ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
Received: 18 July 2025; Accepted: 21 September 2025

https://doi.org/10.17559/TV-20250718002843
Original scientific paper

Session Dependent Zero Knowledge Proof Technique for Enhanced Privacy Verification in Cloud-Based Electronic Health Records

B. ARULMOZHI*, J. I. SHEEBA, S. PRADEEP DEVANEYAN

Abstract: Electronic Healthcare Records (EHRs) provide distributed access to patient and doctor information through pervasive cloud-based storage. As this data is highly sensitive, robust privacy measures are essential to mitigate adversarial impacts. To ensure optimal privacy across multiple shared EHRs, this article proposes a Session-dependent Zero Knowledge Proof Technique (SZKPT). The framework identifies privacy breaches using two truth values: the first representing optimal session closure, and the second reflecting verification at each sharing instance. Both truth values are validated through iterated session validations, which are managed using a deep learning paradigm. During training, different combinations of truth values are employed to maximize privacy during data sharing, while iterative processes train consecutive validation instances to improve breach detection. Truth values are continuously updated to reflect the session closure and the most recent privacy verification. In practice, if either truth value equals zero, the session is suspended; otherwise, if truth values are valid in consecutive iterations, data sharing is delegated to the authorized user. The process is repeatted at regular intervals with updated truth values, ensuring continuous monitoring and adaptive privacy protection. The proposed technique is rigorously evaluated using key performance metrics, including access verification, computational complexity, privacy breach detection, verification time, and access delegation time. Results demonstrate that SZKPT effectively balances privacy preservation with usability, providing a reliable, scalable, and efficient solution for secure EHR management in cloud-based healthcare systems.

Keywords: cloud computing security; deep learning verification; electronic health records (EHR); privacy preservation; zero knowledge proof (ZKP)

1 INTRODUCTION

Electronic health records (EHR) provide necessary details such as health condition, pulse rate, and diagnosis information of the patients. EHR is mostly stored using a cloud system that reduces the latency in identification and verification processes [1]. EHR is mainly used to increase the overall accuracy of disease detection and diagnosis processes. Sharing privacy details is an important task to perform in every healthcare application [2]. Privacy-preserving schemes are used to secure the data from third-party members. A federated learning (FL) based privacy-preserving scheme is used for the EHR data-sharing process. The FL algorithm evaluates the clinical information which provides feasible data for the identification process. The FL-based scheme increases the security and privacy in data sharing. The FL-based scheme enhances the accuracy level in the disease diagnosis process [3, 4]. A blockchain (BC) based privacy-preserving technique is also used to preserve information during the exchange. The BC technology uses an encryption strategy to encrypt the transaction data for the users. The BC technology improves both the privacy and security level of medical data in healthcare applications [5, 6].

Authentication is a crucial task to perform which secures the privacy range of the process. Authentication-based privacy methods are used for EHR data in cloud systems. Various methods and techniques are used for the authentication process in healthcare systems [7]. A blockchain (BC) based aggregation method is used for authentication. The actual goal of the method is to reduce the attacks and threats during the authentication process [8]. The BC-based method verifies the unique properties such as keys and passwords for the authentication process. The BC-based method identifies the session keys for authentication which minimizes the complexity of sharing data for the process [9]. An efficient mutual authentication and privacy-preserving scheme for EHR records in cloud systems is common in such fields. The mutual authentication scheme is mainly used to secure the privacy and communication services of patient's information. The mutual authentication protocol monitors the healthcare condition of the patients. The authentication protocol also detects the anomalies and defects that cause damage to the systems [10, 11].

Machine learning (ML) algorithms are used for the prediction and detection process. The ML is mainly used to increase the accuracy of data sharing process. ML algorithms are also used in data sharing for healthcare applications [12]. A privacy-preserving federated learning (FL) scheme based on homomorphic encryption is used for the healthcare validation process. The main aim of the scheme is to evaluate the healthcare data which contains necessary information for the sharing process [13, 14]. The FL-based is used to encrypt the data and produce feasible data for the authentication process. An access control (AC) technology is also used in the scheme to eliminate unwanted problems for the systems [15]. The FL algorithm also reduces the latency and energy consumption ratio in the computation process. A feature extraction-based validation method is used to ensure privacy privacy-sharing process. The feature extraction method extracts the important features and patterns that are relevant data for data sharing. It is commonly used for data classification process that minimizes the latency in the validation process. The feature extraction-based method improves the quality of service (QoS) range in the healthcare data-sharing process [14, 16].

2 RELATED WORKS

A hybrid blockchain-edge model for electronic health records (EHR) management systems was developed using attribute-based signature aggregation (ABSA) to measure system execution time. Blockchain technology is utilized to verify functions containing necessary data for the management process, increasing the robustness and feasibility of the system [17]. A privacy-preserving scheme for EHR in a hybrid cloud was proposed to verify features

producing relevant information for the verification process. This control model identifies both internal and external details, reducing task failure rates and enhancing the privacy and security of health records [18].

