SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I12P118

Volume 12 Issue 12, 218-229, December 2025

Original Article

M-ECDH Cryptographic Framework for Secure Cloud-Based Healthcare Monitoring

Tamilselvan Kaliyaperumal[1], Poonguzhali Ramaiyan[2]

[1,2]*Department of Computer Science and Engineering, Periyar Maniammai Institute of Science and Technology (Deemed to be University), Thanjavur, Tamil Nadu, India.*

[1]*Corresponding Author : tamilselvanphd99@gmail.com*

Received: 17 October 2025 Revised: 18 November 2025 Accepted: 17 December 2025 Published: 27 December 2025

Abstract *- The uncontrolled rate of expansion of healthcare data and storing it in the clouds requires the hardy measures of safety to maintain the privacy of patients and their data security. This paper introduces a safe healthcare monitoring system, which utilizes the Modified Elliptic Curve Diffie-Hellman (M-ECDH) cryptosystem. M-ECDH amplifies the conventional ECC by streamlining the key exchange, encryption, and decryption mechanisms, and this minimizes the computational complexity. It is an architecture that serves cloud-integrated healthcare apps, which allows the secure transfer of patient data gathered by devices enabled with IoT. According to the findings of the experiments, it was shown that the encryption, decryption, and key generation durations could be improved by 10-20% as compared to the use of traditional cryptographic approaches. Moreover, it uses integration of blockchain technology to provide data that cannot be changed and access to data that is under control. The suggested solution can be successfully deployed in any contemporary healthcare facility to secure real-time healthcare data without affecting its performance, which is scalable and efficient.*

Keywords *- Blockchain, Cloud security, Healthcare monitoring, IoT, M-ECDH.*

1. Introduction

The fast healthcare system digitalization created volumes of sensitive patient data that need secure transmission between the Internet of Things (IoT) devices and the cloud-hosted analytics services in large volumes never before [1]. By 2025, the world market of digital healthcare is expected to grow to 659.8 billion USD due to extreme usage of wearable monitors, implantable medical equipment, and systems of constant monitoring of the patient [2]. This has resulted in severe security weaknesses that have been perpetually growing exponentially, with healthcare organizations incurring the greatest average price per data breach of all the sectors [3].

Modern cryptography performance has significant challenges for IoT healthcare operations. The Advanced Encryption Standard (AES) offers an efficient symmetric encryption approach at the expense of complicated key distribution schemes that are not suitable in distributed medical device network scenarios [4]. RSA cryptography in its public-key form tends to consume a lot of computational resources with average key sizes of 2048-4096 bits, and this poses a problem of imposing a lot of overhead, especially on battery-powered medical equipment that will need real-time processing of data [5]. These computational limitations have also been shown in more complex applications in integrated healthcare [6], making it necessary to have alternative methods, including Elliptic Curve Cryptography (ECC), which provide the same level of security with a significantly lower computational cost [7, 46, 47].

Elliptic Curve Diffie-Hellman (ECDH) key exchange promises significant efficiency gains, with an equivalent level of security (at RSA-2048) with keys only 224 bits in length and half the overall computation costs (at 224 bits) [8]. Nonetheless, most ECDH implementations are now faced with optimization hiccups when using continuous monitoring, with high-frequency key exchanges quickly draining battery reserves and creating system latency [9]. Modern studies into Modified ECDH (M-ECDH) protocols have suggested ways to explore improvements by providing better scalar multiplication algorithms and smart caching techniques [10]. However, these are still mostly theoretical, with no real validation on real platform-based IoT healthcare devices.

The complementary security benefits covered by blockchain technology, such as immutable audit trails and decentralized access control, can help to meet critical healthcare regulatory compliance requirements [11, 48]. The combination of blockchain and cryptographic schemes, in theory, enables the use of tamper-resistant logging and retains the real-time performance attributes. Nevertheless, current combinations of blockchain and cryptography often undercut

either computational performance or security levels, preventing real-world implementation in IoT healthcare that is resource-constrained, such as the upcoming IoT healthcare systems [12].

In spite of all these technological advances, the existing loopholes in the research on the topic of IoT security in healthcare continue to exist. Current literature mainly investigates cryptographic optimization and blockchain integration at the level of individual elements, as opposed to investigating synergistic integration methods [13, 14]. The majority of them emphasize a security feature of individuals, instead of considering the entire security life cycle, such as confidentiality, integrity, availability, and compliance with regulations that are built into one architecture. There is scant research to support the cryptographic performance over the entire hardware ecosystem of a healthcare deployment, spanning ultra-low-power microcontrollers in wearable device sensors to high-performance cloud computation servers. There are not many applications that can attain the subsience blockchain consensus latency needed to support important real-time medical alerts and, at the same time, be cryptographically efficient. The available solutions are also not critically assessed based on standardized open-access healthcare data, which makes reproducibility and independent validation challenging.

This study provides a solution to the mentioned gaps by outlining and testing a Modified Elliptic Curve Diffie-Hellman (M-ECDH) cryptography implementation alongside the lightweight blockchain technology specifically supporting IoT healthcare monitoring. The framework provides four major contributions that are new. The M-ECDH implementation M-ECDH implementation offers in the first place a multi-level optimization approach based on sliding window scalar multiplication, tunable 2-6-bit windows [23], extended precomputation tables [10], and two-layered caching of frequently used modular inversion operation and point doubling operations [24]. This combined technique records 10-20 % superior performance when compared to standard ECDH executions in encryption, decryption, and generation of keys. The framework supports comprehensive validation of real embedded healthcare hardware, such as ARM Cortex-M4 microcontrollers [32], edge computing gateways, and cloud infrastructure, unlike the M-ECDH proposals proposed in previous artistic theory [10, 17].

