SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I12P118

Volume 11 Issue 12, 189-205, December 2024

Original Article

An Efficient Hybrid Elliptic Curve Cryptography for Securing E-Healthcare Data in Cloud Environment

D. Nagamany Abirami[1], M. S. Anbarasi[2]

[1]*Department of Computer Science and Engineering, Puducherry Technological University, India.*
[2]*Department of Information Technology, Puducherry Technological University, Puducherry, India*

[1]*Corresponding Author : abiramimtech@gmail.com*

Received: 23 October 2024 Revised: 27 November 2024 Accepted: 14 December 2024 Published: 30 December 2024

Abstract *- After COVID-19, establishing medical and health records, telemedicine, and mobile treatment has shown the potential to strengthen the healthcare system. Cloud computing is a major part of data communication between patients and medical experts. In healthcare, cloud computing stores and manages large volumes of data, such as Electronic Medical Records (EMRs), patient data, and medical images. Healthcare data contains very sensitive data that needs to be protected from hackers. This paper proposes a comprehensive security framework explicitly tailored for e-health systems, strengthened by integrating Advanced Elliptic Curve Cryptography (AECC) techniques, utilizing a hybrid approach combining Weierstrass and Montgomery forms. The framework addresses various security concerns in e-health systems, including data confidentiality, integrity, availability, and privacy. By leveraging a hybrid AECC approach, combining the advantages of both Weierstrass and Montgomery forms, the framework enhances the encryption and decryption processes critical for safeguarding sensitive health information. Key components of the proposed framework include robust access control mechanisms, advanced data encryption strategies, secure data transmission protocols, and resilient authentication mechanisms. By leveraging the strengths of both Weierstrass and Montgomery forms, the framework balances security and computational efficiency, ensuring seamless operation within cloud environments while maintaining robust protection for sensitive healthcare information. The efficiency of the proposed security framework is evaluated through comprehensive simulations and performance analyses, demonstrating its effectiveness in safeguarding e-health data while minimizing computational overhead. The results indicate that the hybrid ECC approach offers a practical and efficient solution for securing e-health systems and enhancing trust and compliance with regulatory requirements in the healthcare domain.*

Keywords *- e-Health systems, Comprehensive security framework, Advanced Elliptic Curve Cryptography, Data encryption, Data integrity, Access control, Cloud computing, Data privacy.*

1. Introduction

As the health industry moves towards population health, automation of the health care system became a must-have ¨ criteria. Healthcare providers are insufficient in number to continually track and search for the latest treatment model for broader patient populations [1]. The financial information of a typical hospital states that 50%-60% of the cost was spent on salaries and compensation. Healthcare is an inflationary system by default, but it is complicated because everyone chooses to appoint more people instead of worrying about survival with several people. In this healthcare industry, the challenges are to get people involved in the work and recognize them for looking at creative making and use of innovation for faster and cheaper completion [2].

The present Scenario of analyzing the Electronic Health Record (EHR) outcome lacks computer literacy among healthcare providers and user-centered design for efficient use. There is no uniformity in EHR software maintained globally, which results in poor change management practices and communication [3]. Also, there is a shortage of collaboration between healthcare professionals, leading to non-interoperability and "Data hugging" by clinical establishments. Moreover, people in clinical research are quite unaware of the privacy and health information security protocols. There is no mandatory requirement for the current health care system to electronically track and report to a centralized nodal agency on clinical outcomes. The government provides no integrated healthcare portal/software for all stakeholders to plug and play with citizen health records [4].

Medical diagnosis presents a great deal of difficulties. The healthcare systems are flawed in their structure to encourage safe and accurate diagnostics, which is the root cause of the diagnostic mistakes. The reality is that doctors may not be giving enough thought to the mental component of medicine—the process of generating accurate diagnoses [5]. Cloud computing has convenient features for sharing and distributing goods and has become widely used in today's digital world. Cloud computing offers a user-oriented platform for sharing resources such as applications, servers, networks, and storage. The cloud

is characterized by two main features: storage, a method for storing data, and data sharing, transmitting data from one individual to another [6].

Users may store and share their personal, financial, and corporate data in the cloud, a virtual storage system utilized on demand. The public cloud includes platforms such as Google Application Engine and Windows Azure. As for the second, it is a private cloud tailored to a single company and uses on-site or off-site servers [7]. It outshines the previously described cloud solution in terms of security and offers superior personalization options. Companies like Dell, IBM, Cisco, and HP are examples of this cloud system. Figures 1 (a) and (b) depict the fundamentals of public and private e-health cloud systems, respectively.

A type of health system known as an e-health system stores and shares medical records between patients and healthcare professionals through computers, electronic systems, and cloud computing, as the name implies [8]. Patients can access P-HR's mobile health services, which allow them to upload and share their health records, among the several P-HR cloud providers. With the help of e-health services, which include a more reliable method of transmitting medical records over the Internet, doctors and other medical professionals can keep tabs on their patients in real-time, which improves the quality of care they provide by allowing for more precise diagnosis and treatment [9].

Maintaining the integrity and accuracy of patient data while it travels across the network is of the utmost importance. Therefore, we are doing all in our power to reduce potential threats. Quickly transitioning from a paper-based healthcare system to a digital one has made data management an even more pressing issue, and dealing with an ever-increasing volume of data is no easy feat [10]. From now on, any cloud-based e-health system will adhere to all applicable security standards, guaranteeing constant data availability regardless of location or time of day, ensuring user and data background authentication, protecting data integrity, and keeping data confidential while in transit [11].

Crypto techniques, including symmetric and asymmetric encryption, attribute-based encryption, and hybrid methods, are one of the three approaches to attain security. There is also the option of using non-crypto approaches, such as role-based policy implementation or access control, to specify the responsibilities and permissions of each user [12]. The third type of authentication and authorization system relies on a person's unique biometric characteristics. The security mechanisms are classified according to the principles of biometrics and cryptography. Biometrics refers to using an individual's unique physical characteristics for authentication and authorization purposes, while cryptography refers to the practice of encrypting and decrypting data using various crypto methods [13].

