JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. 8, No. 3, Desember 2025, pp. 220-228 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v8i3.10709 e-ISSN: 2656-1948

COMPARISON OF ECDSA DAN EDDSA ALGORITHMS IN BLOCKCHAIN-BASED HEALTH RECORDS SECURITY

Nicholas Alexander[1], Bayu Angga Wijaya[2], Rico Wijaya Dewantoro[3], Monalisa[4]

[1,2,3,4]Fakultas Teknologi dan Ilmu Komputer, Universitas Prima Indonesia, Medan, 20118, Indonesia
[*]Email: [1]nicochuang88@gmail.com, [2]bayuanggawijaya@unprimdn.ac.id, [3]rico@unprimdn.ac.id, [4]monalisaxiao29@gmail.com

(Received: 9 September 2025, Revised: 24 September 2025, Accepted: 21 October 2025)

Abstract

The development of blockchain technology presents significant opportunities for the management of Electronic Health Records (EHR), owing to its decentralized, transparent, and tamper-resistant characteristics. However, security challenges remain, particularly regarding the use of the Elliptic Curve Digital Signature Algorithm (ECDSA), which, despite being compact and secure, has limitations in efficiency and potential vulnerabilities related to random nonce usage. This study aims to compare the effectiveness, efficiency, and security of ECDSA with the Edwards-curve Digital Signature Algorithm (EdDSA) in safeguarding the integrity and confidentiality of blockchain-based EHR systems. The research methodology involved simulations and evaluations of digital signature algorithms using an EHR dataset from Kaggle, focusing on performance testing, data validation, and the implementation of the Proof-of-Work (PoW) consensus mechanism. The results indicate that EdDSA outperforms ECDSA in terms of both speed and security. EdDSA achieved a signing time of 0.000180 seconds and a verification time of 0.000200 seconds, compared to ECDSA's 0.000962 seconds and 0.003204 seconds, respectively. While both algorithms successfully validated the data, neither was able to detect data alterations. From a blockchain perspective, PoW demonstrated high computational resistance, as evidenced by increased mining times—from 1,504 seconds for 4,000 blocks (difficulty target = 5) to 7,702 seconds for 20,000 blocks (difficulty target = 5)—thereby enhancing system integrity. Overall, EdDSA is considered more suitable for modern blockchain-based EHR implementations, although further research is needed to develop mechanisms for detecting data alteration.

Keywords: *Blockchain, Electronic Health Records (EHR), ECDSA, EdDSA, Proof-of-Work, Data Security*

**Corresponding Author: Nicholas Alexander*

1. INTRODUCTION

The adoption of Blockchain technology in electronic health record (EHR) systems continues to grow due to its decentralized, transparent, and immutable nature, which enables it to ensure the integrity and authenticity of patient data more effectively compared to conventional systems [1][2][3]. Nevertheless, several previous studies have shown that the implementation of blockchain in healthcare still faces major challenges in terms of security and privacy, particularly in preventing unauthorized access and protecting sensitive data confidentiality [4][5]. Therefore, strong, efficient, and attack-resistant cryptographic algorithms are needed to support reliable and secure Blockchain-based EHR systems [6].

To address these challenges, many blockchain systems currently rely on the Elliptic Curve Digital Signature Algorithm (ECDSA) because of its ability to produce compact digital signatures while maintaining strong security through the Elliptic Curve Discrete Logarithm Problem [7][8]. However, the efficiency of this algorithm remains a concern, as complex mathematical processes such as modular inversion and scalar multiplication can lead to performance degradation, especially when applied to large-scale systems like EHR [9]. Furthermore, research also indicates that ECDSA is vulnerable to implementation flaws, for example in the use of weak Random Number Generators (RNG), which could open critical security loopholes in healthcare data that should be protected.

In response to the limitations of ECDSA, the Edwards-curve Digital Signature Algorithm (EdDSA) was developed to provide a more efficient solution without compromising security. EdDSA leverages Twisted Edwards curves, deterministic nonces, and a faster verification process, making it highly suitable for implementation in blockchain-based systems that require high speed and low resource consumption [10].

Recent advancements have further emphasized the need for signature schemes that are resistant to side-channel attacks and offer robust security even under constrained environments, which are common in IoT-integrated healthcare infrastructures. In their studies, EdDSA has been proven to outperform ECDSA in terms of performance, particularly in the context of Blockchain and IoT. Moreover, according to a publication by Wiley, EdDSA is considered an efficient and cost-effective alternative to ECDSA, although its signature verification is slightly more computationally intensive [11]. Despite this, EdDSA's resistance to implementation errors, such as poor randomness, provides a compelling security advantage in privacy-sensitive applications like healthcare.

However, most existing studies tend to focus on the theoretical strengths of each algorithm or their performance in general-purpose blockchain and IoT environments, without evaluating them directly in the specific context of EHR systems. Moreover, few studies have conducted comprehensive implementation-based comparisons that examine both performance and security aspects simultaneously, especially in realistic blockchain-based healthcare scenarios.