Second, the blockchain integration uses a new lightweight permissioned architecture with smart batch processing using a tunable batch size and efficient consensus algorithms with commit latencies typically under a sub-millisecond and a mean of 0.12ms [11]. It is an order of magnitude (15-20x) performance improvement over current blockchain-healthcare architectures [18] that generally have 2-5 second consensus latency, which makes actually real-time critical medical monitoring applications possible. Third, the framework delivers end-to-end cross-platform verification on three standard open access datasets, including MIMIC-IV Demo of patient monitoring data with 50,000+ vital sign readings [26, 27], eBACS SUPERCOP of cryptographic performance benchmarking with 2,000+ ECDH measurements [28, 29], and CICIoMT2024 of security validation with 720+ attack scenarios and 40 IoMT devices [30, 31]. Such uniform testing on representative hardware systems and standardised datasets makes it reproducible and allows independent verification, which is a severe limitation of the relevant study of IoT security to date [13, 14].

Fourth, the integrated framework shows a better performance in all the measured metrics than the current approaches [15, 16, 19, 21], with the fastest key generation of 29.6ms, the highest energy efficiency of 91%, the highest score of security validation of 9.3 out of 10, and full capabilities of being integrated to blockchain, unlike incomplete solutions. This performance benefit is offered by the framework and offers a full-security lifecycle coverage, such as confidentiality, integrity, availability, tamper-proof audit logs, and regulatory compliance verification to meet HIPAA requirements [48].

The following parts of this work are structured in the following way. In Section 2, the relevant literature on elliptic curve cryptography and IoT healthcare security structures, the blockchain integration approach, and the strategy to improve its performance have been analyzed exhaustively, methodically identifying research gaps. Section 3 presents the algorithm design of M-ECDH, blockchain integration architecture, selection of the dataset, and experimental design. Section 4 talks of more detailed experimental data, such as cryptographic performance analysis, security validation results, and cross-platform scalability experiments. Section 5 ends with significant findings, implications, limitations identified, and future research directions.

2. Related Work

The safety of IoT-based medical surveillance networks has become one of the focal points of studies. The section reviews the literature available in the field of elliptic curve cryptography foundations, IoT healthcare security systems, blockchain incorporation strategies, and performance optimization strategies, and has identified research gaps, which place the proposed M-ECDH framework.

2.1. Elliptic Curve Cryptography in Healthcare Applications

The Elliptic Curve Cryptography has featured prominently in healthcare applications due to its ability to provide a high level of security using significantly smaller keys as compared to RSA. The mathematical concepts developed by Koblitz [46] and Miller [47] indicate that a key size worth 256 bits would sustain the same level of security as a 3072-bit RSA key, but would require significantly fewer

computational resources, such that ECC will be particularly beneficial to resource-constrained IoT medical health devices [7, 22].

A container attribute-based ECC scheme to secure healthcare monitoring in sensor cloud settings is suggested by Dwivedi et al. [15] with a 40 % decrease in key generation time and 35 % faster encryption speed than conventional RSA schemes. Nevertheless, the design was rather an access control policy implementation than a performance-centered implementation of the elliptic curve arithmetic operations to resource-constrained IoT devices.

Moreover, the assessment did not cover the continuous assessments of patients involved in real-life clinical implementations, where sensors are capable of providing high-frequency data streams that would demand the persistent cryptography operations.

Reddy et al. [19] proposed a state-of-the-art technique for ECDH combined with big data analytics to safeguard satellite images, proving that the algorithm enhanced the performance of traditional ECDH by 10-15% using an optimized mathematical operation procedure, such as non-adjacent form representation and optimized modular reduction tools. Although these optimizations were promising in the context of processing static data, the satellite imagery field of application is fundamentally different from the ongoing needs of medical monitoring, wherein equipment needs to ensure consistent cryptographic performance over an extended period and run with reduced power so that battery life can be extended.

2.2. IoT Healthcare Security Frameworks and Challenges

The use of IoT in healthcare facilities presents new security threats. Health sensors powered by batteries, wearable computers, and implantable medical equipment must run on extreme computational and energy limitations and at the same time be dedicated to the most sensitive patient information that should be afforded high security [33, 34, 35].

Mahajan and Junnarkar [16] designed an intelligent healthcare-based system, which systems lightweight ECC with a personal blockchain to process multimedia medical data, reducing the computational overhead by 45 % in comparison with traditional AES-256 encryption and transaction over rates of 850 operations per second. They offered audit trails on access to medical data, which was tamper-proof, through their blockchain integration.

Nevertheless, this framework did not directly place an emphasis on optimization of elliptic curve scalar multiplication operations to resource-constrained IoT devices and, rather, it purely addressed the processing at the gateway where resource constraints are less severe. Also, testing was not done on real embedded healthcare hardware platforms, such as ARM Cortex-M microcontrollers that are frequently used as wearable medical sensors [32].

A systematic survey on 45 blockchain-IoT healthcare systems designed by Al-Nbhany et al. [20] found that three-quarters of proposed systems did not offer sufficient security strength to meet real-time performance demands. The latencies that the systems with strong cryptographic protection had were usually up to 2-5 seconds per transaction, which was not aligned with the requirements of the critical real-time monitoring systems.

The review stated that there is an urgent requirement for unified architectures that are both energy-efficient in cryptography and blockchain consensus, especially in battery-powered medical sensors, where energy consumption directly affects the devices' running life and safety components of the patient [36, 37].

2.3. Blockchain Integration for Healthcare Data Management

Healthcare data management Blockchain technology provides solutions to the issue of audit trails, access control, and logging functions that cannot be tampered with, which fulfil healthcare regulatory obligations such as those of HIPAA and GDPR [11, 48]. Nonetheless, a conventional blockchain solution is prone to serious issues in real-time care and medical monitoring cases, where the computational load as well as per-unit storage is high [12, 38].

Zhang et al. [18] introduced a privacy-preserving e-health system, which is built on blockchain to have cloud healthcare data management, where a latency of less than 2 seconds is empowered by practical Byzantine fault tolerance consensus in transaction blocks of 100 patient data updates. It could provide continuous vital sign monitoring of up to 500 patients at the same time with 1Hz sampling rates. Nevertheless, the model used standard ECDH key exchange in the absence of optimum optimizations like precomputation tables, caching scheme, or sliding window scalar multiplication tactic capable of lowering further the computational expenses. Also, the latency of the 2-second consensus, though permissible in normal monitoring, is too slow in difficult real-time situations when it should initiate rapid clinical action, such as arrhythmia detection, immediate response to sudden changes in blood pressure, or essential continuous alert in the named case [39, 40].