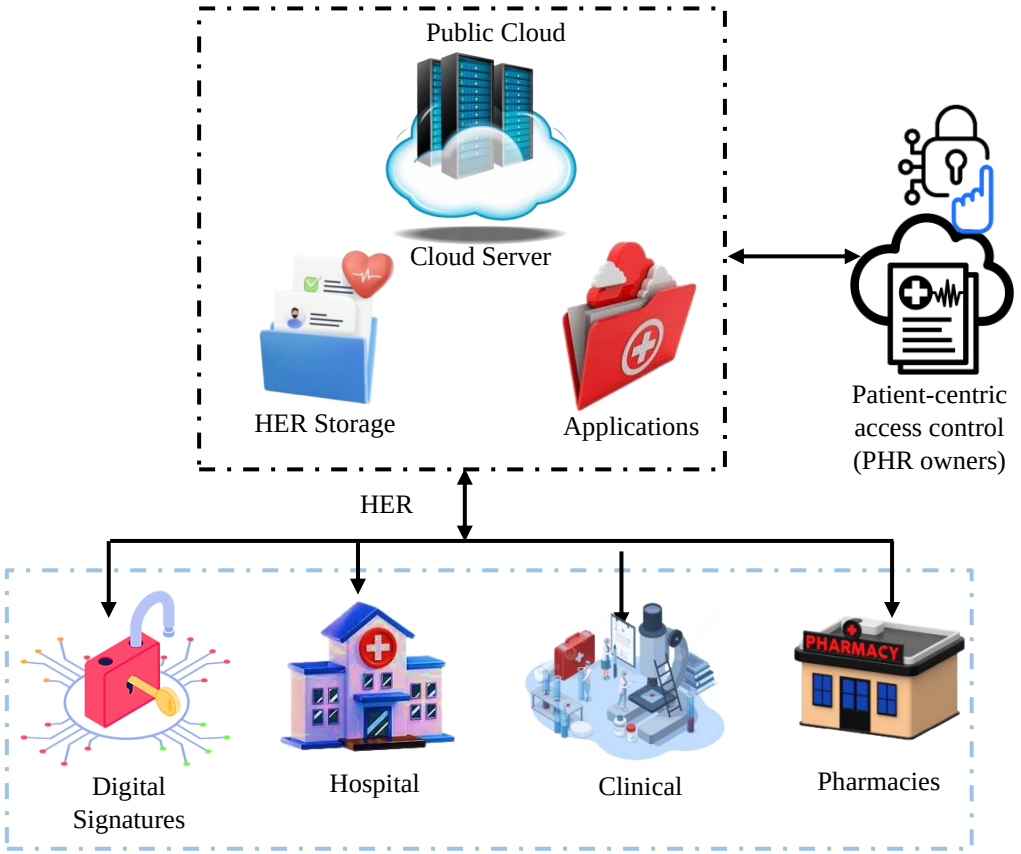

Fig. 1 (a) Public e-health cloud system

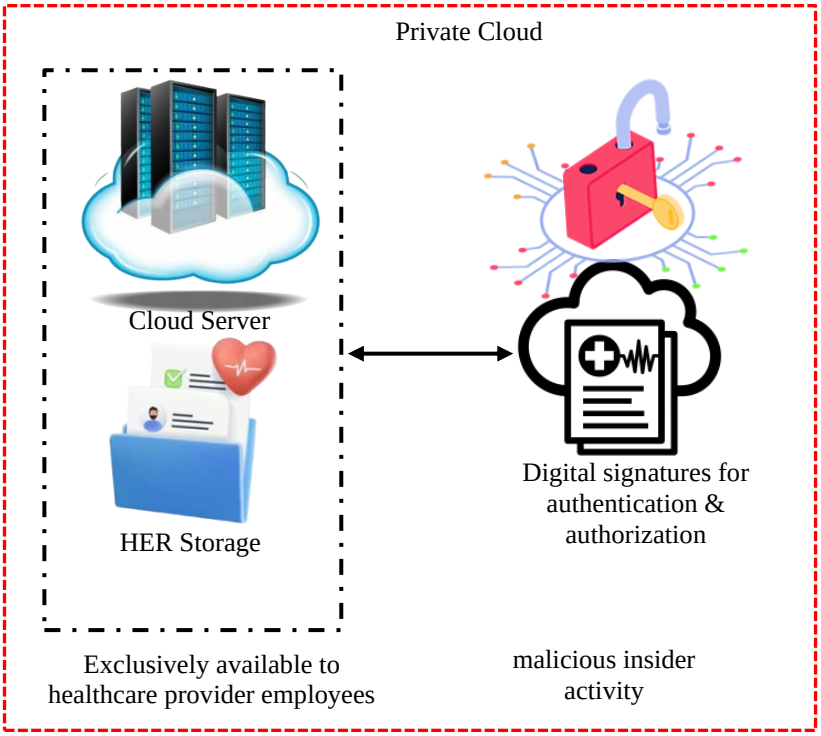

Fig. 2 (b) Private e-health cloud system

The non-crypto approach encompasses all other security measures that do not rely on biometric or cryptographic techniques. To ensure that cloud-based e-health systems can securely store and transmit patient health data across public clouds, gather as much information as possible on how to keep these systems' security requirements in check [14].

1.1. Problem Statement

Integrating e-health systems into cloud environments presents a pressing challenge in ensuring the security of sensitive patient data. While the cloud offers scalability and accessibility benefits, it also introduces vulnerabilities to unauthorized access and data breaches. Existing security measures often struggle to address these challenges comprehensively, leaving e-health systems exposed to potential exploitation. Moreover, the dynamic nature of cloud environments complicates security efforts further. Therefore, there is an urgent need for a tailored security framework that can effectively safeguard e-health data in the cloud. Such a framework must prioritize data confidentiality, integrity, access control, and authentication while leveraging advanced technologies to mitigate evolving threats. By addressing these concerns, healthcare providers can enhance patient trust and ensure compliance with regulatory standards, ultimately fostering the secure and efficient delivery of e-health services.

1.2. Motivation

- Growing cyber threats: Healthcare organizations face a surge in cyberattacks, including ransomware and data breaches, highlighting the urgent need for enhanced security protocols.
- Regulatory compliance requirements: Stringent regulations such as HIPAA and GDPR mandate the implementation of strong security frameworks to ensure patient privacy and data integrity.
- Safeguarding patient confidentiality and trust: Ensuring the security of e-health systems data in cloud environments is crucial for maintaining patient confidentiality and fostering trust in healthcare services.

1.3. Objectives

1.3.1. Improve Data Confidentiality

Use cutting-edge ECC methods to encrypt all e-Health data before it is saved or sent to the cloud, ensuring that no one other than authorized users can decipher it.

1.3.2. Ensure Data Integrity

Utilize ECC to verify the integrity of e-Health data, detecting any unauthorized modifications or tampering attempts throughout its lifecycle within the cloud environment.

1.3.3. Strengthen Access Control Mechanisms

Develop robust access control policies leveraging ECC-based authentication mechanisms to regulate and restrict data access based on user roles and privileges.

1.3.4. Optimize Resource Efficiency

Design ECC algorithms optimized for cloud environments to minimize computational overhead and resource utilization while maintaining high-level security for e-Health data.

1.3.5. Ensure Regulatory Compliance

Align the security framework with relevant regulatory standards such as HIPAA, GDPR, and others to ensure compliance with data protection and privacy regulations governing e-health systems.

1.3.6. Facilitate Seamless Integration

Design the security framework to seamlessly integrate with existing e-Health systems and cloud infrastructure, minimizing disruption to workflows and operations.

1.3.7. Provide Scalability and Flexibility

Ensure that the security framework can scale effectively to accommodate the dynamic nature of e-health systems and evolving cloud environments, providing flexibility to adapt to changing requirements.

1.3.8. Enhance Trust and Confidence

By implementing a comprehensive security framework enhanced by Advanced ECC, the aim is to enhance trust and confidence among healthcare providers, patients, and other stakeholders regarding the confidentiality, integrity, and security of e-health data in the cloud system.

2. Related Works

When patients receive high-quality therapy to prevent or treat an illness, they say they receive healthcare. Healthcare services are provided to patients in a hospital setting and at their homes. The healthcare business has seen constant changes in software and technology since the middle of the past century [15]. This leads to the development of new technologies that enhance patients' lifestyles and healthcare while reducing costs and saving time. The healthcare business has gone through many generations, beginning with healthcare industry V.1.0 in the 1970s and continuing up to healthcare industry V.4.0 in the present day [16]. Automated wireless medical sensors began making preliminary decisions about patients' health and alerting them in 2015, marking the beginning of healthcare generation V.4.0. Deployment of intelligent sensing technology is progressing rapidly, allowing for precise patient decision-making in real-time regardless of location or time constraints. The third. An HIS [17] is a system that facilitates the administration of healthcare data, including the gathering, storing, managing, and transmission of an individual's Electronic Health Record (EHR), assists with the operational administration of a healthcare facility, and offers a foundation for policy decisions about healthcare data. Gen. V.4.0 HIS technology includes client-server architecture for an all-inclusive database management system, wireless sensors, Internet of Things (IoT) and communication technologies for linked healthcare. Wireless Sensor Networks (WSNs) and the IoT include small devices that combine sensing, computation, and communication. In recent years, cloud computing has emerged as a popular new standard of HER administration, serving as a centralized internet backbone for data storage and computation [18].

The latest version of HIS, V.4.0, uses cloud computing to store massive volumes of healthcare data and analyze and make real-time decisions with little involvement from healthcare practitioners. Utility computing in the cloud allows HIS to use more processing power, a massive storage capacity, and a variety of networking capabilities. The healthcare industry increasingly turns to cloud computing to maximize productivity, optimize workload, decrease healthcare delivery costs, and provide patients with more individualized treatment [19]. Lower operating costs, telemedicine, patient data ownership, powerful medical analytics, ease of interoperability, and cloud computing are some benefits of cloud computing in an HIS setting [20].

Eliminating security threats and privacy issues is crucial, as cloud computing is quickly becoming the norm for patient EHR data storage and computation as a centralized online system. Another major concern in HIS is patient privacy, which encompasses the confidentiality of a patient's identification, data, use, and whereabouts. Since the patient's data is gathered, stored, and transported across the network, it is an exciting problem in cloud computing. To protect patients' identities (e.g., phone number, address, UID, etc.), data must be kept private to prevent unlawful or unauthorized use, use must be kept private to maintain patients' regular patterns, and location must be kept private to prevent patients' whereabouts from being tracked [21].

Ciphertext Policy Attribute Based Encryption (CP-ABE) was implemented to safeguard against smart health risks. CP-ABE use in smart healthcare has its own distinct set of difficulties [22]. Encrypted smart health records only reveal the name attribute in PASH; the value of the access policy attribute remains concealed. Attribute values also tend to include more sensitive information than other kinds. Here, PASH decrypts SHR relatively easily (using just a small number of bilinear pairings) [23].

Many people are worried about their privacy on Mobile Healthcare Social Networks (MHSN). Plans call for cloud-based MHSN profile matching and information exchange. Data encryption may be outsourced to the cloud using Identity Based Broadcast Encryption (IBBE). On top of that, the data is sent securely and quickly to the medical group. When medical records are made public, there is a risk of data breaches and assaults on the cloud distributor. To solve this problem, the authors of the AFBS WOA algorithm combined AFBSO and WOA, an optimization technique for fractional brains [24].

Developing nations like India are still attempting to pass legislation along these lines. There is an information technology statute, and some suggested rules from the Medical Council of India (MCI) concerning the use, storage, and sharing of EHRs. A security concern is ensuring patients' electronic health records' confidentiality, integrity, and availability. When unauthorized parties access EHRs, concerns about confidentiality arise; when unauthorized parties alter EHRs while in transit, concerns about integrity arise; and when unauthorized parties block HIS services, concerns about availability arise.

Several studies have suggested a security framework regarding patient data integrity, the certifying authority's function, protecting the network from distributed denial of service attacks, controlling access to electronic health records, and other related topics [25].

2.1. Research Gap

Identifying research gaps in the security framework for e-health systems data in cloud systems involves recognizing areas where existing literature or practical implementations fall short or lack sufficient attention. Here are some potential research gaps in this domain:

2.1.1. Integration Challenges

While there is significant research on security frameworks for e-health systems and cloud computing individually, there is a gap in understanding the specific challenges and requirements for integrating these two domains seamlessly.

Research could focus on identifying integration challenges, such as interoperability issues and data migration complexities, and ensuring continuity of care.

2.1.2. Adaptation to Emerging Technologies

Research in this area could explore novel approaches to enhance security using these technologies while considering their implications for data privacy and confidentiality.

2.1.3. Dynamic Threat Landscape

Cybersecurity threats evolve constantly, with attackers developing new tactics and techniques.