A new exchange method using a trust-based blockchain network for EHR was introduced to address challenges in data exchange. It secures patient health data and transmission among individuals, increasing the accuracy and security of the system [19]. A leveled homomorphic encryption (LHE) based privacy-preserving scheme for EHR data was proposed to identify sharing list details. The scheme addresses risks and issues during EHR data sharing and produces relevant solutions for management problems [20]. A blockchain-based EHR automation system for healthcare applications was designed to provide detailed health records. The system exchanges data between healthcare centers and patients while reducing latency and computational cost [21]. A patient-controlled blockchain-enabled EHR for Healthcare 4.0 was introduced, offering optimal information for disease identification. It aids doctors in health condition prediction, reducing latency and improving data exchange accuracy [22].

A cloud system-based secure EHR transaction system was proposed using blockchain and key-based access control to protect patient data. Cloud servers evaluate unique EHR properties, improving system performance and application significance [23]. A blockchain-based data exchange technique was developed for healthcare applications to secure health information. It protects both private and public user data from third parties, enhancing mobility and flexibility in healthcare applications [24].

A new EHR security method using blockchain for IoT-enabled healthcare was introduced. It analyzes patient-centric and medical-centric data to improve the quality of medical records, boosting system performance [25]. A blockchain-based confidentiality and privacy-preserving big data scheme was proposed for cloud-enabled healthcare. Digital signature frameworks are used to evaluate medical data patterns, reduce computational complexity, and improve data transmission accuracy [26].

A privacy-aware decentralized self-management model (DSMAC) based on blockchain was developed for EHR data. It addresses process-damaging issues and reduces identification latency, improving system sustainability and scalability. A privacy-preserving electronic medical record (EMR) exchange method was introduced for healthcare centers. It uses anonymous transactions and local differential privacy (LDP) strategies to protect healthcare information, enhancing data exchange accuracy [27].

A privacy-preserving control scheme using blockchain for e-health applications was introduced. It provides secure diagnosis and is used for sensitive medical data, enhancing overall application security . A blockchain-based privacy-preserving architecture was proposed for IoT-enabled applications. It evaluates transparency between patient and medical data, and analyzes access control levels to improve system efficiency and feasibility [28].

3 PROPOSED METHOD

This proposed technique is used for privacy-preserving health records of the patients through iterated session validations for breach detection and sharing access delegation in the current session. The privacy breach occurrence is detected using two truth values. There are optimal session closures and verification per sharing instances. Therefore, this validation is performed and avoids the adversary impacts for securing sensitive data. The individual and multiple EHRs are stored and updated consecutively to improve smart healthcare systems through deep learning. If a breach occurs in any particular patient data is identified to ensure privacy for the sharing of EHRs in the current session, then the truth values are constructed to indicate breach occurrence for generating new electronic health records. In particular, the truth values are constructed; if the privacy and sharing increases, then the truth value is 1 otherwise the truth value is 0. If any breach occurrence is identified in the current session, the truth value for both privacy and sharing is 0. In this condition, a new session is created to secure the data. Both truths are validated through iterated session validations using deep recurrent learning. On the other hand, the session-dependent zero-knowledge proof (SZKPT) technique is used to ensure that one party proves to another party that they know a secret message without revealing any data other than possession of the privacy. As this process output, SZKPT can be applied as a model to secure the privacy of users during the session verification process. The complete process of SZKPT is depicted in Fig. 1.

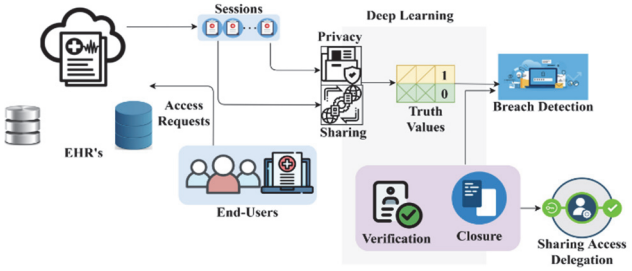

Figure 1 Process of SZKPT depiction

This SZKPT avoids adversary impacts in any system. In cryptography, an SZKPT is a method; the end-users can convince sessions such that they know secret data D of other users, without sharing any data. In this technique, the end-user only knows the secret data D. Based on the access requests between the end-users and sessions, there are two truth values constructed: first is the optimal session closure and second is the verification per sharing instances. This validation is pursued using deep learning. A SZKPT must satisfy three properties:

• Completeness: If the privacy and sharing are verified in any session output as 1, the privacy is used to ensure data security.

• Soundness: There is no such privacy or sharing in a particular session, if the session does not validate the requests correctly.

• Zero-knowledge: The proof of knowledge can be validated without revealing any sensitive and significant data which means that no privacy and sharing identify other than the fact that the truth value is 1. SZKPT can be

implemented to address privacy issues in the healthcare system. In particular, SZKPT is used to guarantee that sharing in EHRs in any network is valid without revealing any sensitive and significant data about the end users.

The access requests are processed iteratively for the session's verification. Second, the proposed technique identifies the security breaches using truth values. The truth values are updated through deep learning to reduce access delegation time and complexity. Third, deep learning is used to perform the iterative processes for training the sequential validation instances in particular sessions for maximizing breach detection. After the session closure for the last known privacy verification, the truth values are updated. In this privacy verification, if either of the truth values is 0 then that session is suspended. Instead, if the truth values are updated, then that sharing is delegated to the end user. In this proposed technique, the stored EHR security verification is considered to improve privacy breach detection and reduce adversary impacts. However, the consecutive training iteration is performed for the precise sharing of access delegations to the users; the proposed technique verifies the security of health records across shared EHRs. Tab. 1 presented the comparision analysis of Zero-Knowledge proof models in healthcare.