This research aims to fill that gap by implementing and comparing ECDSA and EdDSA in a blockchain-based EHR setting, focusing not only on computational efficiency but also on security robustness and practical deployability. The findings are expected to guide future improvements in cryptographic protocol design for secure and scalable electronic health record systems.

2. RESEARCH METHOD

In this study, the researcher employed a quantitative research approach, which involves the collection of numerical data and statistical analysis to understand phenomena or answer research questions [12]. In this research, the research methodology involved simulations can be seen in Figure 1.

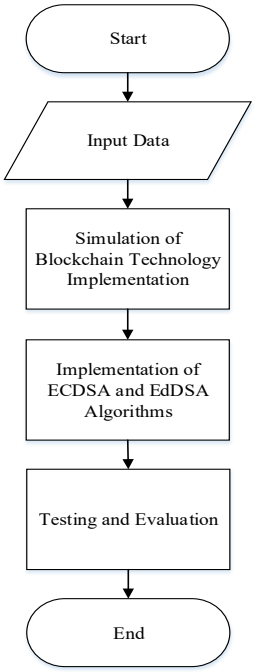


Figure 1. Stages of Research Methods

2.1 Input Data

The data used in this study consists of an Electronic Health Record (EHR) dataset obtained from Kaggle, comprising 20,000 records. The dataset can be accessed at the link: https://www.kaggle.com/datasets/gauravsrivastav2507/ehr-dataset. Table 1 below presents the dataset schema used in this study.

2.2 Simulation of Blockchain Technology Implementation

Table 1. Research Dataset

No	Patient_ID	Age	Gender	Tumor_Size (cm)	Tumor Type	Biopsy_Result	Treatment	Response_to_Treatment	Survival_Status
1	c044501a-43ca-4a0c-8b8b-991439ba1b6a	52	Female	5.08	Benign	Positive	Surgery	No Response	Survived
…	…	…	…	…	…	…	…	…	…
20.000	7af66d60-f88e-	62	Fema	7.46	Malign	Positive	Chemother	Complete	Survived

Implementation

At this stage, a simulation of integrating electronic health record (EHR) data with Blockchain technology is carried out. The main objective of this simulation is to ensure that each recorded data has an authentic, immutable digital footprint, and its validity can be verified [13][14][15]. The steps undertaken include:

1. Retrieving the EHR dataset, where each patient is stored in one block.
2. Performing hashing on the data to generate a unique and concise digital fingerprint.
3. Preparing the process of recording the data hash and digital signature into the Blockchain system simulation

2.3 Implementation of ECDSA and EdDSA Algorithms

This stage aims to compare two digital cryptographic algorithms, namely ECDSA and EdDSA, in the context of protecting EHR data on Blockchain. The implementation steps include:

1. Performing the digital signature process on EHR data using each algorithm (ECDSA and EdDSA). This involves generating a key pair, consisting of a private key and a public key, for each algorithm.
   a. In the case of ECDSA (Elliptic Curve Digital Signature Algorithm), the algorithm is based on the mathematical principles of elliptic curve cryptography and relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The private key is a randomly selected integer, and the public key is computed by scalar multiplication of the generator point on a chosen elliptic curve—commonly secp256k1. The signing process involves generating a random nonce k, computing a curve point R = kG, and producing a signature pair (r, s) where r is the x-coordinate of R and $s = k^{-1} (z + r \cdot d) \mod n$ (with d as the private key and z as the hashed message).
   b. In contrast, EdDSA (Edwards-curve Digital Signature Algorithm), particularly the Ed25519 variant, is based on Twisted Edwards curves and uses deterministic signatures. The key pair is derived from a hashed seed, and the signing process avoids the use of random nonces, which mitigates risks from weak RNGs. Instead, the algorithm computes a deterministic r from the message and private key, calculates a curve point R = rB, and derives the signature as (R, S) where $S = r + H(R \parallel A \parallel M) \cdot a \mod q$. Here, H is a hash function, A is the public key, and M is the message. These differences result in EdDSA offering better resistance to certain attack vectors and more efficient computation in constrained environments.
2. Integration into Blockchain.
   After the digital signing process is completed, the signature is embedded into the Blockchain block. Each block stores the original EHR data, the data hash and the previous block hash, the digital signature (ECDSA or EdDSA), as well as the public key for verification. This structure ensures multilayer authenticity and data integrity.

The results of this implementation serve as the basis for evaluating the strengths and weaknesses of each algorithm in the context of EHR protection.

2.4 Testing and Evaluation

As an extension of the simulation, testing of the Proof-of-Work (PoW) mechanism was carried out in the Blockchain system to enhance the security of EHR data recording. PoW is a consensus method in Blockchain that requires a mining process, namely searching for a nonce until a hash with a leading zero is obtained according to the difficulty target. The tests were conducted with varying numbers of blocks (4,000–20,000) and difficulty levels of 1–5. The results showed that the higher the difficulty level, the longer the mining time, which strengthens the role of Blockchain in maintaining integrity, validity, and resistance to data manipulation.