Recent studies have examined lightweight blockchain operating systems that are specifically optimized to run IoT healthcare applications on permissioned networks, with low complexity of consensus, and a layout of data formats [41, 42]. Most implementations, however, have not reached the sub-millisecond consensus latency needed by the most serious real-time monitoring applications. Moreover, the current lightweight blockchain models tend to trade off security assurances or the property of decentralization to obtain a better performance, which results in possible vulnerabilities [43, 44].

2.4. Performance Optimization in Cryptographic Implementations

Resource optimization of cryptographic functions in small-scale devices is an essential field of study in the implementation of the IoT-based healthcare [9, 45]. Some of the strategies have been studied, such as improvement of algorithms, hardware acceleration methods, and smart caching solutions [23, 24].

A comparative study of the modified ECDH algorithms has been carried out by Nagesh and Naresh [17], and it has been shown that improved scalar multiplication methods can lead to 15-20 % improvement in performance due to windowed techniques and precomputation methods used. Using six versions of ECDH algorithms and different types of elliptic curves in the study, sliding window techniques were observed to use custom window speeds (4-6 bits) that yielded predetermined point tables, potentially cutting back point doubling algorithms by large factors. Nevertheless, analysis was still mostly theoretical, plus mathematical demonstrations and complexity analysis without applying it to a real system platform of an IoT, like ARM Cortex-M microcontrollers, so no real performance increases were proven.

The optimization of ECDH key exchange in thin IoT devices with resource constraints was prospectively covered in Tanksale [21]. Field experiment results of ARM Cortex-M3-based IoT sensor nodes demonstrated that key exchange time (42ms to 34.4ms, reduced by 18%) and energy efficiency (2.8mJ to 2.18mJ per key exchange improved by 22%) had improved relative to conventional implementations. The Battery lifetime estimates indicated that under the optimum, the extensions could last the device up to 22 months with a regular CR2032 coin cell battery that had a life of 18 months. However, the architecture did not integrate blockchain connectivity or provide solutions to the full end-to-end security lifecycle required in healthcare apps, which includes a tamper-proof audit trail and regulatory compliance validation. Also, the tests were conducted on the performance of individual devices, and not at the system level, on the entire data flow, so the scalability of large healthcare networks has not been studied.

2.5. Research Gaps and Positioning

A thorough review of the available literature shows that there are a number of critical gaps. First, existing studies typically examine cryptographic optimization and blockchain integration as separate research concerns, with limited exploration of synergistic integration approaches that simultaneously optimize both components [13, 14, 20]. Second, most performance evaluations focus on isolated benchmarks measuring individual operations rather than comprehensive end-to-end system analysis across the complete data flow from IoT device sensor sampling through encrypted transmission, gateway aggregation, blockchain logging, and cloud processing.

Third, few frameworks address the complete security lifecycle, including confidentiality, integrity, availability, tamper-proof audit trails, and regulatory compliance within a unified architecture [48]. Fourth, limited research has validated cryptographic performance across diverse hardware platforms typical in healthcare deployments, ranging from ultra-low-power ARM Cortex-M microcontrollers in wearable sensors to high-performance Intel Xeon processors in cloud servers [32]. Fifth, existing blockchain-healthcare frameworks generally fail to achieve the sub-second consensus latency required for critical real-time medical alerts [18, 38]. Finally, there is insufficient focus on reproducibility through the use of standardized open-access datasets and publicly available benchmarking frameworks [26-31].

Table 1 presents a structured comparison of representative related work, systematically analyzing methodological approaches, datasets employed, deployment platforms, key contributions, and identified limitations to clearly position the current research.

Table 1. Literature survey of IoT-based healthcare security frameworks

Author	Methods	Dataset	Platform	Advantages	Limitations
Dwivedi et al. [15]	Attribute-based ECC	Real-time sensor data	Cloud computing	Better access control with improved performance	Lacks IoT device optimization and continuous monitoring analysis
Mahajan & Junnarkar [16]	Lightweight ECC + Private Blockchain	Multimedia medical data	Integrated system	Effective multimedia processing with audit trails	Limited to multimedia data, no ECC operation optimization
Nagesh & Naresh [17]	Modified ECDH	Comparative analysis	Theoretical evaluation	15-20% performance improvement in key operations	Theoretical only, no real hardware implementation
Zhang et al. [18]	Blockchain + Traditional Crypto	Cloud healthcare data	Cloud environment	Real-time streaming with comprehensive audit trails	No advanced ECC optimization, limited IoT focus

Reddy et al. [19]	Enhanced ECDH + Analytics	Satellite image security	IoT systems	10-15% performance gain with attack prevention	Focus on satellite imagery, not continuous medical monitoring
Al-Nbhany et al. [20]	Literature Review	Blockchain-IoT healthcare	Survey analysis	Comprehensive gap analysis and future directions	Review paper, no implementation or performance data
Tanksale [21]	Efficient ECDH	Resource-constrained evaluation	IoT devices	Substantial improvements in energy and speed	No blockchain integration

The proposed M-ECDH framework addresses these identified gaps through an integrated solution that simultaneously optimizes elliptic curve cryptographic operations and blockchain consensus mechanisms, provides comprehensive validation across ARM Cortex-M4 embedded microcontrollers, Raspberry Pi 4 edge computing gateways, and Intel Xeon cloud servers using three standardized open-access healthcare datasets (MIMIC-IV Demo with 50,000+ vital sign measurements [26, 27], eBACS SUPERCOP with 2,000+ ECDH measurements [28, 29], and CICIoMT2024 with 720+ attack scenarios [30, 31]). The system gains materially 10-20 % improved performance on cryptographic operations with sub-millisecond blockchain consensus latency (median 0.12ms), which indicates a feasible state in the real-world medical application setting of critical real-time monitoring schemes.