Table 1 Comparison of zero-knowledge proof models in healthcare

Model	Proof Size / Setup	Complexity	Limitations in Healthcare	SZKPT Advantage
zk-SNARK	Small proof size, requires trusted setup	$O(n^2)$	Trusted setup impractical, slower with large EHRs	No trusted setup, faster validation
zk-STARK	Larger proof size, no trusted setup	O(n log n)	High proof generation time, heavy computation	Lightweight O(n), scalable
SZKPT	Truth-value based session validation	O(n)	-	Real-time, privacy-preserving, optimized for EHR access

This comparison highlights that while zk-SNARK and zk-STARK models provide strong cryptographic guarantees, they face scalability and latency issues in healthcare environments. The proposed SZKPT framework overcomes these challenges by offering lightweight computation, faster validation, and practical suitability for real-time Electronic Health Record (EHR) access.

The end user requests in n intervals and $\exists^S$ sessions are arbitrary for two conditions: $P \le R^t$ and $P > R^t$. If the first condition is satisfied then sharing is pursued else the adversary check is performed. Depending on the verification conditions multiple $(P + S)$ cases are validated for improving EHR privacy during $\exists^S$. The failing S is trained using deep learning and its allied truth values across different P sessions (Fig. 2). Therefore, in this first EHR analysis $(P + S)$, the first user is represented as End_{u_a} whereas the sequential users $\left(End_{u_a}+1\right)$ co-exist with distributed EHR of $R^t \in [S + 1, P]$ at regular intervals. If End_{u_a} means the active user. This iterative process improves the healthcare system for both End_{u_a} and $(End_u)_N$. Contrarily, the second case used to identify the adversary impacts in any session relies on $(P + S)$ condition and also verifies if no privacy and sharing is performed in any session for achieving successive patient-doctor access and diagnosis information with security and $\text{argmin} \sum_{\exists^S=1}^{D} \text{Access}_{\text{req}} \forall\left(P+S\right)$ is satisfied. The access and sharing processes are illustrated in Fig. 2.

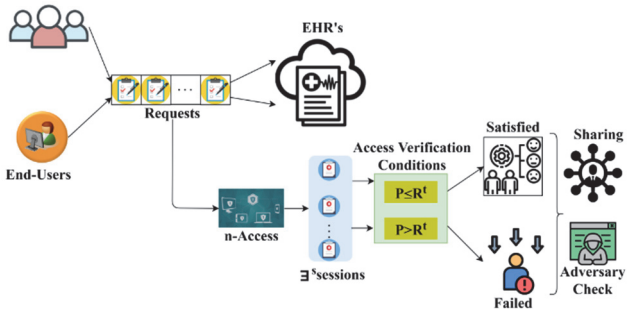

Figure 2 Access and sharing process illustrations

The proposed technique administers both the privacy and sharing of EHR using deep learning. Privacy verification and sharing session closure are the two important considerations that are performed to achieve optimal privacy. In this multiple access requests processing, the iterative processes are also used for training (TR^i) the consecutive/occurring validation instance for increasing privacy breach detection. The truth value 0 identified instances are carried out until breach detection, that session is suspended and then the next sharing session is created. However, the complexity and adversary impact less iterative processes performed in stored EHRs for maximizing sharing access delegation. From the case (i) and (ii), the TR^i is expressed as:

$$TR^i = \max\left\{P_1, P_2, ..., P_n\right\},\ \forall\forall\, End_{u_a} \in \left(End_u\right)_N \tag{1}$$

$$= \left(P+S\right)+\left(P+1-R^t\right),\ \forall\, P \le R^t \le S \tag{2}$$

The training is performed for differentiating the different combination of truth values and individual request access are compared with previous successful sessions for gaining optimal security for EHRs. This training is performed to reduce the access delegation time and verification time. The optimal privacy across various distributed EHRs is done through the condition $R^t \in \left[S+1, P\right] \forall \left(End_u\right)_N$ does not perform training, then the truth values are not updated after the session closure for the last known privacy verification. The truth values update is continuously performed to maximize breach detection at regular intervals. The stored EHR for diagnosis is iteratively processed with some security. The truth value representation, analysis, and verification are portrayed in Fig. 3.

The possible truth table values (for positive and false) are the inputs analyzing the verification. In this verification, the continuous and single $\exists^S$ are validated for

access delegation. The delegation alone updates the truth value by filtering the positive and false inputs. Contrarily, if the verification for S fails, then pending n are reassigned by terminating the previous session. Therefore, the specific R^t is alone updated for new n verification represented in Fig. 3. This learning paradigm helps to improve the authentication for the sharing. In the following, the privacy verification and sharing session closure are analyzed using truth values, and deep learning is discussed.