After the Blockchain system testing was completed, testing and evaluation were conducted to compare the performance of the two digital signature algorithms:

1. Security.
   a. Assessing resilience against cryptographic attacks, such as the reuse of random value *k* in ECDSA.
   b. Observing signature length and stability in each algorithm as part of storage and communication efficiency within Blockchain.
2. Efficiency (Performance).
   a. Measuring the speed of the signing and verification processes.
   b. Evaluating which algorithm is more efficient in the context of real-time use for Blockchain-based EHR systems.
3. Effectiveness (Validation and Data Integrity).
   a. Assessing whether the digital signatures can be correctly validated.
   b. Testing whether modified data can be detected as invalid, indicating that integrity protection functions properly.

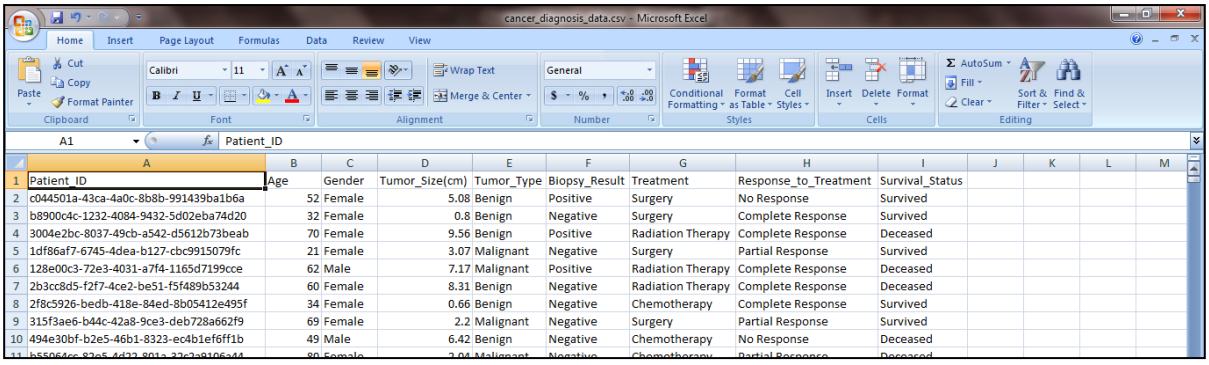
The evaluation results are then used to conclude which algorithm is more suitable for application in Blockchain-based EHR data protection scenarios, taking into account the balance between efficiency, effectiveness, and security.

3. RESULT AND DISCUSSION

The results of this study are a comparison of the security, as well as the effectiveness and efficiency of performance, between the ECDSA and EdDSA algorithms in protecting the integrity and confidentiality of Blockchain-based Electronic Health Record (EHR) systems.

3.1 Data Input Results

The dataset used in this study is an Electronic Health Record (EHR) dataset that can be downloaded from the previously provided link, in the form of an Excel file containing patient health records, as shown in Figure 2.



cancer_diagnosis_data.csv - Microsoft Excel

	A	B	C	D	E	F	G	H	I
1	Patient_ID	Age	Gender	Tumor_Size(cm)	Tumor_Type	Biopsy_Result	Treatment	Response_to_Treatment	Survival_Status
2	c044501a-43ca-4a0c-8b8b-991439ba1b6a	52	Female	5.08	Benign	Positive	Surgery	No Response	Survived
3	b8900c4c-1232-4084-9432-5d02eba74d20	32	Female	0.8	Benign	Negative	Surgery	Complete Response	Survived
4	3004e2bc-8037-49cb-a542-d5612b73beab	70	Female	9.56	Benign	Positive	Radiation Therapy	Complete Response	Deceased
5	1df86af7-6745-4dea-b127-cbc9915079fc	21	Female	3.07	Malignant	Negative	Surgery	Partial Response	Survived
6	128e00c3-72e3-4031-a7f4-1165d7199cce	62	Male	7.17	Malignant	Positive	Radiation Therapy	Complete Response	Deceased
7	2b3cc8d5-f2f7-4ce2-be51-f5f489b53244	60	Female	8.31	Benign	Negative	Radiation Therapy	Complete Response	Deceased
8	2f8c5926-bedb-418e-84ed-8b05412e495f	34	Female	0.66	Benign	Negative	Chemotherapy	Complete Response	Survived
9	315f3ae6-b44c-42a8-9ce3-deb728a662f9	69	Female	2.2	Malignant	Negative	Surgery	Partial Response	Survived
10	494e30bf-b2e5-46b1-8323-ec4b1ef6ff1b	49	Male	6.42	Benign	Negative	Chemotherapy	No Response	Deceased

Figure 2. Research Dataset

The dataset is input into Google Colab by placing it in the dataset section, as shown in Figure 3.