2.1.4. User-Centric Security

While existing research often emphasizes technical aspects of security, there is a gap in understanding the human factors that influence the effectiveness of security frameworks in e-health systems. Research could explore user perceptions, behaviors, and preferences related to security measures and strategies for improving user awareness and adherence to security protocols.

2.1.5. Regulatory Compliance Challenges

Compliance with HIPAA, GDPR, and other regulations is critical for e-health systems handling sensitive patient data. However, there may be gaps in understanding the specific requirements of these regulations concerning security frameworks in cloud environments.

Research could focus on clarifying regulatory requirements and developing practical guidelines for ensuring compliance while maintaining security and usability.

2.1.6. Evaluation Metrics and Benchmarks

Research could focus on developing comprehensive evaluation frameworks that consider factors such as security efficacy, performance impact, scalability, and usability.

2.1.7. Cost-Effective Security Solutions

Security measures can impose significant costs on e-health systems, particularly in resource-constrained environments. Research could explore cost-effective approaches to security, such as optimizing resource allocation, leveraging open-source solutions, or adopting innovative business models for security-as-a-service in cloud environments.

Addressing these research gaps can contribute to developing more robust, adaptable, and user-centric security frameworks for e-health systems data in cloud environments, ultimately enhancing the confidentiality, integrity, and availability of healthcare information while ensuring compliance with regulatory requirements.

2.2. Security Requirements

An improvement over the traditional healthcare system, the electronic health system is a network of interconnected computers allowing real-time data transfer over the cloud. The electronic health record system's many forms of sensitive information directly or indirectly impact the patient's life.

Ensuring the data is securely transferred to the owner within a given timeframe via completely trusted media is crucial for providing good service. Managing the security of the data storage place and the network that transfers massive amounts of data from origin to destination are the real problems here.

Considerations include ensuring the e-health system can adapt to new needs, has an intuitive interface, and is scalable. Another crucial feature that could be included is the ability for the system to be accessible at all times and in any location to handle and control patient data. It should also be reliable so that users do not make mistakes when using it, and it should be able to communicate with other systems using established protocols.

Data transfers to many locations, including patients, health centers, insurance companies, and cloud service providers, make network and data security management challenging. The e-health system lets certain people see and access certain parts of the E-HR. One difference is that a doctor can access a patient's medical record, whereas an insurance company only has access to a subset of that record. Handling the validation and verification of varied users with varying access entitlements becomes tough in this way.

3. Proposed System

Designing a comprehensive security framework for e-Health systems data enhanced by AECC, integrating both Weierstrass and Montgomery forms, represents a significant step towards fortifying the confidentiality, integrity, and accessibility of sensitive healthcare information within cloud environments.

This innovative approach capitalizes on the strengths of both ECC forms to ensure robust cryptographic operations while optimizing efficiency and resource utilization. By leveraging the unique properties of Weierstrass and Montgomery curves, the security framework aims to address the evolving security challenges e-Health systems face in cloud deployments.

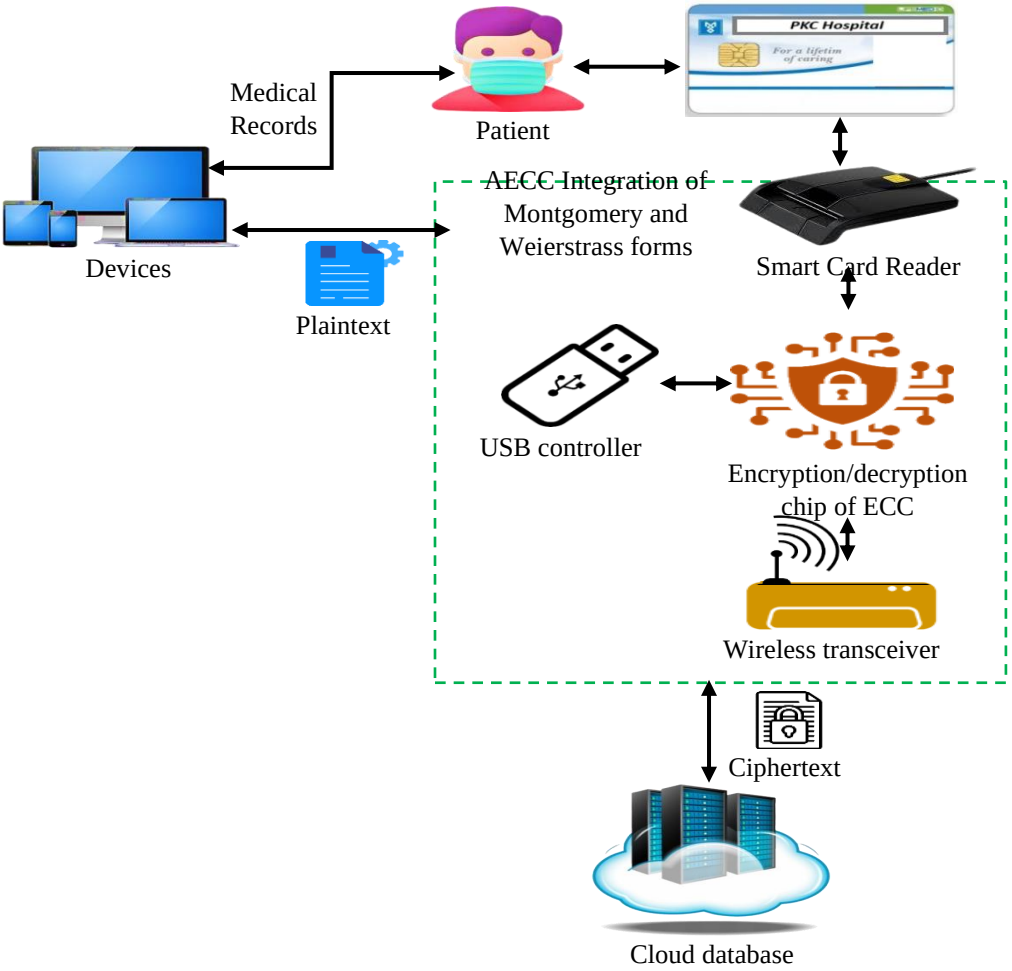

Fig. 2 Proposed architecture

At its foundation, the security framework prioritizes data confidentiality by applying AECC encryption techniques. Utilizing Weierstrass and Montgomery forms for encryption operations, the framework enhances the security of e-Health data stored and transmitted within the cloud system. This involves leveraging the computational efficiency of Montgomery curves and the flexibility of Weierstrass curves to encrypt patient health records, diagnostic images, and other sensitive information, thereby safeguarding it from unauthorized access or disclosure.

Moreover, the security framework emphasizes data integrity by implementing AECC-based digital signatures and authentication mechanisms. By incorporating Weierstrass and Montgomery forms for digital signature generation and verification, the framework enables healthcare providers to verify the authenticity and integrity of e-Health data exchanged within the cloud environment. This ensures that data remains unaltered during transmission and storage, enhancing trust in the reliability and accuracy of patient information within e-health systems.

In addition to data confidentiality and integrity, the security framework focuses on access control mechanisms to regulate user access to e-health systems data based on predefined policies. Integrating AECC-based authentication mechanisms, such as digital certificates and key-based authentication, ensures that only authorized users with valid credentials can access sensitive healthcare information stored in the cloud. This enhances patient privacy and confidentiality while mitigating the risk of unauthorized access or data breaches within e-Health systems deployed in cloud environments.

Furthermore, the security framework emphasizes scalability and adaptability to accommodate the dynamic nature of e-Health systems and evolving cloud infrastructures. The framework offers a scalable solution that seamlessly integrates with existing e-health systems and cloud environments by leveraging the computational efficiency and flexibility of both Weierstrass and Montgomery forms. This enables healthcare providers to effectively manage and protect sensitive patient data while ensuring compliance with regulatory standards and industry best practices.

3.1. Datasets

Create or compile datasets by combining publicly available healthcare datasets, including text and image data, to address specific research questions or tasks in e-health.

Here are some publicly available datasets that researchers commonly use for e-health research, though they may not contain both textual and image data in a unified dataset:

- Medical Information Mart for Intensive Care III (MIMIC-III): A freely accessible critical care database containing de-identified health data associated with over 60,000 ICU admissions. While primarily focused on structured data like clinical notes, laboratory measurements, and diagnostic codes, it also contains some medical imaging data.
- ChestX-ray14: A dataset containing over 100,000 chest X-ray images and associated radiology reports designed for automated chest X-ray interpretation.
- PubMed/MEDLINE: A vast collection of biomedical literature comprising millions of abstracts and articles from various medical journals. While primarily textual, researchers have developed methods to extract and analyze medical concepts, relationships, and entities from this dataset.
- MIMIC-CXR: A dataset of chest X-ray images associated with radiology reports from the MIMIC-III database provides a large-scale resource for training and evaluating automated chest X-ray interpretation algorithms.
- NIH Chest X-ray Dataset: Over 100,000 chest X-ray images labeled with various thoracic pathology annotations, including common and rare thoracic pathologies.
- Kaggle Datasets: Platforms like Kaggle host various healthcare-related datasets, including textual and image data. While not specifically tailored for e-health, these datasets can be repurposed for research in the field.

Researchers often pre-process and integrate data from multiple sources to create benchmark datasets tailored to specific research tasks or objectives in e-health. However, there remains a need for more comprehensive and unified datasets that encompass both textual and image data to facilitate research across various domains within e-health.