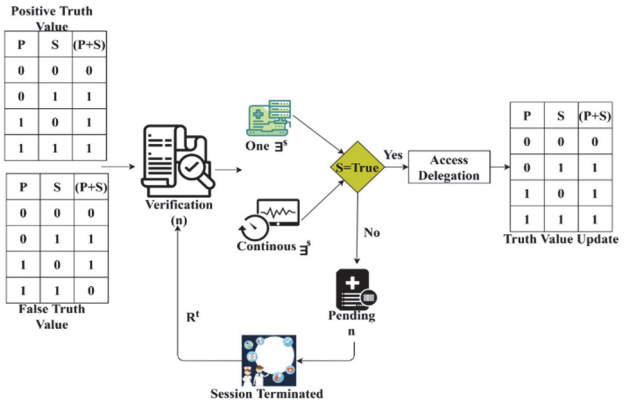

Figure 3 Truth value representation, analysis and verification

Privacy Verification and Sharing Session Closure

In this privacy verification process, the authentication for EHRs in cloud-based storage and breach occurrence is verified using truth values. The first EHR is processed for training the iterative validation; it continuously improves the optimal privacy using the modified zero-knowledge proof. In this Sharing Session Closure analysis repeatedly performs the truth values for maximizing breach detection in all sessions for $P \leq R^t$ and $P \leq R^t \leq S$ for preventing adversary impacts in this storage. In this process, the condition $\phi_v(\text{Access}_{\text{req}}, D + 1)$ used to check the data availability and breaches in the current session and thus perform sharing for further process. However, the sharing session closure is identified at the time of both truth values are 0, hence an update is performed in the next session with current data. The consecutive validation is performed through deep learning and satisfies the condition $P \leq R^t$ for reducing verification time and privacy breaches. The individual EHR is computed for achieving high privacy using the zero-knowledge proof and verifies the sharing instances through truth values until the condition $P \leq R^t$ fails.

The final evaluation of $A\omega_{\text{deleg}_i}$ for the consecutive iteration validation for improving privacy for the available data whereas the sharing access delegation is performed at regular intervals with the truth value updates. If $S + P + 1$ is satisfied by the EHRs. During EHR update data overload is also identified such that the chances of false recommendation are prevented. The session closure process is illustrated in Fig. 4.

The access delegated across various sharing intervals is validated for $\phi_v(S)$ fails the alternative $(S + 1)$ is verified across n and $(n - 1)$ accesses. In these cases the authentication and R^t update is used for training the learning paradigm. The failing verification $\forall \phi_V(S+1)$ is used for impact detection for terminating R^t. This serves as the closure for the n (or) $(n - 1)^{th}$ session preventing new access illustrated in Fig. 4.

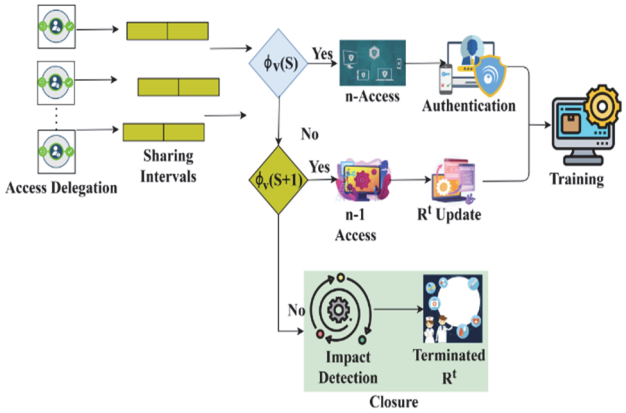

Figure 4 Session closure process

Through deep learning, the above derived two considerations privacy verification and sharing session closure to be repeatedly performed to ensure optimal privacy for EHRs. The continuous sharing access delegation verification with the truth value updates is computed as:

$$A\omega_{\text{deleg}_i} = \left(1 - \frac{\text{Access}_{\text{req}_n}}{P+1}\right) + \left(\frac{\alpha_{d_n}}{\varnothing_{v_i} - TR^i}\right) \tag{3}$$

And,

$$\varnothing_v\left(\text{Access}_{\text{req}}, S\right) = \left(1 - \frac{\exists^s}{\text{P}}\right) + \left(\frac{S+1-\alpha_d}{R^t+1}\right) \tag{4}$$

Instead,

$$\varnothing_v\left(\text{Access}_{\text{req}}, S+1\right) = \left(1 - \frac{\exists^s}{\text{S}}\right) + \left(\frac{P+1}{A\omega_{\text{deleg}_i}+1}\right) \tag{5}$$

The above equations verify the sharing access delegation based on privacy verification and sharing session closure in both the truths, respectively. In this continuous validation is performed using sensitive data and requests access in the cloud platform for maximizing breach detection. In this manuscript, the RSA algorithm is used to secure the EHR information with a session-dependent zero-knowledge proof technique. The RSA algorithm is an asymmetric cryptographic algorithm used to encrypt and decrypt health data continuously and the iterative processes are trained until achieving maximizing breach detection. RSA algorithm is described as:

- Generate Keys for securing health data
- Let's take the random variables I, J and create $\Delta = I + J$
- Assume the integer E for binary variable representation with $(I - 1) \times (J - 1)$
- Output of the variable F by the equation $F \times E = 1(\text{mod}((I - 1) \times (J - 1)))$

- In this algorithm (E, n) denotes public key and (F, n) denotes private key for encryption and decryption of EHRs.
- $h = g^E \bmod n$, $g = h^F \bmod n$. Where g means random integer and h represents cipher text.