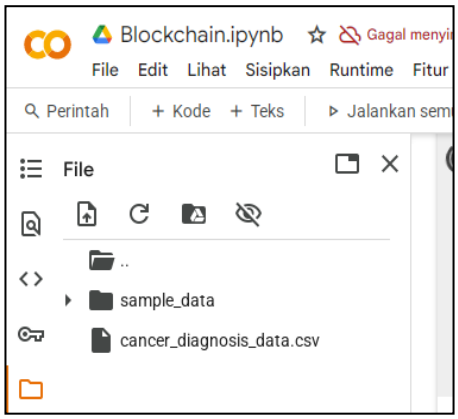


Figure 3. Data Input Results

3.2 Results of Blockchain Technology Implementation Simulation

The simulation was carried out by integrating electronic health record (EHR) data into a simple Blockchain system using Google Colab. The main objective of this implementation is to evaluate the ability of Blockchain to maintain the authenticity, integrity, and security of medical data. The results of the Blockchain technology implementation in securing health records are shown in Figure 4.

records. Each block in the chain contains a set of data—in this case, patient information such as Patient_ID, Age, Gender, and Tumor_Size—along with a cryptographic hash of the previous block, and its own current hash value. For example, Block 0 starts the chain with an initial hash, while Block 1 references the hash of Block 0 through its Prev Hash field. This chaining mechanism creates a continuous and tamper-evident ledger, where any modification to the data in a previous block would change its hash and break the link to all subsequent blocks, making tampering easily detectable.

This structure ensures the integrity and authenticity of Electronic Health Records (EHR), safeguarding sensitive medical data from unauthorized alterations or deletions. The presence of the patient's digital signature or cryptographic verification process embedded in each block further strengthens trust in the data's validity.

Moreover, the decentralized nature of blockchain means that this ledger is distributed across numerous nodes rather than centralized in one location, providing redundancy and fault tolerance. This distribution protects against data loss from hardware failures or cyberattacks targeting a single server. Additionally, permissioned blockchain frameworks can restrict access, so only authorized healthcare providers and patients can interact with the

```
Blok ke-0
    Data          : {"Patient_ID":"c044501a-43ca-4a0c-8b8b-991439ba1b6a","Age":52,"Gender":"Female","Tumor_Size(cm)":5.0..
    Prev Hash     : 0
    Current Hash  : a4df3226865a46e0c1ea6dba49c8b32bde0f7287b87bf5be267c959632031c1f

Blok ke-1
    Data          : {"Patient_ID":"b8900c4c-1232-4084-9432-5d02eba74d20","Age":32,"Gender":"Female","Tumor_Size(cm)":0.8..
    Prev Hash     : a4df3226865a46e0c1ea6dba49c8b32bde0f7287b87bf5be267c959632031c1f
    Current Hash  : dab0e6f661da923eada625eebf8636ed928cffadc821989f7fe1bedc7f899f14

Blok ke-2
    Data          : {"Patient_ID":"3004e2bc-8037-49cb-a542-d5612b73beab","Age":70,"Gender":"Female","Tumor_Size(cm)":9.5..
    Prev Hash     : dab0e6f661da923eada625eebf8636ed928cffadc821989f7fe1bedc7f899f14
    Current Hash  : 38b75eb9f35557f38b3494eae7b800a576e2c09ec061d3695c651d3fd0c1f6b9

Blok ke-3
    Data          : {"Patient_ID":"1df86af7-6745-4dea-b127-cbc9915079fc","Age":21,"Gender":"Female","Tumor_Size(cm)":3.0..
    Prev Hash     : 38b75eb9f35557f38b3494eae7b800a576e2c09ec061d3695c651d3fd0c1f6b9
    Current Hash  : a0182139e22ccebe539afb9f9c6c5b7d78cb8cfc99a35d95b02b907ad4030ebf
```

Figure 3. Results of Blockchain Technology Implementation Simulation

As shown in Figure 4, blockchain technology is used to securely and transparently store medical records, maintaining privacy and complying with data protection regulations.

By combining cryptographic hashing, decentralized storage, and strict access control, blockchain offers a robust solution to many of the security and privacy challenges facing modern EHR systems. This model not only secures data but also promotes transparency and patient empowerment by providing immutable audit trails for every modification or access to their health records. If any changes occur in the medical records, the hash value will change, as demonstrated in Figure 5.