3.2. Proposed Architecture

By AECC's overarching design, the following components constitute an effective healthcare system (Figure 3):

HC: The HC's cloud services allow users to save, edit, and restore healthcare data. The server at the HC stores all of the medical records and is the backbone of all cloud services. Numerous threats necessitated the need to safeguard the health cloud's data. The security of patient information is guaranteed by encrypting data in the health cloud.

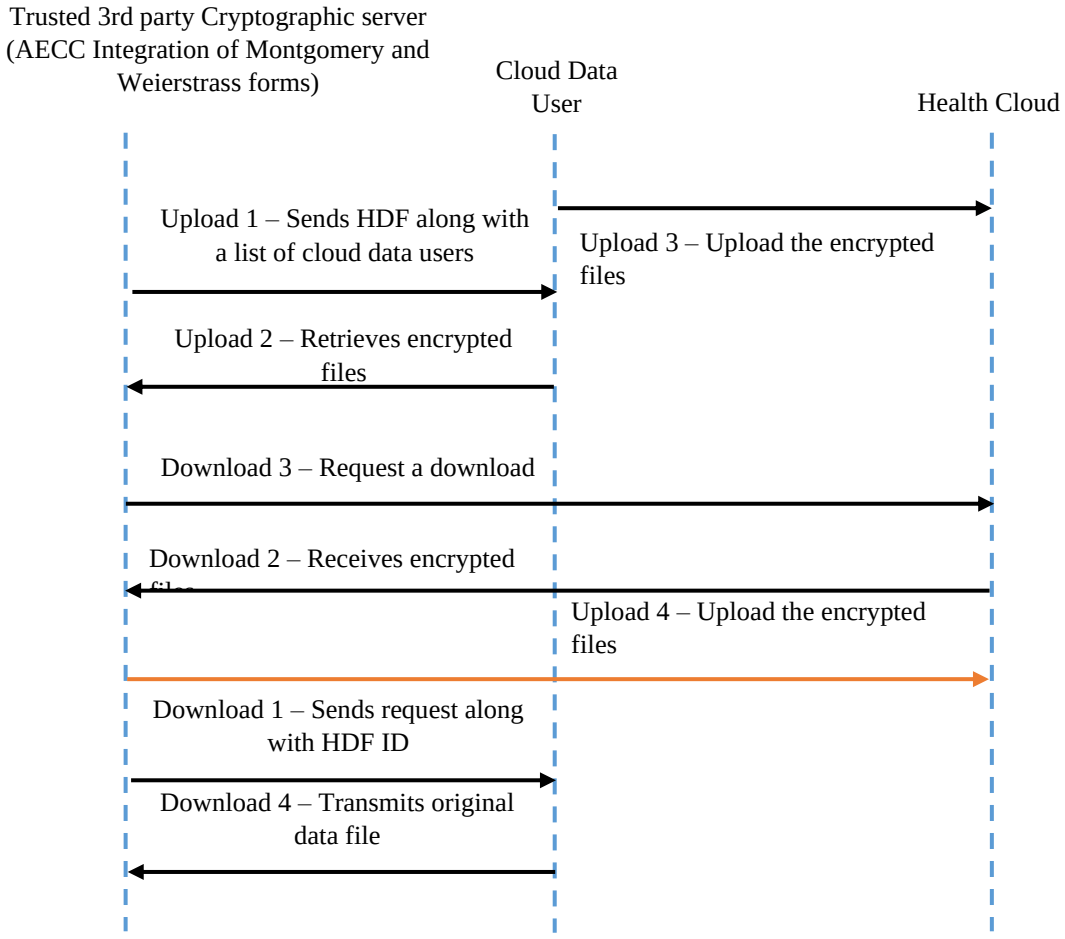

Fig. 3 Optimized AECC based secure health record in the cloud

TTP-CS: Relying on a trusted third party outside the cloud to carry out the cryptographic procedure is known as TTP-CS. To make sure that private medical information is safe, this system has tweaked the AECC algorithm. It is responsible for data secrecy, integrity, and key management to ensure that healthcare data may be shared safely.

CUs: Researchers, analysts, doctors, and everyone else who uses the cloud are considered clients of the health cloud. To provide security services, CUs must be registered with the TTP-CS. All other CUs will only be able to access the data that one CU owns.

3.3. System Design: Advanced Elliptic Curve Cryptography

Integrating Weierstrass and Montgomery forms in AECC represents a sophisticated approach to enhancing the security and efficiency of cryptographic operations. Weierstrass and Montgomery curves are two common representations of elliptic curves, each with advantages and computational characteristics. By combining these forms, researchers aim to leverage the strengths of both approaches to optimize cryptographic performance while maintaining strong security guarantees.

Weierstrass curves, characterized by their cubic equations, offer flexibility and compatibility with various cryptographic protocols. They allow efficient point addition and doubling operations, making them well-suited for many ECC applications. However, Weierstrass curves may suffer from increased computational complexity, particularly in resource-constrained environments.

On the other hand, Montgomery curves, represented by quadratic equations, offer advantages in terms of computational efficiency and resistance to certain side-channel attacks. They feature faster scalar multiplication operations, which can lead to improved performance, especially in hardware implementations or environments with limited computational resources.

By integrating Weierstrass and Montgomery forms in advanced ECC, researchers aim to balance efficiency and security. This integration involves developing algorithms and protocols that leverage each curve form's computational strengths while addressing potential vulnerabilities or limitations. For example, techniques such as curve isogenies or efficient point conversion methods may be employed to facilitate interoperability between Weierstrass and Montgomery curves.

Integrating Weierstrass and Montgomery forms in advanced ECC represents a promising avenue for enhancing cryptographic security and performance in various applications, including e-health systems. However, further research is needed to explore this approach's practical implications, implementation challenges, and potential benefits in real-world settings.

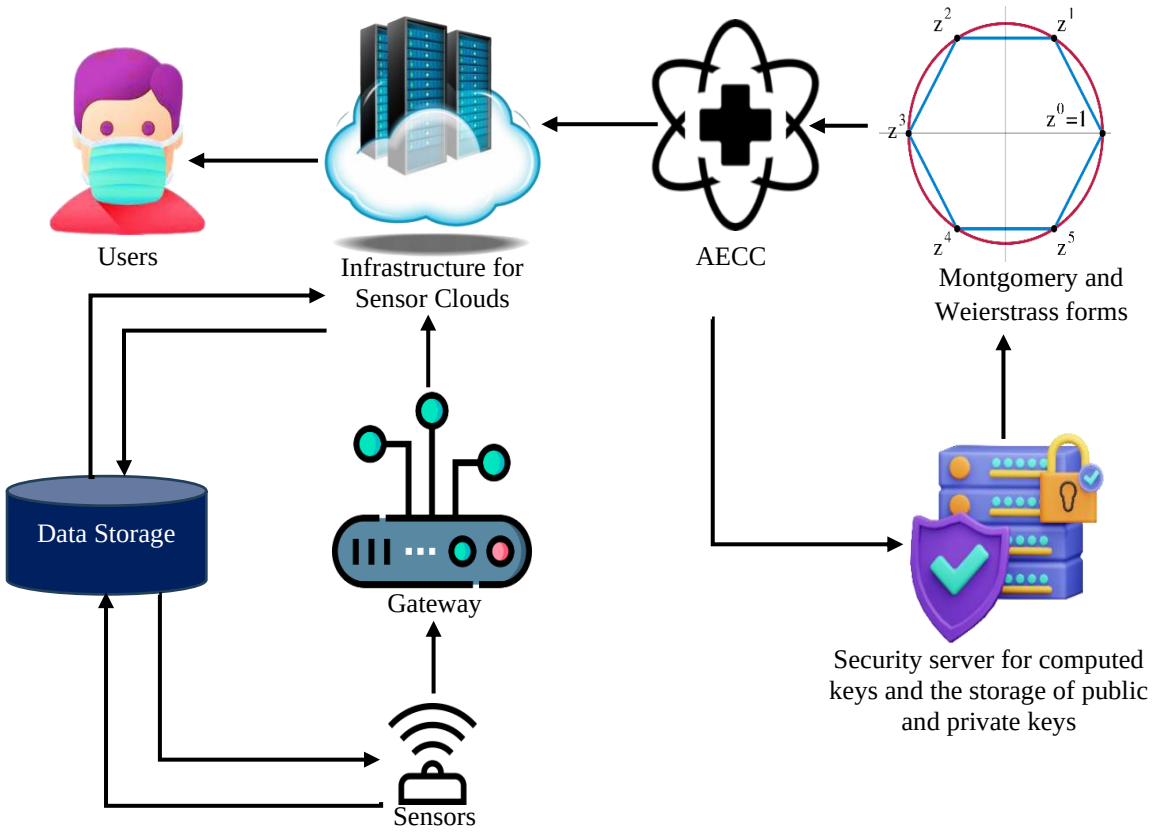

Fig. 4 Sensor cloud architecture using the proposed system

The proposed ECC model with Abelian group theory is applied to sensor cloud infrastructure, as seen in Figure 4. The architecture flow of embedding the proposed model in sensor cloud infrastructure. The proposed AECC security protocol operates using algebraic operations for all computations using its operators.

The complexity of computation increases as intrusion detection problems are difficult to find using algebraic operations in AECC. Hence, handling the algebraic properties makes it difficult to analyze the protocol.

