International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

CLOUD BASED SECURE AND EFFICIENT FRAMEWORK FOR SMART MEDICAL SYSTEM USING ECC

Sreenikethan S
PG,Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sreenikethanmca2025@gmail.com

Sowmya J
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sowmyaj@theoxford.edu

ABSTRACT

Real-time monitoring, remote diagnosis, and effective data sharing have all been made possible by the quick development of smart healthcare systems, which has greatly enhanced medical services. However, there are serious issues with data security, patient privacy, and system efficiency when cloud computing is included into such systems. This research uses Elliptic Curve Cryptography (ECC) to offer a cloud-based, efficient, and secure framework for a smart medical system. Because of its robust security features and comparatively short key sizes, which guarantee quicker encryption and decryption processes while reducing computational cost, ECC is widely used. The suggested framework ensures confidentiality, integrity, and authenticity while facilitating the safe transfer and storage of private patient data on the cloud. Additionally, it facilitates interoperability and scalability across various medical applications and devices, improving accessible for patients and healthcare providers.

KEYWORDS: Cloud Computing, Smart Medical Systems, Internet of Things (IoT) in Healthcare, Elliptic Curve Cryptography (ECC), Data Security.

INTRODUCTION

The way healthcare services are provided has changed dramatically as a result of the quick development of digital healthcare systems and the extensive use of the Internet of Things (IoT) in the medical field. Remote diagnosis, effective medical record administration, and real-time patient health parameter monitoring are all made possible by smart medical systems. However, there are significant issues with data security, privacy, and system effectiveness when sensitive patient data is integrated with cloud platforms. Building confidence between patients and healthcare professionals requires safe transfer and storage of medical data, which is extremely sensitive.

Cryptographic methods are essential for addressing these issues and protecting private health data. Even if they are secure, traditional cryptographic techniques frequently need a lot of processing power, which makes them less appropriate for medical IoT

devices with limited resources. When compared to more traditional techniques like RSA and AES, Elliptic Curve Cryptography (ECC) proves to be an effective alternative, providing robust security with smaller key sizes and lower computational overhead. Because of this, ECC is especially well-suited for healthcare systems, where strong encryption that is lightweight is crucial.

LITERATURE SURVEY

The expanding integration of cloud computing, improved cryptography, and the Internet of Medical Things (IoMT) to enable safe healthcare data management is highlighted by recent research on cloud-based smart medical systems. Numerous studies stress that although cloud systems offer cost-effectiveness, scalability, and flexibility for processing and storing massive amounts of electronic health records (EHRs), they also raise serious issues with patient privacy, data integrity, and confidentiality. Although traditional cryptographic methods like RSA and DES have been used extensively, their processing complexity renders them inappropriate for real-time applications and medical devices with limited resources. Because of its good security with smaller key sizes, lower computational complexity, and lower energy consumption, Elliptic Curve Cryptography (ECC) has emerged as a preferred choice among the numerous researchers who have investigated lightweight cryptographic systems.