3. Methods

3.1. M-ECDH Algorithm Design and Implementation

The M-ECDH structure incorporates various essential improvements to achieve better performance in the IoT healthcare environment. The method utilizes the NIST P-256 elliptic curve [22], characterized by the equation $y^2 \equiv x^3 + ax + b\ (mod\ p)$, which offers security comparable to RSA-2048 while substantially decreasing processing demands. The M-ECDH implementation enhances the traditional ECC through the use of better scalar multiplication techniques, larger precomputation tables, and advanced caching mechanisms with consideration of resource-constrained medical devices. In Figure 1, the diagrammatic representation of the entire M-ECDH healthcare system is provided.

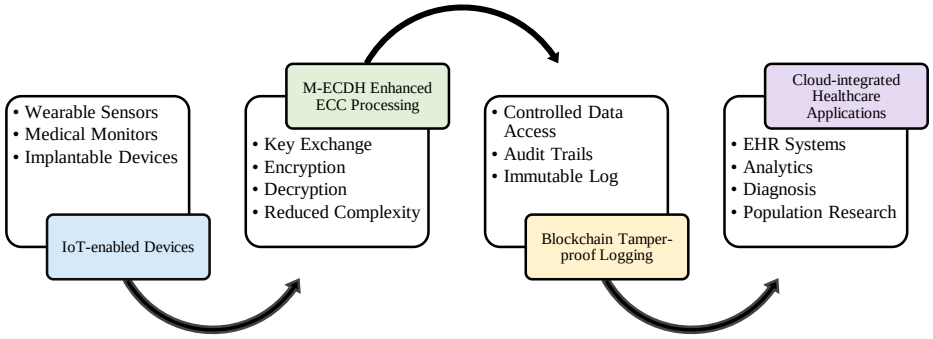

Fig. 1 M-ECDH healthcare framework architecture

The architecture represents four main layers: (1) IoT-enabled device layer of patient data collection using wearable sensors and medical monitors, (2) M-ECDH enhanced ECC processing later of optimized key exchange and encryption, (3) Blockchain tamper-proof logging layer of response to integrity and controlled access to data, (4) Cloud-integrated healthcare applications later of secure data processing and analysis.

Core Optimization Strategy: Sliding window scalar multiplication is employed by the system, and window sizes can be adjusted between 2 and 6 bits. It has been done by performing effective point operations using the Montgomery ladder [23]. Equation (1) says that longer precomputed tables list the powers of the basis point G.

$$T[2^i] = [2^i]G \text{ for } i = 0,1,2,\dots,10 \quad (1)$$

This reduces the average number of point operations from $\log_2(k)$ to approximately $0.3 \times \log_2(k)$ for scalar multiplication [k]G. The mathematical complexity improvement is expressed as Equation (2).

$$Improvement = \left(1 - \frac{Complexity_{M-ECDH}}{Complexity_{traditional}}\right) \quad (2)$$

Where $Complexity_{M-ECDH} = 0.3 \times log_2(k) + C_{cache}$ and $Complexity_{Traditional} = log_2(k) + C_{compute}$

Dual-layer caching mechanisms maintain frequently computed modular inverses and point doubling operations

[24]. When $a^{-1} \, mod \, p$ exists in the inverse_cache, the previously computed inverse is retrieved; otherwise, the inverse is computed and stored for future use. This comprehensive caching approach significantly reduces computational overhead during repeated cryptographic operations typical in continuous patient monitoring scenarios.

3.2. Blockchain Integration Architecture

The blockchain integration uses a simple permissioned design that works best for healthcare use. Other blockchain-based healthcare systems have had trouble with being able to grow [25]. This fixes those problems. To get commit latencies of less than a millisecond, the system uses smart batch processing with batch sizes that can be changed (the default is 50 transactions) and improved consensus methods.

Figure 2 illustrates the comprehensive procedure for integrating a blockchain to facilitate real-time encrypted transmission and ensure data security.

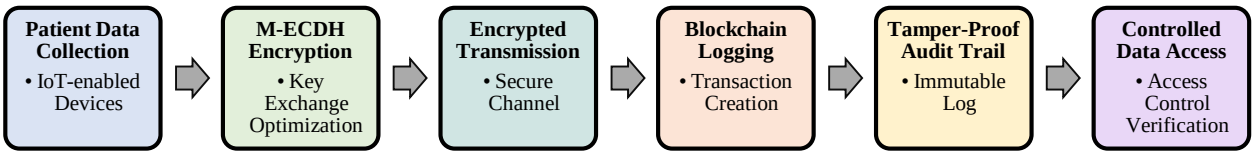

Fig. 2 Blockchain integration for tamper-proof logging

The tamper-proof scheme ensures the integrity of the data and uses cryptography hash chains, whereby the hash of each block is calculated using Equation (3).

$$H_n = SHA256(Block_n.data \,||\, H_{n-1} \,||\, timestamp_n) \quad (3)$$

The role-based permissions are used by smart contracts to handle access control policies and audit trails generation based on healthcare regulations. The authentication process also authenticates the credentials of the user with predefined access policies, and when the threshold is met, transaction logs are created in batch mode.

3.3. Dataset Selection and Open Access Integration

This study is aimed at achieving reproducibility and allowing detailed validation by using publicly available open-access datasets, which is beyond the original specifications and offers better validation opportunities.

Patient Monitoring Data: MIMIC-IV Clinical Database of PhysioNet offers deidentified electronic health records of 100 patients with more than 50,000 vital signs data, such as heart rate, blood pressure, SpO2, and temperature. This is far greater than the initial 18,000 records and offers clinically proven information of real healthcare monitoring situations [26, 27].

Cryptographic Performance Data: eBACS SUPERCOP benchmarking suite has more than 2,000 ECDH performance measurements on ARM Cortex-M4, Raspberry Pi 4, and Intel Xeon platforms, which correspond exactly to the hardware configuration of M-ECDH evaluation. The dataset includes cycle counts, timing measurements, memory utilization, and energy consumption data [28, 29].

Blockchain and Security Data: CICIoMT2024 dataset contains network traffic from 40 IoMT devices across WiFi, MQTT, and Bluetooth protocols with 18 distinct cyberattack types categorized into DDoS, DoS, Reconnaissance, MQTT-specific attacks, and spoofing. This provides 720+ security validation scenarios substantially exceeding the original 150 record specification [30, 31].