3.3.1. Weierstrass to Montgomery

- Given a Weierstrass curve equation:
  $j^2 = i^3 + ai + b$ (1)
- The transformation to Montgomery involves expressing the curve in terms of a new variable u:
  $u = \frac{3i^2+2ai+1}{2j}$ (2)
- Substituting this expression into the Weierstrass equation yields the curve in Montgomery form:
  $Bj^2 = i^3 + Ai^2 + i$ (3)
  Where A & B are derived from the parameters a & b

3.3.2. Montgomery to Weierstrass

- Given a Montgomery curve equation:
  $Bj^2 = i^3 + Ai^2 + i$ (4)
- The transformation to Weierstrass involves expressing the curve in terms of a new variable i':
  $i = \frac{i'-A}{B}$ (5)
- Substituting this expression into the Montgomery equation yields the curve in Weierstrass form:
  $j^2 = 3i'^3 + ax' + b$ (6)
  Where a & b are derived from the parameters A & B

Use the Weierstrass form for some operations and the Montgomery form for others within the same ECC system. For example, Montgomery curves are more efficient for point multiplication operations, while Weierstrass curves might be more suitable for other operations. Some ECC libraries and protocols might support multiple curve forms for flexibility and optimization.

3.4. Generating Keys

Generating cryptographic keys using user input is not typical in cryptographic protocols, as it introduces potential security risks. However, if considering a scenario where user input is used as part of a key generation process, it is essential to ensure that the resulting keys remain secure and unpredictable.

Here is a conceptual outline of how user input could potentially be incorporated into the key generation process within the context of AECC integrating Weierstrass and Montgomery forms:

3.4.1. User Input

The user provides input data, such as a passphrase, biometric data, or other unique identifiers. This input serves as additional entropy or randomness for the key generation process.

3.4.2. Entropy Generation

The user input is combined with other sources of entropy, such as system-generated randomness or cryptographic PRNGs, to increase the unpredictability of the resulting keys. This helps prevent attackers from guessing or predicting the keys.

3.4.3. Key Derivation

The combined entropy is fed into a key derivation function (KDF), which processes the input data to generate cryptographic keys. The KDF may utilize techniques from Weierstrass and Montgomery forms to derive keys optimized for ECC operations.

3.4.4. Key Validation

The generated keys undergo validation to ensure they meet security requirements, such as length, randomness, and adherence to ECC standards. Invalid keys are discarded, and the key generation process may be repeated.

3.4.5. Key Management

The generated keys are securely stored and managed according to established key management practices. This includes protecting keys from unauthorized access, securely distributing them to authorized parties, and regularly updating or rotating keys as needed.

It is important to note that while incorporating user input into the key generation process may provide additional entropy, it also introduces potential security risks, such as the possibility of weak or predictable keys if the user input is insufficiently random or the key generation process is not implemented correctly. Therefore, careful consideration and thorough testing are essential when integrating user input into cryptographic key generation processes. Additionally, cryptographic protocols typically rely on well-established key generation algorithms and practices to ensure the security and reliability of generated keys.

Generating cryptographic keys using user input involves integrating additional entropy the user provides into the key-generation process. While this approach may not involve complex equations, it can be conceptualized within the context of Key Derivation Functions (KDFs) used in cryptographic protocols.

Let us consider a simplified scenario where User Input (UI) is combined with system-generated randomness (R) using a cryptographic hash function to derive a cryptographic key (K). The key derivation process can be represented as follows:

$$K = \mathrm{KDF}(UI||R) \quad (7)$$

Where:

- K represents the resulting cryptographic key.
- KDF denotes the key derivation function.
- UI denotes the user input.
- R denotes the system-generated randomness.

The concatenation of user input and system-generated randomness ($UI||R$) ensures that both sources of entropy contribute to the key derivation process, increasing the unpredictability of the resulting key.

The key derivation function may involve applying a cryptographic hash function, such as SHA-256, to the concatenated input data to produce the final key. Mathematically, this can be expressed as:

$$K=\text{SHA-256}(UI||R) \quad (8)$$

Where:

- SHA-256SHA-256 represents the SHA-256 hash function.

In this simplified example, the resulting key K is derived from the combined entropy of user input and system-generated randomness, ensuring that the key generation process benefits from both sources of entropy.

However, it is essential to note that the actual key generation process may involve additional steps, such as salting, iteration, or other cryptographic operations, to enhance security and randomness. Additionally, the key management practices described earlier remain critical to ensure the security and integrity of generated keys.

3.5. Encryption

3.5.1. Key Generation

- Generate a private key k_w and a corresponding public key K_w using the Weierstrass form.
- Choose a random integer k_w as the private key.
- Compute the public key $K_w = k_w \times G_w$, where G_w is a generator point on the Weierstrass curve.

3.5.2. Message Encoding

- Convert the plaintext message M into a point on the Weierstrass curve.
- This step may involve techniques such as point compression or encoding schemes like the Elliptic Curve Integrated Encryption Scheme (ECIES)

3.5.3. Encryption

- Choose a random integer r as the ephemeral private key for the Montgomery form.
- Compute the ephemeral public key R_m using the Montgomery form: $R_m = r \times G_m$, where
- G_m is a generator point on the Montgomery curve.
- Compute the shared secret point S_w using the Weierstrass form: $S_w = k_w \times R_m$.
- Compute the ciphertext point C_w as the sum of the plaintext point and the shared secret point: $C_w = M + S_w$

Note:

- This algorithm combines the computational advantages of Montgomery curves for ephemeral key generation with the flexibility of Weierstrass curves for computing the shared secret.
- Generator points Gw and Gm should be chosen carefully to ensure security and efficiency.
- Actual implementations may involve additional steps to ensure cryptographic security and compatibility, such as point conversions and error handling.
- Careful consideration should be given to parameter selection, curve choice, and cryptographic standards adherence for real-world applications.

3.6. Decryption

3.6.1. Key Generation

- Derive the Montgomery private key k_m from the Weierstrass private key K_w.
- This step involves transforming the Weierstrass private key into the Montgomery form.

3.6.2. Decryption

- Compute the shared secret point S_m using the Montgomery private key k_m and the ephemeral public key R_m: $S_m = k_m \times R_m$.
- Compute the plaintext message M as the difference between the ciphertext point C_w and the shared secret point S_m: $M = C_w - S_m$

Note

- The key derivation step ensures compatibility between the private keys used in the encryption and decryption processes.
- The transformation function f converts the Weierstrass private key k_w to the Montgomery private key k_m.
- Actual implementations may involve additional steps, such as point conversions and error handling, to ensure cryptographic security and compatibility.
- Careful consideration should be given to parameter selection, curve choice, and cryptographic standards adherence for real-world applications.

3.7. Security Analysis

1. Listening in on conversations with someone: The certificate authority sends the patient the private key over an encrypted link. Consequently, the encrypted data will remain inaccessible to hackers.
2. The replay assault: The physicians have extensively used the EGC cryptography techniques. The optimal solutions are found by determining the EGC values via the optimization mechanism. Therefore, launching a replay attack using the patient-provided keyword is impossible.
3. The man-in-the-middle (MIM) assault and masquerade: Masquerade attacks are rendered useless due to the characteristics' usage in file encryption. To hack a file, the hacker has to know its characteristics.

Algorithm

To ensure secure storage, access, and transmission of e-healthcare data in a cloud environment by combining Elliptic Curve Cryptography (ECC) with hybrid techniques for enhanced performance and security.

Steps of the Algorithm

Step 1: System Initialization: Define the elliptic curve parameters:
Prime modulus p, base point G, order n, and curve equation $y^2=x^3+ax+b \bmod p$
Distribute public parameters to all stakeholders in the e-healthcare system.

Step 2: Key Generation
Private Key: Each user generates a private key d, where $d \in [1,n-1]$.

Public Key: Compute the public key $Q=d \cdot G$, where G is the base point on the elliptic curve.

Step 3: Data Encryption
Convert the e-healthcare data into a binary string and partition it into blocks for efficient processing.
Select a random ephemeral key k, where $k \in [1,n-1]$.
Compute the shared key using the recipient's public key Q_r: $S= k \cdot Q_r$.
Encrypt each data block M using the shared key S:
$C=E_k(M)$
E_k is a symmetric encryption algorithm (e.g., AES).

Step 4: Hybrid Approach for Encryption
Use ECC to exchange and generate the shared key.
Apply a symmetric encryption algorithm (like AES or ChaCha20) to encrypt large e-healthcare data efficiently.
Concatenate the ECC-encrypted key and the symmetric ciphertext for secure transmission.

Step 5: Data Upload to Cloud
Securely transmit the encrypted data C and the ECC-encrypted symmetric key kG to the cloud server.
Add metadata (e.g., timestamp, user ID) for tracking and access management.

Step 6: Access Control in the Cloud
Implement role-based or attribute-based access control (RBAC/ABAC) mechanisms to regulate user permissions.
Use ECC-based digital signatures to authenticate and verify user identities.

Step 7: Data Decryption
Retrieve the encrypted symmetric key kG and the ciphertext C from the cloud.
Compute the shared key using the recipient's private key d_r
$S= d_r \cdot kG$.
Decrypt the symmetric key using SSS and then decrypt the data:
$M=D_k(C)$, where D_k is the decryption algorithm corresponding to E_k.

Step 8: Data Integrity Verification
Generate a hash value of the decrypted data using a secure hash algorithm (e.g., SHA-256).
Compare the hash with the stored hash to ensure data integrity.

Step 9: Audit and Monitoring
Maintain logs for all data transactions and access activities.
Use anomaly detection techniques to monitor unauthorized access attempts in real-time.