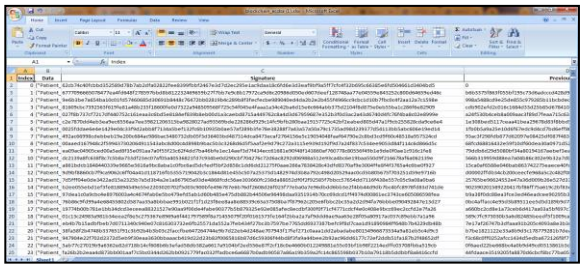


Figure 6. Results of ECDSA Algorithm Implementation in Blockchain-Based Digital Signature

Figure 5. Results of Health Record Manipulation Simulation

Based on Figure 5, it can be seen that the blockchain structure becomes inconsistent after manipulation is carried out on block 1. Initially, each block in the Blockchain is interconnected through hash values, where each block stores the hash of the previous block as the *prev hash*. However, after the data in block 1 was manipulated, the hash value of that block changed, making it inconsistent with the *prev hash* recorded in block 2. This inconsistency breaks the integrity of the chain and indicates that unauthorized data modification has occurred. Thus, Blockchain is capable of automatically detecting data manipulation, since even the slightest change will alter the hash and break the authenticity chain of the subsequent data

3.3 Results of ECDSA and EdDSA Algorithm Implementation

The implementation results of the ECDSA and EdDSA algorithms are presented in the form of an Excel file as a documentation medium. Each entry in the file represents one block in the Blockchain containing electronic health record data along with the results of the cryptographic process. This Excel file includes important information such as the original EHR data, block hash values, the generated digital signatures (from both the ECDSA and EdDSA algorithms), as well as the public keys used in the verification process. Figure 5 below shows the implementation results of the ECDSA algorithm in generating Blockchain-based digital signatures.

Next, Figure 7 shows the implementation results of the EdDSA algorithm in generating Blockchain-based digital signatures.

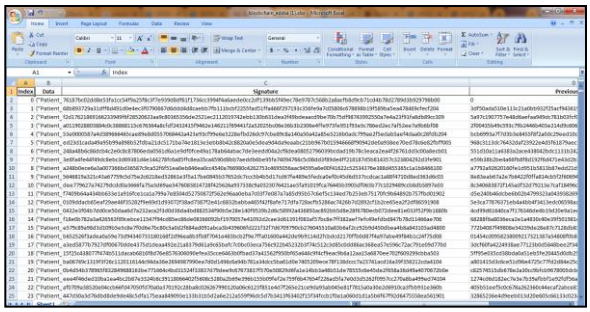


Figure 7. Results of EdDSA Algorithm Implementation in Blockchain-Based Digital Signatures

These implementation results serve as a comparative reference to evaluate the performance and output of the ECDSA and EdDSA algorithms within a blockchain-based digital signature system. By documenting the data in a structured Excel format, researchers and developers can easily analyze the differences in signature length, processing time, and security properties between the two algorithms. This documentation also supports traceability and reproducibility in future cryptographic studies, especially in the context of securing electronic health records (EHR) using blockchain technology

3.4 Results of Testing and Evaluation

To demonstrate the security level of Blockchain, testing was also carried out on the Proof-of-Work (PoW) mechanism, which is a consensus method that requires each new block to undergo a complex computational process to find a nonce value that produces a hash in accordance with a certain difficulty level. Thus, this PoW testing reinforces the evidence that Blockchain provides a high level of security and is highly reliable in maintaining the integrity and validity of data, especially in sensitive systems such as Electronic Health Records (EHR). Table 3 shows the results of Blockchain security testing in safeguarding health records.

Next, testing and evaluation were carried out to compare the ECDSA and EdDSA algorithms in securing health records using Blockchain-based digital signatures. The results of the testing and evaluation are presented in Table 2 below.

Table 2. Results of Testing and Evaluation of ECDSA and EdDSA Algorithms

Evaluation Aspect	Method	ECDSA	EdDSA
Security (Signature & k Reuse	Signature Length	64 byte	64 byte
	Reuse k	Different Reuse (Secure)	Not applicable (deterministic, secure)
	Conclusion	Secure if k is unique, vulnerable if not	More secure from k reuse threats
Efficiency (Performance)	Signing Time	0.000962 detik	0.000180 detik
	Verification Time	0.003204 detik	0.000200 detik
	Conclusion	Slower	More efficient and faster
Effectiveness (Validation & Integrity)	Authentic Validation	True	True
	Data Change Detection	False	False
	Conclusion	Validation successful, integrity not yet optimal	Same, integrity not yet optima

Based on Table 2, the test results show that both ECDSA and EdDSA produce a digital signature length of 64 bytes. In terms of security regarding k reuse, ECDSA uses different k values, making it secure, but it is still potentially vulnerable if k is not unique. Meanwhile, EdDSA does not use random k but instead applies a deterministic approach, thereby eliminating the risk of k reuse and making it more secure. From the efficiency perspective, ECDSA requires 0.000962 seconds for the signing process and 0.003204 seconds for verification. In contrast, EdDSA requires shorter times, 0.000180 seconds for signing and 0.000200 seconds for verification, demonstrating faster performance. In terms of effectiveness, both algorithms can validate data correctly (authentic validation = true), but cannot detect data modifications (change detection = false). This indicates that although signature validation is successful, the mechanism for detecting data integrity is not yet fully optimal.

