems. He is a life member of ACM and the Indian Society of Technical Education.
Mailid: sakvel75@gmail.com