EXISTING WORK

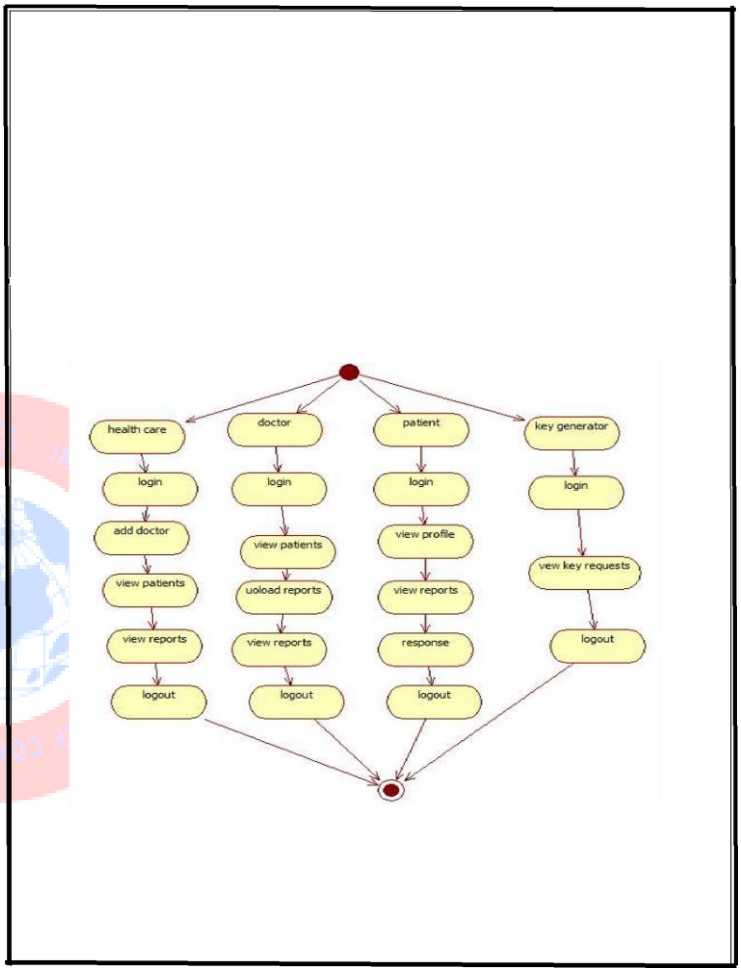
The majority of the work that has been done in the field of cloud-based smart medical systems has concentrated on integrating cloud computing platforms, electronic health records, and Internet of Medical Things (IoMT) devices in order to facilitate remote healthcare services and ongoing patient monitoring. Traditional cryptographic techniques like RSA and AES have been used by a number of researchers to propose secure data transmission models; however, these methods frequently encounter difficulties because of their high computational overhead and energy consumption, which makes them less appropriate for lightweight medical devices. Elliptic curve cryptography (ECC), a more effective substitute that offers comparable security strength with smaller key sizes and reduced resource requirements, has been presented in recent studies as a solution to this problem.

PROPOSED SYSTEM

Using Elliptic Curve Cryptography (ECC), the suggested solution offers a cloud-based, safe, and effective framework for intelligent medical applications that guarantees the confidentiality, integrity, and controlled access of private medical data. In contrast to conventional cryptographic techniques, this system minimizes computational and energy overhead by encrypting patient health data obtained from wearable sensors and IoT-enabled medical equipment using lightweight ECC algorithms before sending it to the cloud. Only approved physicians, caretakers, or institutions may access the data thanks to ECC-based authentication methods, and the cloud platform acts as a central location for the safe processing, storage, and analytics of medical information.

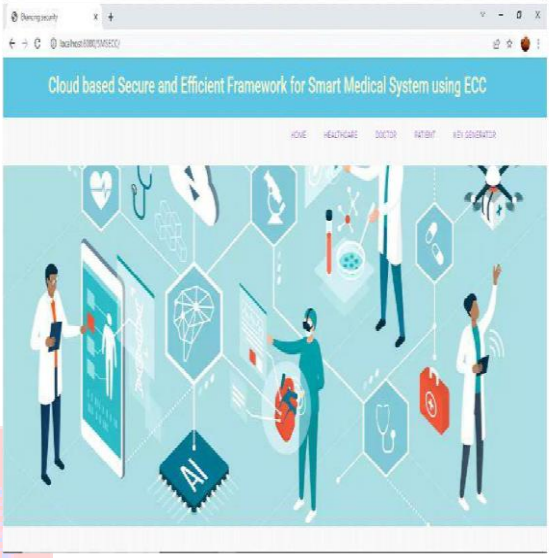
METHODOLOGY

To ensure the secure and efficient processing of sensitive medical data, the proposed architecture integrates cloud computing, elliptic curve cryptography (ECC), and smart medical devices. During the first phase, patient health data is continuously recorded by smart medical sensors and Internet of Things (IoT)-enabled devices that monitor vital indicators like heart rate, blood pressure, glucose level, and oxygen saturation. These data streams are transmitted to the cloud via secure communication channels. ECC is perfect for medical devices with limited resources because it provides similar security to traditional public key cryptosystems with much smaller key sizes. To guarantee data integrity, confidentiality, and authenticity, lightweight encryption is applied at the device layer before transmission.