Table 3. Results of Blockchain Technology Security Testing and Evaluation

Number of Blocks	Mining Time (Seconds)				
	DT=1	**DT=2**	**DT=3**	**DT=4**	**DT=5**
4,000	3.96	7.67	62.76	962.39	1,504.51
8,000	7.92	15.34	125.52	1,924.78	3,081.02
12,000	11.88	23.01	188.28	2,887.17	4,621.53
16,000	15.84	30.68	251.04	3,850.56	6,162.04
20,000	19.80	38.35	313.80	4,813.95	7,702.55

Based on Table 3, it can be seen that mining time increases significantly as the number of blocks and the difficulty target (DT) rise. This indicates that the Proof-of-Work (PoW) algorithm functions as intended, by creating a high computational barrier for adding new blocks.

For example, at DT=5 with 4,000 blocks, the mining process takes approximately 1,504 seconds (25 minutes), and increases to more than 7,700 seconds (2 hours) when the number of blocks reaches 20,000. In addition, raising the DT from 1 to 5 at the same number of blocks also results in a significant surge in time, such as from 4 seconds to 1,500 seconds for 4,000 blocks.

This very long duration shows that manipulating data in Blockchain would require enormous resources and time, making it nearly impossible to execute without detection. This reinforces the strength of PoW in maintaining data integrity and security, especially in sensitive systems such as Electronic Health Records (EHR), where authenticity and traceability of data are crucial.

3.5 Discussion

The main problem underlying this research is the growing demand for a secure, tamper-resistant, and integrity-preserving electronic health record (EHR) storage system. EHRs are highly sensitive data that are vulnerable to leakage and unauthorized modifications. Therefore, a technology-based solution is needed to ensure security, integrity, and efficiency in data management. Blockchain, with its consensus mechanism, combined with digital signature algorithms, was chosen as an approach to address this issue [16].

The testing and evaluation results indicate that the integration of Blockchain technology with digital signature algorithms such as ECDSA and EdDSA can provide strong security guarantees for electronic health records (EHR). One of the key elements in ensuring data security within this system lies in the Proof-of-Work (PoW) consensus mechanism, which imposes significant computational barriers to adding new blocks to the Blockchain [17]. The substantial increase in mining time proportional to both the number of blocks and the difficulty target demonstrates that tampering with historical data would be extremely difficult, as it requires intensive and time-consuming recomputation [18].

For illustration, the mining process for 20,000 blocks with the highest difficulty level (DT=5) required more than two hours. This increase is exponential with respect to both the number of blocks and difficulty, indirectly proving the effectiveness of PoW in maintaining data integrity and authenticity. In other words, the larger and more complex the network, the more difficult it becomes for unauthorized parties to manipulate data, making it highly suitable for sensitive data such as EHRs, which require strong integrity and reliability.

In addition, testing of two digital signature algorithms—ECDSA and EdDSA—revealed significant differences in terms of efficiency and security. Although both produce signatures of the same size (64 bytes) and successfully validate data, EdDSA outperformed ECDSA in signing and verification speed. This makes EdDSA more efficient for high-volume and rapid transaction scenarios, such as Blockchain-based EHR systems that require instant data communication responses [19].

From a security standpoint, EdDSA offers an additional advantage because it uses a deterministic approach in generating signatures, eliminating the risk of random nonce (k) reuse that could expose private keys, as is possible with ECDSA. Although in this test ECDSA's k values were unique and secure, the vulnerability remains an issue if the implementation is careless or the device environment is compromised. Therefore, in systems requiring very high levels of security, EdDSA is considered more resilient against reuse-based attacks.

However, the results for data integrity effectiveness indicate that both algorithms were unable to detect altered data (change detection = false). This suggests that while signature validation was successful, the integrity mechanism is not yet optimal for providing comprehensive protection against manipulated data. This limitation opens opportunities for further development, such as combining digital signatures with hash chaining or employing additional cryptographic algorithms to ensure real-time change detection.

Overall, the combination of Blockchain technology with digital signature algorithms, particularly EdDSA, demonstrates strong potential in securing EHRs. Nevertheless, certain aspects, such as data integrity validation, still require enhancement for the system to be fully reliable and aligned with healthcare data confidentiality and security standards.

Between the two algorithms, EdDSA can be considered superior to ECDSA in terms of time efficiency and cryptographic security. EdDSA is faster, more secure against k reuse attacks, and better suited for modern implementations that demand high performance and maximum protection for sensitive data. Still, the integrity validation aspect needs improvement to ensure the system is fully robust

These findings are consistent with previous studies, which reported that PoW provides strong protection against data manipulation, albeit with weaknesses in energy efficiency [7]. The finding that EdDSA is more efficient than ECDSA is also in line with the work of Mendrofa et al. (2024), which demonstrated that EdDSA achieves higher speed and stronger security than ECDSA in modern implementations [20]. Thus, this research strengthens the evidence that Blockchain, supported by advanced digital signature algorithms, can serve as an effective solution for health data security.