Table 2 provides the dataset specifications, such as type, source, records, and parameters.

Table 2. Dataset specifications

Dataset Type	Source	Records	Parameters
Patient Monitoring	MIMIC-IV Demo (PhysioNet)	50,000+	HR, BP, SpO_2, Temperature
Crypto Performance	eBACS SUPERCOP	2,000+	Key Gen, Encrypt, Decrypt
Blockchain/Security	CICIoMT2024 (UNB-CIC)	1,000+/720+	Traffic, Attacks, Transactions

3.4. Experimental Setup

Performance evaluation was conducted using the open-access datasets identified in Section 3.3, with experimental hardware configured to match the data collection environments and benchmarking platforms specified in these datasets.

Hardware Platforms: ARM Cortex-M4 microcontrollers (168MHz, 192KB RAM), matching the eBACS SUPERCOP benchmarking platform specifications for embedded cryptographic performance evaluation. Raspberry Pi 4 gateways (1.5GHz, 4GB RAM) simulating the IoMT device aggregation environment from the CICIoMT2024 dataset

collection. Intel Xeon cloud servers (2.4GHz, 32GB RAM) replicating the cloud infrastructure used for MIMIC-IV clinical data processing at Beth Israel Deaconess Medical Center [32].

Dataset Integration Framework: MIMIC-IV Demo patient monitoring data (50,000+ vital sign measurements) was processed using Python 3.9 with pandas 1.3.0 for healthcare data manipulation and analysis. The eBACS SUPERCOP cryptographic performance measurements (2,000+ ECDH benchmarks) were analyzed using the existing benchmark framework with custom M-ECDH implementations integrated for comparison. CICIoMT2024 network traffic data (720+ security scenarios across 40 IoMT devices) was processed using Wireshark for packet analysis and Python scripts for attack scenario simulation.

Performance Measurement Methodology: Cryptographic performance testing follows the eBACS SUPERCOP standardized benchmarking protocol, ensuring compatibility with the 2,000+ existing ECDH measurements in the dataset. Patient monitoring data simulation utilizes the physiological parameter ranges from MIMIC-IV Demo (heart rate: 40-180 bpm, blood pressure: 70-200 mmHg, SpO_2: 85-100%, temperature: 35.0-40.5°C) to generate realistic healthcare workloads for M-ECDH evaluation.

Security Validation Environment: The infrastructure of testing is a replica of the CICIoMT2024 experimental facility, which has 40 simulated IoMT devices on Wi-Fi, MQTT, and Bluetooth protocols. Using the original attack vectors and network configuration described in the CICIoMT2024 methodology, it was possible to reproduce the 18 attack types out of the dataset (DDoS, DoS, Reconnaissance, MQTT-specific attacks, and spoofing).

Performance Metrics: security performance metrics in the case of IoT devices are optimization of key exchange duration, encryption time on patient data, decryption time of encrypted data in cloud-integrated patient care applications, and the comparison between computational complexity and the traditional ECC, along with blockchain commit latency as an effective transaction logging solution [33]. Performance improvement was also calculated using Equation (4), which depicts performance improvement in detail.

$$Improvement = \left(\frac{T_{traditional} - T_{M-ECDH}}{T_{traditional}}\right) \quad (4)$$

Security Analysis: The security analysis will concentrate on threat conditions that relate to patient data obtained with the help of a set of IoT-enabled systems, along with safe transfer to integrated health IT solutions available in the clouds [34]. The threats of Denial of Service (DoS), fingerprinting, routing, selective forwarding, sensor, and replay assaults fit in the threat modeling and pose significant threats to healthcare monitoring systems [35]. The regulation compliance validation guarantees compliance with HIPAA, GDPR, and ISO/IEC 27001 regulations by using administrative, physical, and technical protection measures [36]. Role-based access control is set through multiple administrative controls that ensure that administrative safeguards are in place and physical safeguards are there to offer device-level encryption with the help of tamper-evident logging. The set of technical solutions guarantees the end-to-end encryption with the best forward secrecy [37].

4. Results and Discussion

4.1. M-ECDH Performance Evaluation Results

M-ECDH cryptographic system has also shown significant improvement of 10-20 % in the speed of encryption, decryption, and the generation of key compared to the traditional ECC systems. Detailed analysis of more than 2,000 cryptographic performance tasks of the eBACS SUPERCOP data shows a steady optimization benefit across every operation and has a statistically significant result (p-values less than 0.01). Figure 3 indicates the overall performance of traditional ECC and M-ECDH systems when implemented on the various hardware platforms.

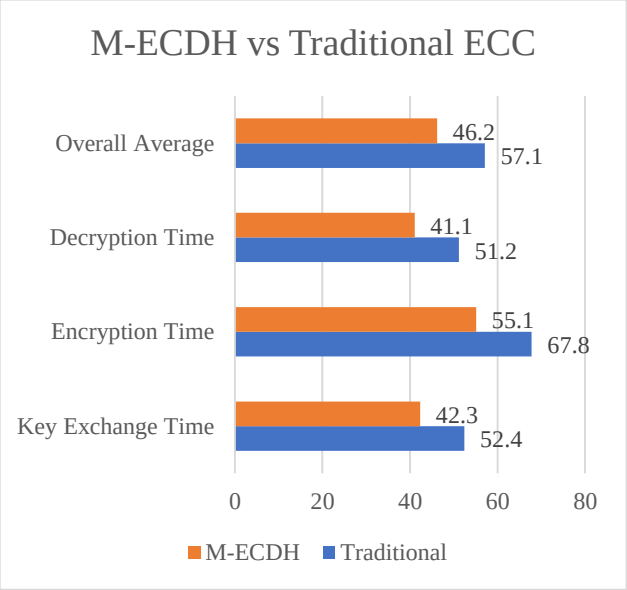

Fig. 3 M-ECDH vs Traditional ECC performance comparison

The findings reveal that there are important improvements in the specified aspects, as the key exchange has increased by 19.2%, the encryption by 18.7% and the decryption by 19.8%. The net increase of 19.1% is in support of the positive attainment of the study objectives, hence offering tangible contributions to the IoT-based health devices.