This RSA algorithm is used to ensure privacy for the sharing of multiple EHRs at the same time. The iterative process is performed at regular intervals with the truth value updates. These two considerations rely on TR^i and privacy verification for reducing adversary impacts. The deep learning used for validating both truths using iterated session validations is performed and then sharing session closure is identified from the instance. The above-mentioned cases (i) and (ii) are continuously performed to achieve maximum breach detection using session-dependent zero-knowledge proof and deep recurrent learning. The authentication process is illustrated in Fig. 5.

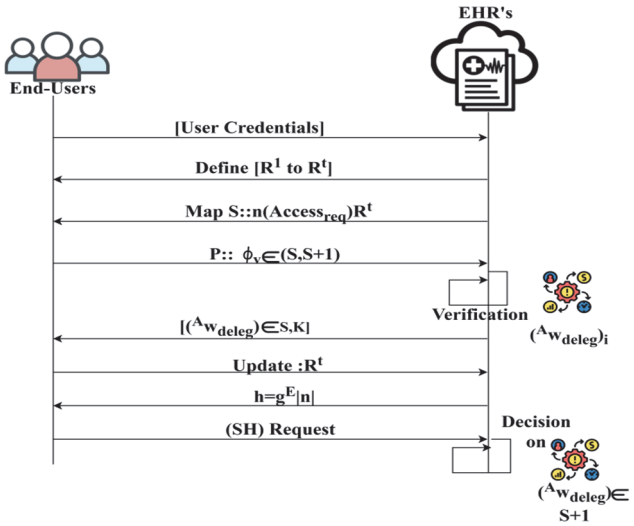

Figure 5 Authentication process for privacy preserving

The SZKPT framework minimizes false positives and false negatives through deep learning, truth-value, based iterative session validation, and adaptive feature analysis. False positives are reduced by analyzing historical access patterns and contextual session data, differentiating legitimate activity from suspicious behavior, while adaptive thresholds fine-tune anomaly detection sensitivity. False negatives are mitigated by hierarchical feature extraction capturing subtle unauthorized access patterns, multi-session correlation to detect dispersed anomalies, and continuous retraining on updated logs to learn new adversarial behaviors. Evaluation using precision, recall, and F1-score ensures a balanced trade-off between security and usability, maintaining accurate breach detection without disrupting legitimate healthcare operations.

4 RESULTS AND DISCUSSIONS

In this section, the comparative analysis of the metrics of breach detection, access delegation time, complexity, verification time, and access verification is presented. The sharing intervals (10 s to 120 s) and the number of EHRs (1000 to 10000) are varied for validating the proposed technique. In this section, a detailed comparative analysis is presented for key performance metrics, including breach detection rate, access delegation time, computational complexity, verification time, and overall access verification accuracy. To validate the robustness and scalability of the proposed SZKPT framework, experiments were conducted by varying two critical parameters: sharing intervals (ranging from 10 seconds to 120 seconds) and the number of Electronic Health Records (EHRs) (from 1000 to 10000). The variation in sharing intervals allows us to measure the system's efficiency under different data exchange frequencies, reflecting both short-term and long-term access scenarios in healthcare environments. Similarly, scaling the number of EHRs enables the evaluation of SZKPT's performance in handling large volumes of sensitive data across multiple access requests.

Results demonstrate that SZKPT consistently achieves higher breach detection rates while maintaining reduced access delegation and verification times compared with baseline methods. The computational complexity remains near-linear with respect to the number of EHRs, ensuring scalability. Moreover, access verification accuracy remains stable even under increased workload, confirming the system's suitability for real-time deployment in clinical settings. The existing BCHealth [30], CP-BDHCA [28], and PP-LHE[20] methods are augmented from the related works section for the comparative analysis.

The deep learning component of SZKPT was trained using 10000 anonymized Electronic Health Records (EHRs) from 1500 patients, containing structured data (demographics, lab tests, vitals, medications) and semi-structured clinical notes. Data preprocessing included normalization of continuous features, one-hot encoding of categorical variables, and handling missing values via imputation. Labels captured diagnosis outcomes and access authorization, including breach detection and verification success. The dataset was split into 70% training, 15% validation, and 15% testing, with stratified sampling to balance legitimate and adversarial cases. SMOTE was applied to augment rare breach instances, ensuring robust model generalization while preserving patient privacy and data security.

In this data privacy improvement using the modified zero-knowledge proof based on access requests analysis from the EHRs is to satisfy high privacy breach detection due to adversary impacts occurrence in cloud-based storage and is represented in Fig. 6. Through distributed patient-doctor access and diagnosis information, the privacy verification and sharing session closure is validated for identifying breach.