Nonetheless, this study remains limited to testing in a simulated environment with a defined number of blocks and difficulty levels. It does not cover real network conditions with distributed nodes or more complex attack scenarios. Moreover, the data integrity mechanism relied solely on digital signatures without incorporating additional security features such as full hash chaining or multi-signature verification

From a practical perspective, the results of this study can serve as a foundation for developing more secure Blockchain-based EHR systems, particularly in selecting appropriate digital signature algorithms. From an academic perspective, this study enriches the discourse on Blockchain technology integration in healthcare. From a policy perspective, the results can provide valuable input for regulators in formulating health data security standards that accommodate modern cryptographic technologies

For future research, it is recommended to conduct testing in larger and more realistic Blockchain networks, involving distributed nodes and diverse attack scenarios. Furthermore, integrating digital signatures with hash chaining, Merkle Trees, or alternative consensus mechanisms such as Proof-of-Stake (PoS) could be explored to improve data change detection. Developing hybrid methods that combine EdDSA's efficiency with additional verification mechanisms also presents opportunities for creating a more robust Blockchain-based EHR system.

4. CONCLUSION

Based on the test results, EdDSA outperforms ECDSA in terms of security due to its deterministic nature and immunity from the risk of *k* reuse, as well

as its higher efficiency, requiring only 0.000180 seconds for signing and 0.000200 seconds for verification, compared to ECDSA which requires 0.000962 seconds and 0.003204 seconds, respectively. Both algorithms successfully validated the data, but neither was able to detect data modifications. Meanwhile, the Proof-of-Work (PoW) mechanism in Blockchain proved to be highly secure, as evidenced by the significant increase in mining time with the growing number of blocks and difficulty level, from 1,504 seconds (4,000 blocks, DT=5) to 7,702 seconds (20,000 blocks, DT=5). This creates a substantial computational barrier, making data manipulation extremely difficult.

5. REFERENCES

[1] V. Mandari$no, G. Pappalardo, and E$. Tramontana, "A Blockchai$n-Base$d Electroni$c He$alth Re$cord (E$HR) Syste$m for E$dge$ Computi$ng E$nhanci$ng Se$curi$ty and Cost E$fficie$ncy," *Compute$rs*, vol. 13, no. 6, pp. 1–26, 2024, doi$: 10.3390/compute$rs13060132.

[2] Andi$, C. Juli$andy, R. Robe$t, O. Pri$badi$, and R. Wi$jaya, "I$mage$ Authenticati$on Appli$cati$on wi$th Blockchai$n to Pre$ve$nt and De$te$ct I$mage$ Plagiarism," *2021 6th I$nt. Conf. I$nformati$cs Comput. I$CI$C 2021*, no. De$cember, 2021, doi$: 10.1109/I$CI$C54025.2021.9632966.

[3] A. Ali$ *e$t al.*, "Se$curity, privacy, and reliability i$n di$gi$tal he$althcare$ syste$ms usi$ng blockchai$n," *E$le$ctron.*, vol. 10, no. 16, pp. 1–27, 2021, doi$: 10.3390/e$le$ctroni$cs10162034.

[4] N. U. A. Tahi$r *e$t al.*, "Blockchai$n-Base$d He$althcare$ Re$cords Manage$me$nt Frame$work: E$nhanci$ng Se$curi$ty, Pri$vacy, and I$nte$rope$rability," *Te$chnologi$e$s*, vol. 12, no. 9, pp. 1–19, 2024, [Online]. Avai$lable$: https://doi$.org/10.3390/te$chnologi$e$s12090168.

[5] M. A. Al-Khasawne$h, M. Fahe$e$m, A. A. Alarood, S. Habi$bullah, and A. Alzahrani$, "A se$cure$ blockchai$n frame$work for he$althcare$ re$cords manage$me$nt syste$ms," *He$althc. Te$chnol. Le$tt.*, vol. 11, no. 6, pp. 461–470, 2024, doi$: 10.1049/htl2.12092.

[6] I$. Lyge$rou, S. Srinivasa, E$. Vasi$lomanolaki$s, G. Ste$rgi$opoulos, and D. Gri$tzali$s, "Corre$cti$on to: A de$ce$ntrali$ze$d hone$ypot for I$oT Protocols base$d on Androi$d de$vices," *I$nt. J. I$nf. Se$cur.*, vol. 22, no. 1, p. 303, 2023, doi$: 10.1007/s10207-022-00628-0.

[7] Andi$, C. Juli$andy, Robe$t, and O. Pri$badi$, "Se$curi$ng Me$di$cal Re$cords of COVI$D-19 Pati$e$nts Usi$ng Ellipti$c Curve$ Digital Si$gnature$ Algori$thm (E$CDSA) i$n Blockchai$n," *CommI$T J.*, vol. 16, no. 1, pp. 87–96, 2022, doi$: 10.21512/COMMI$T.V16I$1.7958.