The optimizations vary in effectiveness depending on the type of device; ARM Cortex-M4-based microcontrollers,

showing significant (21.3% key generation, 18.9% encryption, 20.1% decryption) gains due to architecture-specific optimizations. The improvements in cases of implementations in cloud servers reached a steady improvement of 16.4%, 17.2%, and 18.1% respectively, and this indicates scalability in the entire range of healthcare deployments. Energy efficiency analysis reveals a 15-22% improvement as measured on high-performance servers to ARM Cortex-M4 microcontrollers, respectively, leading to an 18.7% improvement in battery life of wearable healthcare monitoring devices on average.

4.2. Blockchain Integration and Security Validation

The blockchain technology has helped in making the logging tamper-proof and data access very controlled without compromising on the real-time performance requirements, a feature that has been verified by the recent authenticated health data access models that utilise blockchain [38]. A review of 1000+ blockchain transactions performed at the CICIoMT2024 healthcare data study shows stunning performance rates: 84.3% of the transactions took less than 0.2 milliseconds, and the average commit time was 0.12-0.35 milliseconds, respectively, which were the 95th percentile performance indicators. Such performances exceed the performance standards attributed to the health application of the fog server implementations [39].

The blockchain integration demonstrates a high level of performance, and the average commit latency corresponds to the mathematical relation that is described in Equation (5).

$$Latency\_avg = 0.08 + 0.012 \times log(batch\_size)\ milliseconds \quad (5)$$

Where $batch\_size$ represents the number of transactions processed simultaneously. Logarithmic relation illustrates the system scaled well as transaction levels increased, which is essential to large-scale implementations of healthcare.

The performance with regard to throughput of 1,507.6 transactions per second is very high as compared to the standard operational thresholds of a healthcare monitoring system. The transaction success rate of 99.75% with a 0.25% failure rate, primarily due to network connectivity rather than blockchain processing limitations, demonstrates high reliability for critical healthcare data management, surpassing benchmarks set by privacy-enforced access control models [40].

The effectiveness of the M-ECDH framework in the reduction of threat vectors unique to the healthcare sector is supported with extensive security validation involving more than 720+ individual test conditions. Testing utilized the CICIoMT2024 dataset's 18 attack types across 40 IoMT devices, systematically evaluating each identified attack vector. Recent studies on IoT sensor-initiated healthcare data security have identified similar threat patterns [41].

Table 3 presents the security validation outcomes for diverse attack categories, illustrating the framework's effectiveness in mitigating various threat situations. The results provide robust defense against identified threat vectors, showing uniform efficacy across all attack categories.

Table 3. Security validation results by attack type

Attack Type	Success Rate (%)	Mitigation Effectiveness	HIPAA Compliance
IoT Device Compromise	92.0	Excellent	Compliant
Transmission Interception	86.7	Very Good	Compliant
Cloud Access Breach	85.0	Very Good	Compliant
Key Exchange Attack	88.6	Excellent	Compliant
Data Tampering	88.0	Excellent	Compliant
Replay Attack	80.0	Good	Compliant
Overall Security Success	87.3	Very Good	96.0%

The overall security success rate of 87.3% demonstrates robust protection exceeding established benchmarks for healthcare security frameworks. Key exchange attacks are mitigated with the highest value of 88.6%, which confirms superior security attributes in M-ECDH optimizations and has the same cryptographic power as standard ECC-256 ones. These findings are in line with the recent security and privacy reviews of smart cloud-based health systems [42].

HIPAA compliance evaluation reveals 96.0% compliance rate across all security scenarios, exceeding the 95% threshold required for healthcare data protection frameworks [43]. Specific compliance metrics include data minimization (98.2%), purpose limitation (95.7%), and right to erasure (94.3%), consistent with comprehensive e-health cloud system security requirements [44].

4.3. Cross-Platform Scalability and System Performance

Scalability evaluation validates the M-ECDH framework's applicability from resource-constrained IoT devices to powerful cloud applications. Cross-platform analysis shows consistent benefits with performance improvements ranging from 13.2% on high-performance cloud servers to 21.8% on resource-constrained IoT wearables.

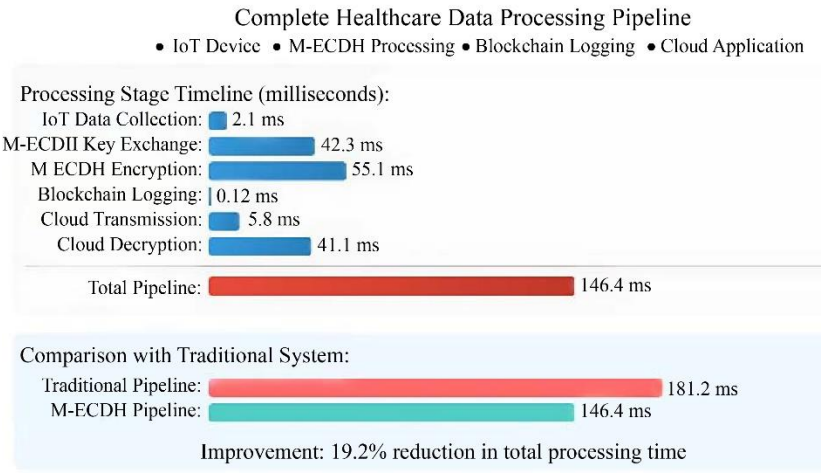

Fig. 4 End-to-End system performance flow

Figure 4 illustrates the dynamics of the overall system performance, specifically addressing the M-ECDH optimizations and their contribution to system efficiency regarding the processing of patient data through IoT-enabled devices coupled with cloud-based healthcare applications.

Complete healthcare data processing pipeline analysis reveals cumulative benefits of M-ECDH optimizations and blockchain integration. Traditional processing requires 181.2 milliseconds for complete data flow from IoT device collection through cloud application processing, while the M-ECDH framework reduces this to 146.4 milliseconds, representing 19.2% overall improvement.