In this continuous validation, the access delegation time and verification time are controlled using the proposed technique and deep learning. In each session, the privacy and sharing may vary; the session closure of the last known privacy is verified for regular time intervals. The accurate recommendation and diagnosis are provided using the truth values for P and S. The continuous breach detection in this manuscript leads to reliable access verification. Based on the access verification through SZKPT, the optimal session closure and verification per sharing instances are validated using the truth values for preventing complexity. Therefore, high privacy breach

detection is achieved using modified zero-knowledge proof.

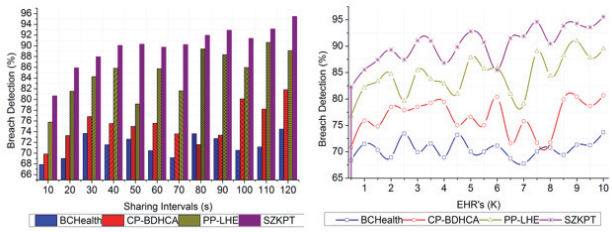

Figure 6 Breach detecion

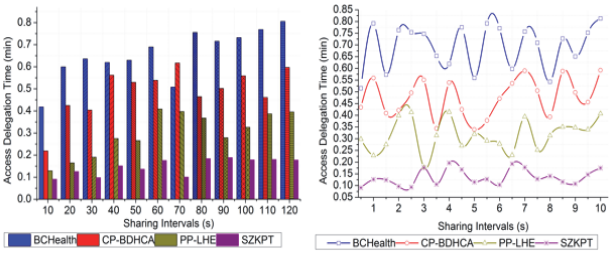

Figure 7 Access delegation time

In this EHR request access from the cloud-based storage is analyzed to provide the best diagnosis recommendations to the patient in the future. The particular end-user accesses any requests from EHRs for privacy and sharing using truths illustrated in Fig. 7. Deep learning is used to achieve less access delegation time for improving data privacy and diagnosis ratio compared to the other factors. In this breach detection, the proposed technique identifies breaches using two truth values for privacy and sharing verification.

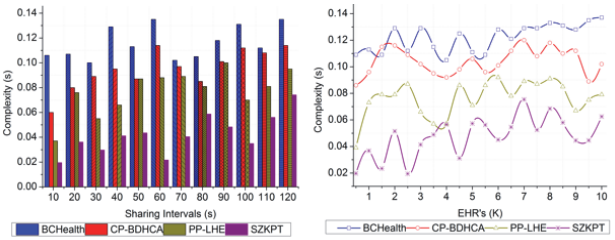

Figure 8 Complexity

This proposed technique for privacy breach detection across shared EHRs is to achieve less complexity and verification time compared to the other factors as illustrated in Fig. 8. The breach detection uses two truth values based on privacy and sharing verification, and the iterative processes are also used for training the consecutive/occurring validation and then reducing breaches using deep learning. The privacy breach occurrence is detected using both truths. Therefore, this validation is performed and avoids the adversary impacts for securing sensitive health data. The current session interaction analysis through the proposed technique is computed for identifying breaches at the time of pervasive cloud-based storage for preventing verification time. If a breach occurs in any particular patient data is identified to ensure privacy for the EHRs in the current session, then the truth values are constructed for generating the next electronic health record.

In this learning process, the different combinations of the truth values are used to secure the sharing through SZKPT and learning using the truth values at various sessions through deep learning. If any breach occurrence is identified in the current session, the truth value for both privacy and sharing is 0, and that session is suspended. In this condition, a new session is created to secure the data. Both truths are validated through iterated session validations using a deep paradigm. Privacy and sharing are verified for improving data security. The breach detection is performed with modified zero-knowledge proof to increase data privacy. From this iterated session validation is performed based on the session closure and privacy verification, preventing breaches. The SZKPT is used to ensure that one party proves to another party, that they know secret data without revealing any message other than possession of the privacy. In this proposed technique, multiple sessions are allocated for improving data privacy, and sharing leads to less verification time as represented in Fig. 9.

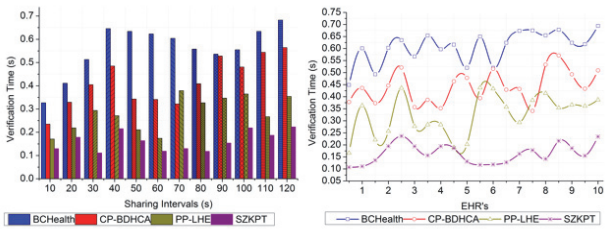

Figure 9 Verification time

This proposed technique achieves high access verification for identifying privacy breach detection and adversary impacts in the different sessions accessing requests from EHRs is performed through deep learning represented in Fig. 10.