4. Results and Discussions

The proposed protocol is simulated in NS-2 Version 2.31 by implementing a security algorithm to guarantee the confidentiality and integrity of patient data.

Here, two scenarios, namely ECC and cloud with security (Sec-cloud), have been simulated to check the efficiency of the proposed work. The simulated input parameter used is indicated in following Table 1.

The computation time of proposed and existing systems is shown in Table 2, and the Key generation time is shown in Table 3. Tables 4 and 5 show the encryption, decryption and uploading time of files.

The recommended method is implemented on a Windows 10 64-bit OS system with an Intel Core i5-6200U CPU running at 2.40 GHz and 8.00 GB of RAM. Three primary parts are detailed in the system model: the HC, the TTP-CS, and the CUs. It employs the JPBC v.2.0.0 Java Pairing-Based Cryptography library for inter-entity communication. Its features make it easy to use elliptic curves and pairing techniques.

The Java libraries allow the entities to communicate with each other. Data sent and received is encrypted using SSL. Key generation time, file upload and download timings, and time to find EGC's value were the metrics used to assess it in the Cloudsim toolkit test.

Tables 1, 2, 3, and 4 display the results of the performance analyses conducted on the suggested mayfly algorithm.

Table 1. Parameter of simulation

Cloud server	1
Doctor PDA	1
Client PDA	2
Sensor Type (per user) ● BP sensor ● HR sensor ● BO sensor ● Temperature sensor	 1 1 1 1
Simulation time (sec)	100
Security method	SHA
Speed (m/s)	Random
Packet size (bytes)	1000
Traffic type	FTP, CBR
Transport layer	UDP, TCP

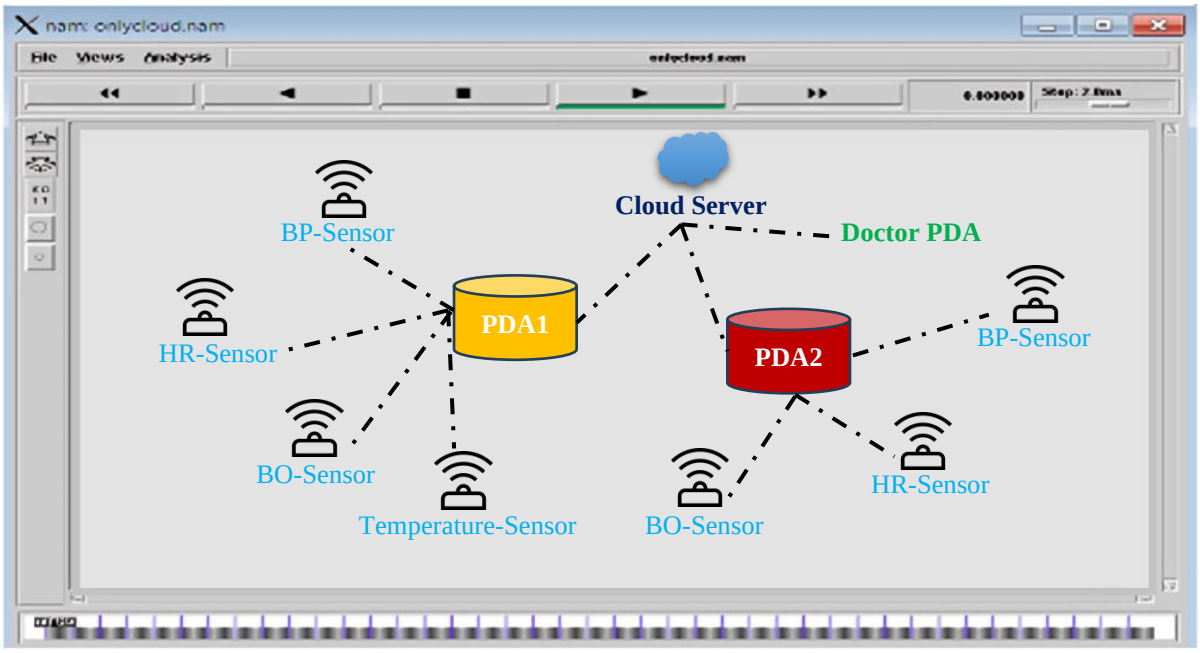

Fig. 5 Simulated environment for proposed work

Table 2. Comparison of the proposed and existing system's computation time

Iterations count	AES	ECC	Proposed
10	1.623	1.635	0.549
20	1.825	1.707	0.689
30	1.898	1.889	0.754
40	2.294	2.202	1.110
50	2.465	2.209	1.292

Table 3. Comparison of proposed and existing systems based on Key Generation time

File size in MB	Methods (sec)			
	EGC	AES	ECC	Proposed
100	2.649	2.643	0.005	0.00213
200	2.814	2.760	0.00430	0.00236
300	2.412	2.748	0.00477	0.00287
400	2.988	2.899	0.006	0.00303
500	2.925	2.966	0.00536	0.00329
600	3.239	2.832	0.0056	0.0036
700	3.368	3.143	0.00599	0.00399
800	3.749	3.292	0.00633	0.00428
900	3.972	3.488	0.00665	0.00464
1000	3.978	3.654	0.00698	0.00501

Table 4. Comparison of proposed and existing systems based on encryption and decryption time

File size in MB	Methods (sec)							
	EGC		AES		ECC		Proposed	
	Encryp	Decryp	Encryp	Decryp	Encryp	Decryp	Encryp	Decryp
100	1.5	0.98	1.5	1.16	0.82	0.82	0.72	0.72
200	1.52	1.04	1.9	1.32	0.96	0.98	0.82	0.84
300	2.07	1.5	2.92	1.86	1.26	1.2	1.22	1.26
400	15.96	9.91	15.60	10.48	6.45	6.5	5.62	5.70
500	59.57	36.58	61.38	35.92	9.02	10.26	8.27	8.80
600	113.42	60.15	116.14	61.62	17.40	20.69	16.36	18.99
700	493.04	230.82	873.08	400.22	33.25	39.26	31.12	38.23

Table 5. Time of uploading files

File size in MB	Uploading speed (mb/s)
100	12.5
200	13
300	12.9
400	13.93
500	13.5
600	14
700	14
800	14

4.1. Network Throughput Analysis

Throughput is calculated by accessing data and measured per unit of time (Kilobyte/second). For analysis, I have taken simulation results of both scenarios (ECC and Proposed system).

The comparison graph concludes that the proposed algorithm achieves 738 kilobytes per second throughput compared to the ECC scenario, where 433.06 KB throughput has been achieved. This data reduction is the result of various attacks shown in Figure 6.

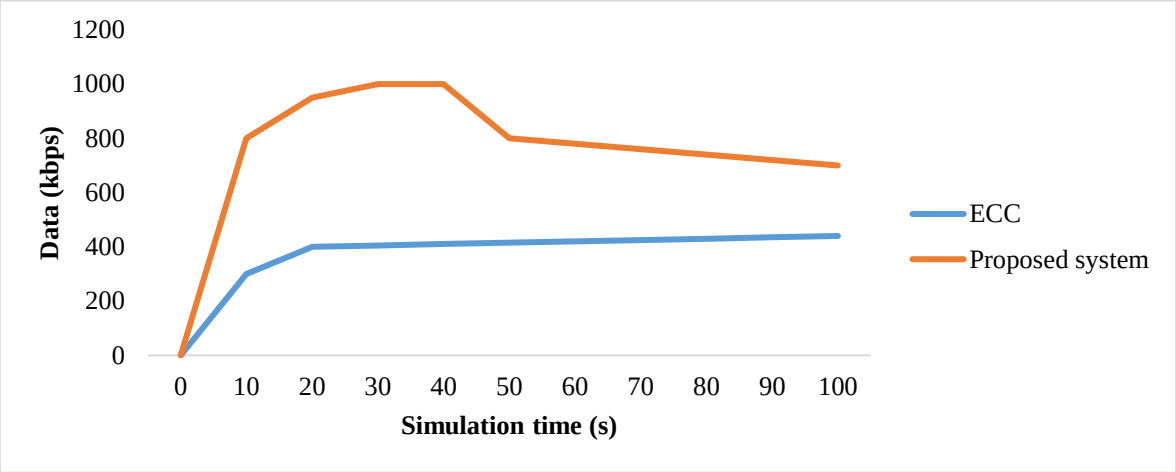

Fig. 6 Throughput analysis

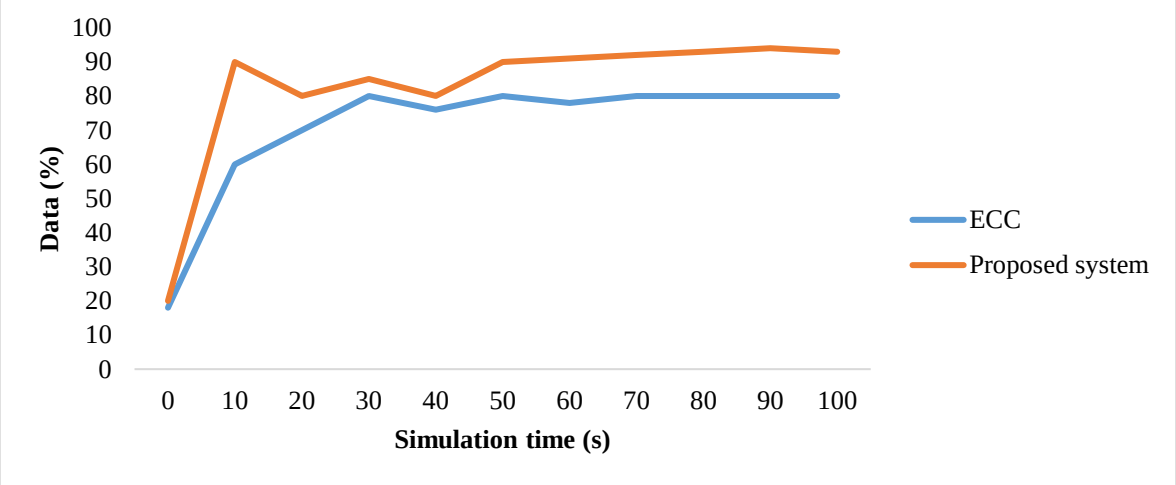

Fig. 7 Packet delivery ratio analysis

4.2. PDR Analysis

Packet Delivery Ratio PDR is a percentage ratio of data received out of the total data sent, where a higher PDR represents lower data loss at the receiving end. Figure 7 shows the PDR analysis and comparison. The comparison shows that the proposed performs well compared to the ECC scenario's packet delivery ratio.