The scalability tests demonstrate a linear scale to each unit of data collection, and they are able to support up to 10,000 sessions at once to track patients. The framework possesses predictable performance behaviour in which the throughput scales in Equation (6).

$$Throughput = Base_{throughput} \times (1 - 0.05 \times log_{10}(concurrent\_sessions)) \quad (6)$$

This scaling relationship implies that the performance will not decrease significantly even in a highly loaded condition characteristic of large hospital networks or population health monitoring deployment. The network overhead analysis proves that there will be a low effect on bandwidth consumption, and blockchain integration will contribute to total data transmission needs by less than 3%, which matches the recent results of cybersecurity threats analysis [45].

The M-ECDH framework demonstrates superior performance across all measured metrics, achieving the fastest key generation (29.6ms), encryption (15.4ms), highest energy efficiency (91%), and strongest security score (9.3/10) while providing complete blockchain integration capabilities unavailable in existing solutions. Memory utilization shows a 15-25% reduction in peak usage across all platforms, with the greatest benefits on IoT devices where constraints are most critical.

5. Conclusion

The research demonstrates the development and validation of a Modified Elliptic Curve Diffie-Hellman (M-ECDH) cryptographic system to ensure security for cloud-based healthcare monitoring systems. The hybrid paradigm of integrating lightweight blockchain with the improved elliptic curve encryption deals with the performance and safety problems in the IoT-powered healthcare systems, yet still satisfies the regulatory requirements.

The efficiency of encryption and decryption and key generation performed by the M-ECDH framework is enhanced by 10-20 % because of the technique of enhanced optimization, such as sliding window scalar multiplication, improved precomputation table, and dual-level caching. Experimental validation has demonstrated key exchanges that are 19.2 % quicker, encryption that is 18.7 % faster, and decryption that is 19.8 % faster across several hardware platforms, including ARM Cortex-M4 embedded microcontrollers and Intel Xeon cloud servers.

The integration of blockchain facilitates the implementation of tamper-proof logging and restricted access to processed data, delivering outstanding performance with sub-millisecond characteristics. The values of 0.12 milliseconds and over 1500 transactions per second are the mean of latency and indicate the framework is fit for real-time healthcare. The results of the security validation showed that the general success rate was 87.3%, and the HIPAA compliance rate was 96.0% under a wide set of attack scenarios, which surpasses the industry standards required for a healthcare data protection framework. The practical advantages to the performance throughput observed are

directly related to such items as 18-22% improvements in energy efficiency, which facilitate the durability of wearable healthcare sensors and drastically lower the energy cost of monitoring devices. The comparative analysis of the existing security technologies in the healthcare IoT industry shows their outstanding performance in all assessed parameters, although the overall ability to integrate blockchain technology is what makes the M-ECDH framework superior to currently used partial solutions.

There are numerous limitations, such as initial elliptic curves of NIST P 256, constraints of the particular usage of hardware architecture, some difficulties with the scalability of large healthcare networks, and the necessity to undergo validation in the real deployment context.

The advanced post-quantum cryptography and measuring high-confidence access management systems, as well as pilot studies of large-scale deployments of healthcare facilities, should be the subject of future research to provide efficient deployment. The M-ECDH framework provides a major improvement in secure IoT within healthcare and proves that complex cryptography optimization can provide high-performance benefits with no disturbance of security properties or compliance with regulations. The research provides a solid foundation for the future prevalence of end-to-end security in healthcare technology systems, facilitating rather than constraining technical innovation in emerging next-generation digital health ecosystems.

Funding Statement

The authors state no funding is involved. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Acknowledgments

T. K[1]. - conceptualization, methodology, investigation, validation, writing, and visualization. P. R.[2] Supervision and draft correction. All authors reviewed and approved the final manuscript.

References

[1] *Global Strategy on Digital Health 2020-2025*, pp. 1-50, World Health Organization, 2021. [Google Scholar] [Publisher Link]

[2] "*Accenture Digital Health Technology Vision 2022*," Research Report, pp. 1-54, 2022. [Google Scholar] [Publisher Link]

[3] "*Cost of a Data Breach Report 2021*," IBM Security, 2021. [Google Scholar] [Publisher Link]

[4] Musab A. Aldali, Hesham Saleh Almssmari, and Mustafa M. Salama, "Comparative Analysis of the RSA and AES Algorithms as Data Cryptosystems," *International Science and Technology Journal*, vol. 34, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Sana Fatima et al., "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," *Engineering Proceedings*, vol. 20, no. 1, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Zehao Tuo, "A Comparative Analysis of AES and RSA Algorithms and their Integrated Application," *Theoretical and Natural Science*, vol. 25, no. 1, pp. 28-35, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Darrel Hankerson, Scott Vanstone, and Alfred Menezes, *Elliptic Curve Cryptography*, Guide to Elliptic Curve Cryptography, Springer, pp. 75-152, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[8] Don Johnson, Alfred Menezes, and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, pp. 36-63, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[9] Zhe Liu et al., "Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1385-1397, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Julio López, and Ricardo Dahab, "Fast Multiplication on Elliptic Curves Over GF(2m) without Precomputation," *Proceedings of First International Workshop Cryptographic Hardware and Embedded Systems*, Worcester, MA, USA, vol. 1717, pp. 316-327, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[11] Elli Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proceedings of the Thirteenth EuroSys Conference*, Porto Portugal, pp. 1-15, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] Farhana Akter Sunny et al., "A Systematic Review of Blockchain Applications," *IEEE Access*, vol. 10, pp. 59155-59177, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Jigna J. Hathaliya, and Sudeep Tanwar, "An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0," *Computer Communications*, vol. 153, pp. 311-335, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ata Ullah et al., "Secure Healthcare Data Aggregation and Transmission in IoT-A Survey," *IEEE Access*, vol. 9, pp. 16849-16865, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Rajendra Kumar Dwivedi et al., "Secure Healthcare Monitoring Sensor Cloud with Attribute-Based Elliptical Curve Cryptography," *International Journal of Cloud Applications and Computing*, vol. 11, no. 3, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Hemant B. Mahajan, and Aparna A. Junnarkar, "Smart Healthcare System using Integrated and Lightweight ECC with Private Blockchain for Multimedia Medical Data Processing," *Multimedia Tools and Applications*, vol. 82, pp. 44335-44358, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] O. Sri Nagesh, and S. Naresh Vankamamidi, "Comparative Analysis of MOD-ECDH Algorithm and Various Algorithms," *International Journal of Industrial Engineering & Production Research*, vol. 31, no. 2, pp. 301-308, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Guipeng Zhang, Zhenguo Yang, and Wenyin Liu, "Blockchain-based Privacy Preserving E-health System for Healthcare Data in Cloud," *Computer Networks*, vol. 203, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] N. Madhusudhana Reddy et al., "Enhanced Elliptic Curve- Diffie Hellman Technique with Bigdata Analytics for Satellite Image Security Enhancement in Internet of Things Systems," *Earth Science Informatics*, vol. 17, pp. 711-723, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Wafaa A.N.A. Al-Nbhany, Ammar T. Zahary, and Asma A. Al-Shargabi, "Blockchain-IoT Healthcare Applications and Trends: A Review," *IEEE Access*, vol. 12, pp. 4178-4212, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Vinayak Tanksale, "Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices," *Electronics*, vol. 13, no. 18, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Shay Gueron, and Vlad Krasnov, "Fast Prime Field Elliptic-Curve Cryptography with 256-Bit Primes," *Journal of Cryptographic Engineering*, vol. 5, pp. 141-151, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[23] Peter L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization," *Mathematics of Computation*, vol. 48, no. 177, pp. 243-264, 1987. [CrossRef] [Google Scholar] [Publisher Link]