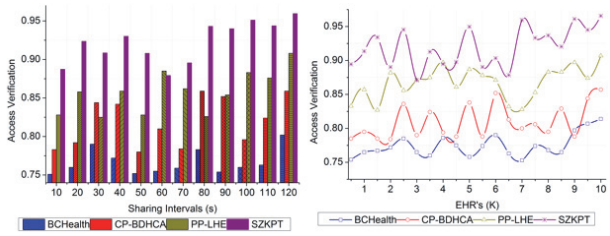

Figure 10 Access verification

In this multiple requests accessing, the iterative processes are also used for training (TR^i) the consecutive/occurring validation instance for improving privacy breach detection and data privacy across various shared EHRs. The truth value 0 is identified in any instances carried out until detecting breaches, that session is suspended and then the next sharing session is created. In this sharing session closure is observed repeatedly using the truth values for maximizing breach detection for $P \leq R^t$ and $P \leq R^t \leq S$, preventing adversary impacts. In this consecutive process, the condition $\phi_v(\text{Access}_{\text{req}}, D + 1)$ used to check the data availability and breaches in the current session and thus pursued sharing for further process. Hence, the sharing session closure is identified at the time both truth values are 0, the truth values are updated and then the next sharing session is created for further process based on breach detection, the less access

verification is achieved. The improvements of the proposed technique are tabulated in Tab. 2 and Tab. 3 for the different sharing intervals and EHRs.

Table 2 Improvements based on Sharing Intervals

Metrics	BCHealth	CP-BDHCA	PP-LHE	SZKPT
Breach Detection / %	74.49	81.84	89.12	95.485
Access Delegation Time / min	0.806	0.597	0.396	0.1777
Complexity / s	0.135	0.114	0.095	0.0741
Verification Time / s	0.683	0.564	0.354	0.2232
Access Verification	0.802	0.859	0.908	0.9595

This proposed SZKPT improves breach detection and access verification by 13.67% and 10.32% respectively. This technique reduces access delegation time, complexity, and verification time by 11.92%, 11.76%, and 9.76% respectively.

Table 3 Improvements based on EHRs

Metrics	BCHealth	CP-BDHCA	PP-LHE	SZKPT
Breach Detection / %	73.66	80.68	89.46	95.597
Access Delegation Time / min	0.813	0.592	0.407	0.1749
Complexity / s	0.137	0.102	0.079	0.0625
Verification Time / s	0.694	0.509	0.387	0.2343
Access Verification	0.814	0.857	0.907	0.9657

This proposed SZKPT improves breach detection and access verification by 14.33% and 10.64% respectively. This technique reduces access delegation time, complexity, and verification time by 11.84%, 13.68%, and 9.29% respectively.

5 CONCLUSION

The proposed SZKPT framework addresses precise diagnosis and secure access management in healthcare by integrating privacy breach detection and access verification within Electronic Health Records (EHRs). Each end-user request triggers an automated session, where patient data is securely stored, analyzed, and used to generate accurate diagnostic recommendations. By combining deep learning with robust access control, SZKPT enhances diagnostic accuracy while safeguarding sensitive information from unauthorized access. Truth-value-based iterative session validation enables continuous monitoring of access requests, minimizing adversary impacts and preventing data theft. Practically, SZKPT offers significant benefits for healthcare providers. It reduces privacy violations, allowing clinical staff to rely on digital records confidently, and facilitates secure data sharing across units, improving care coordination and evidence-based treatment planning. Administrators gain improved regulatory compliance with healthcare data standards and streamlined workflows, as repeated authentication delays and premature session terminations are minimized. Future integration of inverted zero-forcing knowledge-based authentication will further reduce prolonged authentication wait times and mitigate session expiry issues, supporting uninterrupted clinical access and timely decision-making in critical scenarios. SZKPT also demonstrates high breach detection accuracy, real-time access capability, and scalability for 1000-10000 EHRs. Limitations include dependence on dataset quality, moderate hardware requirements, complexity in integrating with existing systems, and slightly lower cryptographic guarantees compared to pure zero-knowledge proof models. Despite these constraints, SZKPT provides a resilient, trustworthy, and efficient solution that prioritizes patient privacy, enhances clinical decision-making, and strengthens the overall healthcare ecosystem. Planned future enhancements will further improve performance, usability, and security for real-world deployment.

6 REFERENCES

[1] Sahi, A., Lai, D., & Li, Y. (2021). A Review of the State of the Art in Privacy and Security in the eHealth Cloud. *IEEE Access*, *9*, 104127-104141. https://doi.org/10.1109/ACCESS.2021.3098708

[2] Cu, O. K., Gajendran, S., Bhavadharini, R. M., Suguna, M., & Krithiga, R. (2023). EHR privacy preservation using federated learning with DQRE-Scnet for healthcare application domains. *Knowledge-Based Systems*, *275*, 110638. https://doi.org/10.1016/j.knosys.2023.110638

[3] Gupta, B. B., Gaurav, A., & Panigrahi, P. K. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, *162*, 113859. https://doi.org/10.1016/j.jbusres.2023.113859

[4] Kiania, K., Jameii, S. M., & Rahmani, A. M. (2023). Blockchain-based privacy and security preserving in electronic health: a systematic review. *Multimedia Tools and Applications*, *82*, 19419-19445. https://doi.org/10.1007/s11042-023-14488-w

[5] Tertulino, R., Antunes, N., & Morais, H. (2023). Privacy in electronic health records: a systematic mapping study. *Journal of Public Health*, *45*(4), 795-814.