[8] A. Nadzi$fari$n and A. Asmuni$n, "Pe$ne$rapan E$lliptic Curve$ Digital Si$gnature$ Algori$thm pada Tanda Tangan Di$gi$tal de$ngan Studi$ Kasus Dokume$n Surat – Me$nyurat," *J. I$nformati$cs Comput. Sci$.*, vol. 4, no. 01, pp. 1–9, 2022, doi$: 10.26740/ji$nacs.v4n01.p1-9.

[9] H. A. F. Kurni$awan, S. N. Ne$yman, and S. H. Wi$jaya, "Pe$nge$mbangan Algori$tma E$cdsa De$ngan Modifikasi$ Pe$rkali$an Skalar Me$nggunakan Double$ Base$ Chai$n," *J. Te$knol. I$nf. dan I$lmu Komput.*, vol. 11, no. 2, pp. 275–284, 2024, doi$: 10.25126/jti$i$k.20241127446.

[10] M. E$lshe$i$kh, İ. K. Paksoy, and M. Ce$nk, "Acce$le$rati$ng E$dDSA Si$gnature$ Verifi$cati$on wi$th Faste$r Scalar Size Halvi$ng," *I$ACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2025, no. 3, pp. 493–515, 2025, doi$: 10.46586/tche$s.v2025.i$3.493-515.

[11] G. J and S. Koppu, "An Empiri$cal Study to De$monstrate$ that E$dDSA can be$ use$d as a Pe$rformance$ I$mprove$me$nt Alte$rnative to E$CDSA i$n Blockchai$n and I$oT," *I$nform.*, vol. 46, no. 2, pp. 277–290, 2022, doi$: 10.31449/i$nf.v46i$2.3807.

[12] H. Ghodang and Hantono, *Me$tode$ Penelitian Kuanti$tati$f Konse$p Dasar & Apli$kasi$ Analisis Regresi$ De$ngan Jalur SPSS*. Me$dan: PT. Penerbi$t Mi$tra Grup, 2020.

[13] B. H. Purnomo, D. A. Ri$smayadi$, M. R. F. Thori$q, U. Pamulang, and U. T. Bandung, "Adopsi$ Blockchai$n se$bagai$ Solusi$ Ke$amanan dan Transparansi$ Transaksi$ Digital di$ I$ndustri$ Fintech," *J. Mi$nfo Polgan*, vol. 13, no. 2, pp. 2486–2492, 2025.

[14] F. N. Nuraini, "Pe$ran Te$knologi$ Blockchai$n Dalam Me$ni$ngkatkan Transparansi$ Akuntansi$," *Profi$t J. Manajemen, Bisnis dan Akunt.*, vol. 4, no. 2, pp. 303–312, 2024, [Online]. Avai$lable$: https://course$work.uma.ac.i$d/index.php/e$konomi$/article/vi$e$w/458.

[15] R. P. Purba, B. A. Wi$jaya, L. W. Nazara, and S. S. Utami$, "De$sai$n Protokol Ke$amanan Data Be$rbasi$s Blockchai$n pada Pe$ngolahan Data Pe$ngguna Apli$kasi$ E$-comme$rce$," *Me$tri$k*, vol. 9, no. 2, pp. 256–263, 2025, doi$: 10.47002/me$ti$k.v9i$2.1104.

[16] J. Huang, Y. W. Qi$, M. R. Asghar, A. Me$ads, and Y. C. Tu, "Me$dBloc: A blockchai$n-base$d se$cure$ E$HR syste$m for shari$ng and acce$ssi$ng me$di$cal data," *Proc. - 2019 18th IEEE I$nt. Conf. Trust. Se$cur. Pri$v. Comput. Commun. I$EEE$ I$nt. Conf. Bi$g Data Sci$. E$ng. Trust. 2019*, pp. 594–601, 2019,

doi$: 10.1109/TrustCom/Bi$gDataSE$.2019.00085.

[17] Andi$, R. Purba, and R. Yuni$s, "Appli$cati$on of Blockchai$n Te$chnology to Prevent The$ Potential Of Plagiarism i$n Sci$entifi$c Publi$cati$on," 2019, doi$: 10.1109/ICIC47613.2019.8985920.

[18] J. Vi$nothkumar and K. Ve$nkatachalapathy, "Protection of Medical Re$cords Usi$ng Block Chai$n Te$chnology," vol. 9, no. 4, 2021.

[19] S. Lyu, "Advance$s i$n Digital Si$gnature$ Algori$thms: Pe$rformance$, Se$curi$ty and Future$ Prospe$cts," i$n *I$TM We$b of Conference$s (I$WADI$)*, 2024, vol. 73, pp. 1–7.

[20] S. A. Me$ndrofa, M. W. Ardyani$, S. S. Cari$ta, and Se$pha Si$swantyo, "Unlocki$ng the$ Future$ of Digital Curre$ncy: A Comparati$ve$ Study of E$CDSA vs. E$dDSA Si$gnature$s wi$th Obli$vi$ous Transfe$r Protocol," 2024.