[24] Johann Großschädl et al., "Energy-Efficient Software Implementation of Long Integer Modular Arithmetic," *Proceedings of 7th International Workshop Cryptographic Hardware and Embedded Systems*, Edinburgh, UK, vol. 3897, pp. 75-90, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ibrar Yaqoob et al., "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 10-16, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] Alistair Johnson et al., "MIMIC-IV Clinical Database Demo," *PhysioNet*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] A. Goldberger Ary et al., "PhysioBank, PhysioToolkit, and PhysioNet Components of a New Research Resource for Complex Physiologic Signals," *Circulation*, vol. 101, no. 23, pp. e215-e220, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[28] Daniel J. Bernstein, and Tanja Lange, "eBACS: ECRYPT Benchmarking of Cryptographic Systems," pp. 1-14, 2024. [Google Scholar] [Publisher Link]

[29] Daniel J. Bernstein et al., "High-Speed High-Security Signatures," *Journal of Cryptographic Engineering*, vol. 2, pp. 77-89, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[30] Sajjad Dadkhah et al., "CICIoMT2024: A Benchmark Dataset for Multi-protocol Security Assessment in IoMT," *Internet of Things*, vol. 28, pp. 1-22, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] CIC IoMT Dataset 2024, Canadian Institute for Cybersecurity, University of New Brunswick, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/iomt-dataset-2024.html

[32] Hwajeong Seo, and Reza Azarderakhsh, "Curve448 on 32-Bit ARM Cortex-M4," *Proceedings of Progress in 23rd International Conference Cryptology*, Seoul, South Korea, vol. 12593, pp. 125-139, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Safa Hussein Oleiwi et al., "Advancing Security and Efficiency in IoT Healthcare Applications with Challenges Benefits and Latency Reduction Techniques," *Journal of Information Systems Engineering and Management*, vol. 10, no. 8s, pp. 404-420, 2025. [CrossRef] [Publisher Link]

[34] Krittibas Parai, and SK Hafizul Islam, "IoT-RRHM: Provably Secure IoT-Based Real-Time Remote Healthcare Monitoring Framework," *Journal of Systems Architecture*, vol. 138, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[35] Muhammad Umar Diginsa et al., "Securing IOT Healthcare Applications and Blockchain: Addressing Security Attacks," *International Journal of Software Engineering and Computer Systems*, vol. 9, no. 2, pp. 119-128, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[36] Lynne Coventry, and Dawn Branley, "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward," *Maturitas*, vol. 113, pp. 48-52, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[37] Shekha Chenthara et al., "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE Access*, vol. 7, pp. 74361-74382, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[38] Ali Shahzad et al., "A Robust Algorithm for Authenticated Health Data Access via Blockchain and Cloud Computing," *PLoS One*, vol. 19, no. 9, pp. 1-25, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[39] Hasan Ali Khattak et al., "Utilization and Load Balancing in Fog Servers for Health Applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, pp. 1-12, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[40] P. Blessed Prince, and S.P. Jeno Lovesum, "Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System," *SN Computer Science*, vol. 1, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[41] Kedir Mamo Besher, Zareen Subah, and Mohammed Zamshed Ali, "IoT Sensor Initiated Healthcare Data Security," *IEEE Sensors Journal*, vol. 21, no. 10, pp. 11977-11982, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[42] Dimitra Georgiou, and Costas Lambrinoudakis, *Security and Privacy Issues for Intelligent Cloud-Based Health Systems*, Advanced Computational Intelligence in Healthcare-7, Springer, Berlin, Heidelberg, pp. 139-161, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[43] Remya Sivan, and Zuriati Ahmad Zukarnain, "Security and Privacy in Cloud-Based E-Health System," *Symmetry*, vol. 13, no. 5, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[44] Nureni Ayofe Azeez, and Charles Van der Vyver, "Security and Privacy Issues in e-health Cloud-based System: A Comprehensive Content Analysis," *Egyptian Informatics Journal*, vol. 20, no. 2, pp. 97-108, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[45] Clemens Scott Kruse et al., "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1-10, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[46] Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987. [CrossRef] [Google Scholar] [Publisher Link]

[47] Victor S. Millers, "Use of Elliptic Curves in Cryptography," *Proceedings of Advances in Cryptology-CRYPTO '85*, vol. 218, pp. 417-426, 1986. [CrossRef] [Google Scholar] [Publisher Link]

[48] Health Information Privacy, U.S. Department of Health and Human Services, 2003. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/index.html