[6] Li, C. T., Shih, D. H., Wang, C. C., Chen, C. L., & Lee, C. C. (2020). A blockchain based data aggregation and group authentication scheme for electronic medical system. *IEEE Access*, *8*, 173904-173917. https://doi.org/10.1109/ACCESS.2020.3025898

[7] Tomar, A., Gupta, N., Rani, D., & Tripathi, S. (2023). Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. *Internet of Things*, *23*, 100849. https://doi.org/10.1016/j.iot.2023.100849

[8] Yao, H., Yan, Q., Fu, X., Zhang, Z., & Lan, C. (2022). ECC-based lightweight authentication and access control scheme for IoT E-healthcare. *Soft Computing*, *26*(23), 12727-12747. https://doi.org/10.1007/s00500-021-06512-8

[9] Mohit, P. (2021). An efficient mutual authentication and privacy prevention scheme for e-healthcare monitoring. *Journal of Information Security and Applications*, *63*, 102992. https://doi.org/10.1016/j.jisa.2021.102992

[10] Indushree, M. & Raj, M. (2023). A novel Blockchain-based authentication scheme for telecare medical information system. *The Journal of Supercomputing*, *79*(17), 19245-19273.

[11] Altameem, A., Kovtun, V., Al-Ma'aitah, M., Altameem, T., Fouad, H., & Youssef, A. E. (2022). Patient's data privacy protection in medical healthcare transmission services using back propagation learning. *Computers and Electrical Engineering*, *102*, 108087. https://doi.org/10.1016/j.compeleceng.2022.108087

[12] Shen, G., Fu, Z., Gui, Y., Susilo, W., & Zhang, M. (2023). Efficient and privacy-preserving online diagnosis scheme based on federated learning in e-healthcare system. *Information Sciences*, *645*, 119261. https://doi.org/10.1016/j.ins.2023.119261

[13] Wang, W., Li, X., Qiu, X., Zhang, X., Zhao, J., & Brusic, V. (2023). A privacy preserving framework for federated learning in smart healthcare systems. *Information Processing & Management*, *60*(1), 103167. https://doi.org/10.1016/j.ipm.2022.103167

[14] Qamar, S. (2022). Healthcare data analysis by feature extraction and classification using deep learning with cloud based cyber security. *Computers and Electrical Engineering*, *104*, 108406. https://doi.org/10.1016/j.compeleceng.2022.108406

[15] Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems*, *144*, 271-290. https://doi.org/10.1016/j.future.2023.03.003

[16] Wang, B., Li, H., Guo, Y., & Wang, J. (2023). PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Applied Soft Computing*, *146*, 110677. https://doi.org/10.1016/j.asoc.2023.110677

[17] Guo, H., Li, W., Nejad, M., & Shen, C. C. (2022). A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-based Cryptographic Mechanisms. *IEEE Transactions on Network and Service Management*, *19*(4), 4605-4618.

[18] Kanwal, T., Anjum, A., Malik, S. U., Khan, A., & Khan, M. A. (2021). Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud. *Computer Standards & Interfaces*, *78*, 103522. https://doi.org/10.1016/j.csi.2021.103522

[19] Babu, E. S., Yadav, B. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster Computing*, *26*(4), 2217-2244. https://doi.org/10.1007/s10586-022-03714-z

[20] d'Aliberti, O. G. & Clark, M. A. (2022). Preserving patient privacy during computation over shared electronic health record data. *Journal of Medical Systems*, *46*(12), 85. https://doi.org/10.1007/s10916-022-01865-5

[21] Chelladurai, U. & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *13*(10), 5071-5081. https://doi.org/10.1007/s12652-021-03520-2

[22] Rai, B. K. (2023). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology*, *23*(1), 80-102. https://doi.org/10.1007/s10742-022-00279-7

[23] Lavanya, M. & Kavitha, V. (2022). Secure tamper-resistant electronic health record transaction in cloud system via blockchain. *Wireless Personal Communications*, *124*(1), 607-632. https://doi.org/10.1007/s11277-021-09374-3

[24] Chandini, A. G. & Basarkod, P. I. (2023). Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records. *Journal of Ambient Intelligence and Humanized Computing*, *14*(4), 4221-4235. https://doi.org/10.1007/s12652-023-04526-8

[25] Yadav, S. G., Gunisetti, L., Koduri, S. B., Scaria, T., Dixit, A., & Lokesh, S. (2023). Securing electronic health records using blockchain technology for IoT in healthcare domain. *Soft Computing*, *27*(18), 13009-13017.

[26] Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2021). CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1937-1948. https://doi.org/10.1109/JBHI.2021.3097237

[27] Saidi, H., Labraoui, N., Ari, A. A. A., Maglaras, L., & Emati, J. H. M. (2022). DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data. *IEEE Access*, *10*, 101011-101028. https://doi.org/10.1109/ACCESS.2022.3207803

[28] Wu, G., Wang, S., Ning, Z., & Zhu, B. (2021). Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1917-1927. https://doi.org/10.1109/JBHI.2021.3123643

Contact information:

B. ARULMOZHI
(Corresponding author)
Department of Computer Science and Engineering,
Puducherry Technological University, Puducherry, India
E-mail: ammuarulmozhi@ptuniv.edu.in

J. I. SHEEBA
Department of Computer Science and Engineering,
Puducherry Technological University, Puducherry, India

S. PRADEEP DEVANEYAN
Department of Mechanical Engineering,
Sri Venkateshwara College of Engineering and Technology, Puducherry