4.3. Normal Routing Load (NRL)

During data transmission in the network, routing overhead is calculated to manage data transfer. For example, during data transmission, some control packets, like ICMP, routing packets, network error control packets, etc., are also transferred to manage the network and facilitate data communication. However, simultaneously, it increases the routing load and overheads of the network. This affects the data transmission capability. So, routing load (Routing overhead) is calculated as the ratio of the total control packet to the actual data packet received by the receiver. Routing load is always lower when network bandwidth is maximally utilized. The resulting graph shown in Figure 8 depicted that the proposed system recorded lower overhead than the only-cloud scenario. This Figure shows that during 100 sec of simulation time, routing overhead is recorded as 18 in the proposed scenario compared to the ECC, where routing overhead is achieved at 37.

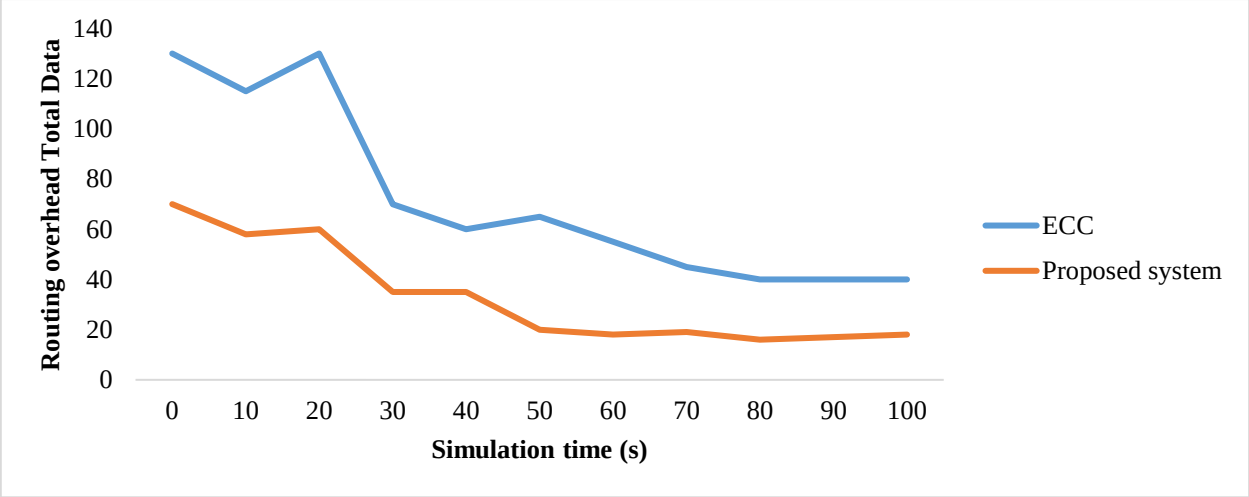

Fig. 8 Routing overhead analysis

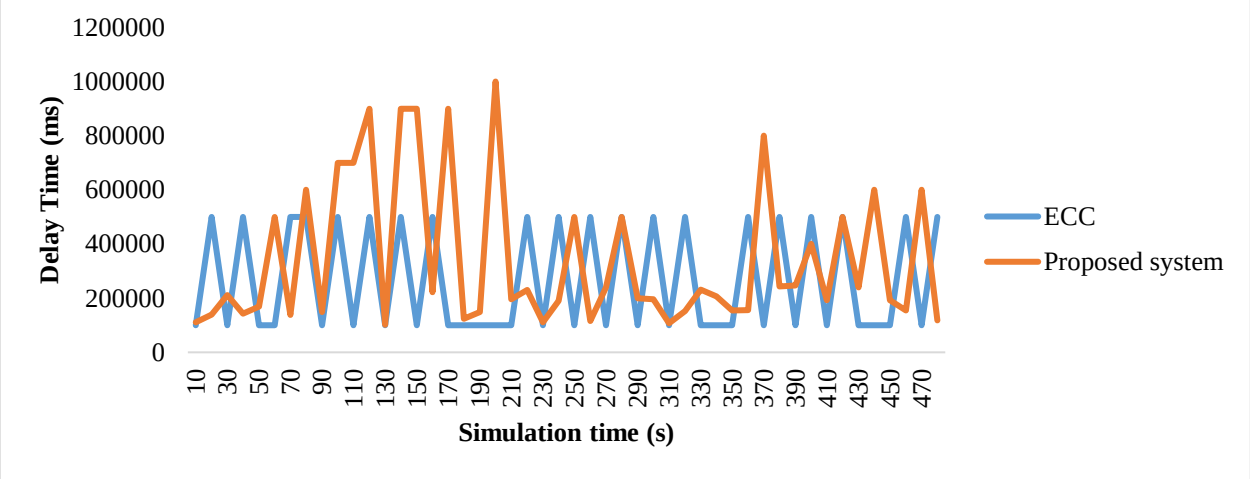

Fig. 9 Delay analysis of end-to-end network

4.4. Per Packet Delay or End-to-End Delay in [ms]

When the delay is higher, the network's performance is lower. The resulting graph in Figure 9 shows that the proposed system scenario records less end-to-end delay than the ECC scenario. The figure shows an 184.62 ms per packet delay in the proposed scenario compared to the ECC scenario, where a delay is recorded at 198.43 ms. This indicates the effectiveness of the proposed algorithm.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

The proposed model on sensor cloud infrastructure increases the accuracy rate with its lightweight computation compared to other methods, as shown in Table 6 and Figure 10.

Table 6. Accuracy rate over sensor cloud environment with intruder detection system

Intruder ratio (%)	Proposed System	ECC	AES
100	99.99	99.8	99.6
200	99.98	99.7	99.2
300	99.96	99.3	98.9
400	99.95	99.2	98.6
500	99.2	99	98.3
600	99.2	98.8	98
700	99.0	98.6	97.4
800	98.9	98.2	97
900	98.81	98	96.4
1000	98.6	97.6	96

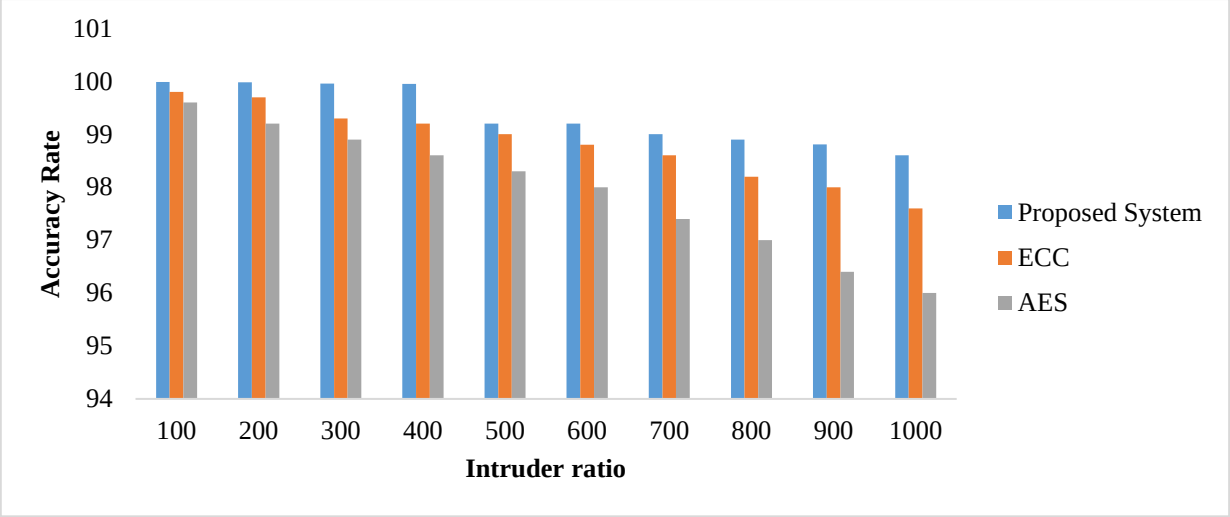

Fig. 10 Accuracy rate over sensor cloud environment with intruder detection system

The detection rate is the ratio of total true positive instances during intrusive sensor behavior to the true and false positive ratio given in Equation (10). DR is shown in Table 7 and Figure 11.

$$Detection\ Rate\ (DR) = \frac{TP}{TP+FP} \quad (10)$$

Table 7. Detection rate over sensor cloud environment with intruder detection system