Role-based access control techniques protect encrypted health data processing and storage at the cloud layer, limiting access to patient data to authorized healthcare personnel. Cloud-based data preparation and analytics modules then process the collected records to generate actionable insights,

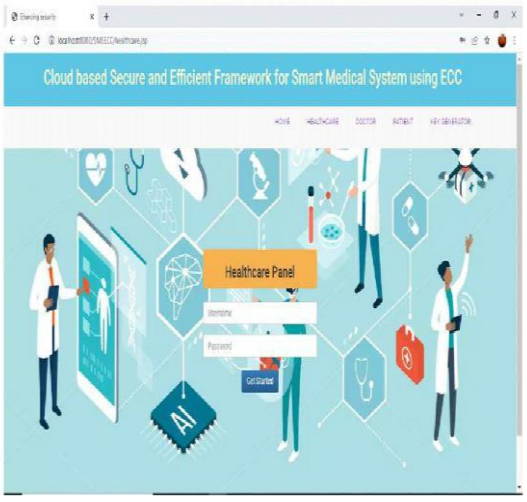
The framework also employs secure key management and digital signatures to prevent tampering and unauthorized access during storage and retrieval. At the edge, encryption offloading techniques and partial processing are used to reduce latency and boost efficiency, ensuring real-time responsiveness for critical medical events. Continuous monitoring modules evaluate system performance in terms of encryption/decryption overhead, communication latency, and security resilience against potential cyberattacks. By combining scalable cloud services with ECC-based lightweight encryption, the framework achieves a balance between high-level security, computational efficiency, and real-time responsiveness. For modern healthcare applications, this enables the development of a trustworthy and secure smart medical system.



EXPERIMENTAL RESULTS

- **Home**: This is the initial page of our project.

In this page we can see our main four modules that is HEALTHCARE, DOCTOR, PATIENT and KEY GENERATOR



- **Schedules :** Patient View Schedules

After booking an appointment with the doctor the schedules will be shown and unless all the previous appointment are complete the patient cannot book new appointment.

CONCLUSION

In conclusion, the crucial need to protect sensitive healthcare data while guaranteeing dependable and scalable medical services is addressed by the suggested cloud-based secure and effective framework for smart medical systems employing Elliptic Curve Cryptography (ECC). The framework is ideal for resource-constrained IoMT devices and real-time patient monitoring because it uses ECC to deliver robust security with low computational and energy overhead. While ECC guarantees confidentiality, integrity, and secure access control, cloud computing integration offers scalable storage, ubiquitous accessibility, and potent analytics to improve clinical decision-making. This double benefit increases efficiency in managing massive amounts of healthcare data while also bolstering confidence in cloud-enabled medical ecosystems.

REFERENCES

1. R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and M. S. Obaidat, ‘‘Design and analys is of an enhanced patient-server mutual authentication protocol for telecare medical information system,’’ J. Med. Syst., vol. 39, no. 11, p. 137, Nov. 2015.
2. C.-M. Chen, C.-T. Li, S. Liu, T.-Y. Wu, and J.-S. Pan, ‘‘A provable secure private data delegation scheme for mountaineering events in emergency system,’’ IEEE Access, vol. 5, pp.3410–3422, 2017.
3. P. Gope and R. Amin, ‘‘A novel reference security model with the situation based access policy for accessing EPHR data,’’ J. Med. Syst., vol. 40, no. 11, p. 242, Nov. 2016.
4. S. K. H. Islam, R. Amin, G. P. Biswas, M. S. Farash, X. Li, and S. Kumari, ‘‘An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments,’’ J. King Saud Univ. Compute. Inf. Sci., vol. 29, no. 3, pp. 311–324, Jul. 2017.
5. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, ‘‘PALK: Password-based anonymous lightweight key agreement framework for smart grid,’’ Int. J. Electr. Power Energy Syst., vol. 121, Oct. 2020, Art. no. 106121.