Intruder ratio (%)	Proposed System	ECC	AES
100	0.99	0.97	0.92
200	0.95	0.92	0.88
300	0.89	0.87	0.81
400	0.84	0.82	0.78
500	0.82	0.79	0.76
600	0.79	0.75	0.69
700	0.76	0.70	0.65
800	0.72	0.66	0.61
900	0.68	0.62	0.59
1000	0.63	0.59	0.56

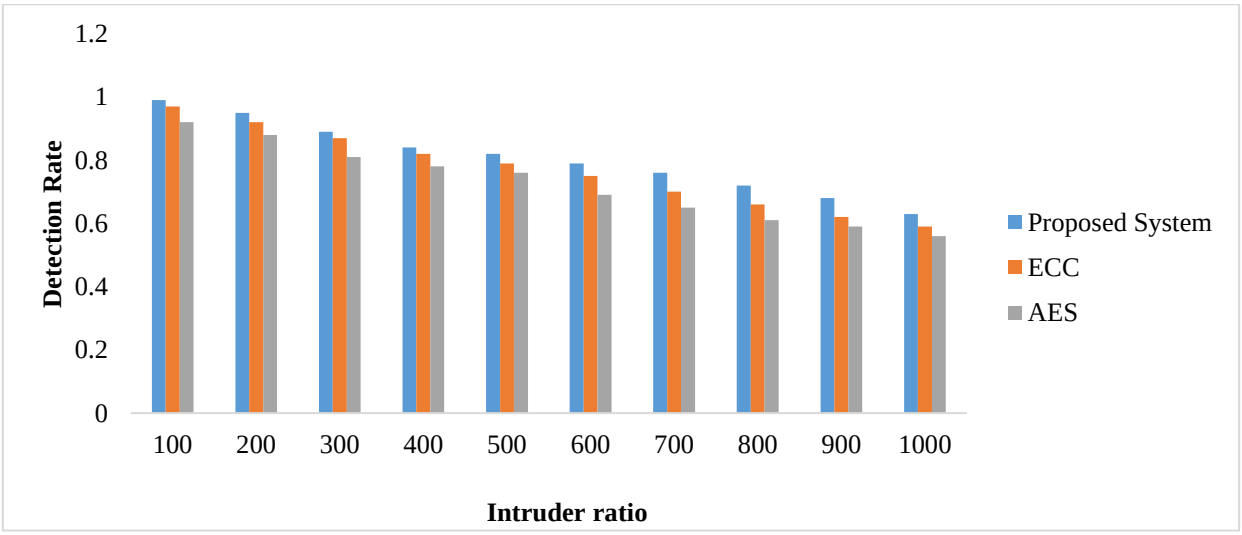

Fig. 11 Detection rate over sensor cloud environment with intruder detection system

5. Conclusion and Future Enhancement

In conclusion, designing a comprehensive security framework for e-Health systems data enhanced by AECC, integrating both Weierstrass and Montgomery forms, presents a significant advancement in ensuring the confidentiality, integrity, and availability of sensitive healthcare information within cloud environments. By harnessing the unique properties of both curve forms, this

framework offers a robust and adaptable solution to address the evolving security challenges faced by e-health systems. By integrating Weierstrass and Montgomery forms, the framework benefits from the computational efficiency of Montgomery curves for certain operations while leveraging the flexibility and compatibility of Weierstrass curves for others. This hybrid approach enables the framework to optimize cryptographic performance while maintaining strong security guarantees that are essential for protecting patient privacy and data integrity. The encryption algorithm outlined in the framework demonstrates how both curve forms can be seamlessly integrated to ensure secure communication and data exchange within e-Health systems deployed in cloud environments. By incorporating key generation, message encoding, encryption, and decryption processes, the framework provides a comprehensive solution for safeguarding e-Health data from unauthorized access and tampering. Moreover, the integration of Weierstrass and Montgomery forms enhances the scalability and adaptability of the security framework, allowing it to accommodate the dynamic nature of e-Health systems and evolving cloud infrastructures. This ensures that the framework can effectively meet the security requirements of diverse healthcare applications while complying with regulatory standards and industry best practices. In conclusion, designing a comprehensive security framework enhanced by AECC, integrating both Weierstrass and Montgomery forms, represents a significant step forward in securing e-Health systems data within cloud environments. Protecting the privacy, authenticity, and accessibility of patients' medical records in the digital era will need ongoing investment in research and development that improves and streamlines existing systems.

References

[1] P. Upender, and P.A. Harsha Vardhini, "Design Analysis of Rectangular and Circular Microstrip Patch Antenna with Coaxial Feed at S-Band for Wireless Applications," *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud (ISMAC)*, Palladam, India, pp. 274-279, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Vansh Arora, "*A Framework for Cloud-Based EHR Security Using Hybrid Cryptographic Methods of AES and ECC*," Master Thesis, Dublin, National College of Ireland, pp. 1-24, 2023. [Google Scholar] [Publisher Link]

[3] Jaganathan Logeshwaran et al., "Evaluating Key Management Strategies for Applied Cryptography Protocols," *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*, Jaipur India, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Prabhakar Marry et al., "Blockchain Based Smart Healthcare System," *Proceedings of the 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, Coimbatore, India, pp. 1480-1484, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] B. Ravi Krishna et al., "Artificial Intelligence Probabilities Scheme for Disease Prevention Data Set Construction in Intelligent Smart Healthcare Scenario," *SLAS Technology*, vol. 29, no. 4, pp. 1-11, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Prathima Subramanian, and R. Durga, "PDHSMICK: A Partial Key-Based Secure EHRs with Distributed Cloud for Healthcare Systems Applying MI-CRYSTALS-Kyber," *Computer Software and Media Applications*, vol. 6, no. 1, pp. 1-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Amjad Rehman et al., "A Novel Resilient and Intelligent Predictive Model for CPS-Enabled E-Health Applications," *Cognitive Computation*, vol. 16, pp. 1321-1330, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] J. Logeshwaran et al., "Clinical Resource Management with AI/ML-Driven Automated Diagnostics in Smart Healthcare," *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] B. Deena Divya Nayomi et al., "A Cloud-Assisted Framework Utilizing Blockchain, Machine Learning, and Artificial Intelligence to Countermeasure Phishing Attacks in Smart Cities," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1, pp. 313-327, 2023. [Google Scholar] [Publisher Link]

[10] P. Lavanya Kumari et al., "Video Object Forgery Detection Using Image Processing Techniques," *7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Kirtipur, Nepal, pp. 785-788, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] B.V. Chowdary et al., "An Effective and Efficient Heart Disease Prediction Model Using Distributed High Performance Light GBM," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, India, pp. 662-667, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] J. Mahalakshmi et al., "Enhancing Cloud Security with AuthPrivacyChain: A Blockchain-Based Approach for Access Control and Privacy Protection," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 6s, pp. 370-384, 2023. [Google Scholar] [Publisher Link]

[13] Srinu Banothu, A. Govardhan, and Karnam Madhavi, "Performance Evaluation of Cloud Database Security Algorithms," *E3S Web of Conferences*, vol. 309, pp. 1-8, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Harish Reddy Gantla et al., "Machine Learning-Based Trust-Aware Secure Traffic Mechanism to Identify DDOS Attacks over Cloud," *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] R. Charanya, R.A.K. Saravanaguru, and M. Aramudhan, "Information Security Protection for eHealth Records Using Temporal Hash Signature," *International Journal of Intelligent Enterprise*, vol. 10, no. 1, pp. 14-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Srinu. Banothu, A. Govardhan, and Karnam. Madhavi, "A Fully Distributed Secure Approach Using Nondeterministic Encryption for Database Security in Cloud," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 7, pp. 2218-2228, 2022. [Google Scholar] [Publisher Link]

[17] Madhavi Karanam et al., "Performance Evaluation of Cryptographic Security Algorithms on Cloud," *E3S Web of Conferences*, vol. 391, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Kaushik Sekaran et al., "Bio-Inspired Fuzzy Model for Energy Efficient Cloud Computing through Firefly Search Behaviour," *New Trends in Computational Vision and Bio-Inspired Computing*, pp. 1043-1049, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] O. Sri Nagesh et al., "Providing Security Properties of Cloud Service by Using REST APIs," *Springer Proceedings in Mathematics and Statistics*, Vizianagaram, India, vol. 421, pp. 631-639, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Santosh Kumar Srivastava et al., "Cloud-Integrated Big Data Algorithms for Deep Learning in Healthcare Systems," *Advances in Science, Technology and Innovation*, pp. 169-179, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Srinu Banothu et al., "A Secure Data Storage Approach for Online Examination Platform Using Cloud DBAAS Service," *Scalable Computing*, vol. 25, no. 5, pp. 3715-3724, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] T. Bala Murali Krishna et al., "Software-Driven Secure Framework for Mobile Healthcare Applications in IoMT," *Intelligent Decision Technologies*, vol. 17, no. 2, pp. 377-393, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Udit Mamodiya et al., "Enhancing Security in Cloud Registration with Multi-Dimensional Features Fusion," *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*, Jaipur, India 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] G. Janardhan, et al., "Adaptive Network Traffic Reduction for Optimal Performance," *Proceedings of the 2024 International Conference on Expert Clouds and Applications (ICOECA)*, pp. 904-908, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] B.V. Chowdary et al., "An Effective and Efficient Alzheimer Disease Prediction System Using Machine Learning Model," *Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC*, India, pp. 342-347, 2021. [CrossRef] [Google Scholar] [Publisher Link]