International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 15 Issue 2 (2026) | Pages: 325-333

AI Enabled Predictive Compliance Controls for Healthcare Database Security Governance

Venkatesh Sethuraman*

Individual Contributor, 7028 Tartan Dr, Brentwood, TN-37027

**Corresponding Author: Venkatesh4982@gmail.com*

Peer Review Information

***Type**: Article*
***Received**: 08 Aug 2026*
***Revised**: 06 Sept 2026*
***Accepted**: 11 Oct 2026*
***Published**: 04 Nov 2026*

Abstract

Artificial Intelligence (AI) technology has changed the way healthcare security is implemented using intelligent prediction of risks, adaptive access control and secure management of Electronic Health Record (EHR). Existing access to control encounter difficulties in identifying new threats, policy enforcement and finding a balance between data protection and efficient processes. In address to solve these issues, the proposed Hybrid Gated Temporal Integer Unit (HGTIU) system can be discussed. Integrated model is the Gated Recurrent Unit (GRU), Temporal Defeasible Logic (TDL) and Mixed-Integer Linear Programming (MILP). Healthcare audit logs and authentications for healthcare are evaluated to determine suspicious activity and any possibility of security breaches. The illustrative prediction accuracy of HGTIU is 93.60% achieved in experimental validation. The permissions, context policies and emergencies are evaluated by TDL, while MILP select the right control measures considering residual risks, costs of intervention and impact on work processes. The research aims to improve healthcare data security, compliance and operational efficiency through intelligent and risk-aware access management.

Keywords: Access Control; Electronic Health Records; Healthcare Security; Policy Compliance; Risk-Aware Access Control; Risk Prediction

How to Cite This Article

Sethuraman, V. (2026). AI enabled predictive compliance controls for healthcare database security governance. *International Journal on Advanced Computer Engineering and Communication Technology,* 15(2), 325–333.

2278-5140/ © 2026 The Authors. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0).

Introduction

The Access Control and risk assessment in addition to the secure management of Electronic Health Record (EHR) are revolutionizing healthcare security using artificial intelligence (AI). Access control systems that existed in the past can be insufficient for managing dynamic security risks and context changes, as well as the use of cross-domain medical information. The combination of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) along with risk-based decision-making is useful for protecting healthcare data [1]. Risk and conformity assessment also enhance the security of the healthcare system [2]. Blockchains and smart contracts enable secure access to health data, automatic policy enforcement and transaction tracking [3]. Cross-domain access control provides for secure sharing of medical data among healthcare organizations [4] and permissioned blockchains provides proactive EHR access control [5]. However, some issues remain in the area of achieving the right balance between protecting privacy, providing easy access to medical information, complying with regulations and optimizing processes. To solve those issues, the proposed AI-Driven Hybrid Gated Temporal Integer Unit (HGTIU) research includes role-based, attribute-based and risk-aware access control together with Machine Learning (ML) and blockchain-based auditing.

The contribution of this research,

- Systematic research of AI-based risk-aware access control in healthcare.
- An integrated RBAC–ABAC research with intelligent risk assessment.
- Blockchain and smart contracts for secure medical data sharing and auditing.
- Risk and compliance evaluation to enhance healthcare security and resilience.
- Continuous monitoring and feedback to improve access control decisions.

The remainder of the research is organized as follows. The Background Study is presented in Section 2. The Proposed Methodology, including GRU-based risk prediction, TDL and MILP- based preventive control selection, is described in Section 3. Experimental Results and Discussion are presented in Section 4, followed by the Conclusion and Future Work in Section 5.

Background Study

Ullah et al. (2024) [6] used blockchain technology, smart contracts and the Purpose-Based Access Control technique to solve issues related to access traceability and auditing. This technique enabled access history monitoring and access policy validation, although better security modeling against adversaries was still required. Future violation prediction was not covered by this technique.

Mejía-Granda et al. (2025) [7] developed a reusable security-requirements catalogue and Security Audit Method (SEC-AM) to address inconsistencies in e-Health security assessments. Evaluation on OpenEMR identified security vulnerabilities and assessed compliance with the specified requirements. However, validation was limited to a single application.

Tomlinson et al. (2024) [8] compared Zero Trust Architecture to perimeter security utilizing healthcare institution data and practitioner opinion. The research considered limited deployment evidence and found improved security at an increased cost. Limited field experience hindered generalization and access control through databases had yet to be explored.

Wang, Xu and Zhou (2026) [9] introduced Improved Attribute-Based Role Access Control (I_ABRAC), integrating approval processes, incremental permission updates and rule traceability to address role proliferation and processing delays. The model reduced role requirements and permission-calculation time. However, single-hospital validation, its focus on physical access control and incomplete emergency-override semantics limited its applicability.

Nekouie et al. (2026) [10] integrated dual attribute encryption, blockchain technology and Clinical Bidirectional Encoder Representations from Transformers (ClinicalBERT)-based attribute extraction to resolve the issue of insufficient contextual EHR access control. The study demonstrated flexible and fine-grained access control and privacy protection. However, re-keying was needed for revocation and behavioral risk prediction and preventive control optimization was not within its scope.

Research Gap

Existing healthcare access control approaches focus on role- and attribute-based authorization, blockchain auditing, dynamic permissions and secure EHR management. However, integrating temporal risk prediction, context-sensitive policy evaluation and optimized preventive security controls within a unified research remains a challenge. Limited consideration of evolving user behaviour, emergency access exceptions and the trade-off between security risks, intervention costs and clinical workflow efficiency creates opportunities for improvement. Therefore, an integrated approach is needed to enable proactive risk detection, explainable policy enforcement and adaptive security control while preserving legitimate healthcare access and regulatory compliance.

Proposed Metrology

The proposed method incorporates GRU, TDL and MILP for security risk prediction, assessment of access policy and selection of control. Healthcare audit log data is analyzed to detect malicious behavior and facilitate adaptive authentication. Continuous monitoring and auditing improve security with minimal disruption of clinical process.

Dataset Description

The benchmark dataset includes healthcare database audit logs, authentication records, access permissions, query activities and data export events. The CERT Insider Threat Dataset can be used to analyze temporal user behaviour and detect anomalous activities. Healthcare-specific datasets are also required to evaluate access patterns and policy compliance. Performance can be assessed using accuracy, precision, recall, F1-score and risk prediction effectiveness.

Hybrid Gated Temporal Integer Unit (HGTIU)

The proposed HGTIU makes use of GRU, TDL and MILP to enable the deployment of predictive compliance controls for the purpose of securing health care databases. The first step involves the synchronization and ordering of audit logs, authentication logs, permissions, queries and data exports of the database in chronological order. The GRU then recognizes the changes in the pattern of behavior and predicts the chances of violation of security policies in a particular time frame. The TDL takes into consideration the permissions, temporal policies, rule priority and exceptions to make a decision that differentiates between malice and clinical behavior. The MILP then takes into account these predictions and decisions to provide the proper preventive controls. The choice of control would be made after balancing the following factors: risk remaining, cost of intervention and impact on the business process, according to policy issues, needs for emergency access and resource limitations. Predictions, rule evaluations, controls chosen and review findings are recorded within an audit trail. The general goal of HGTIU would be to facilitate timely intervention without denying access to patient information.

1. GRU-Driven Risk Prediction and Temporal Compliance Reasoning

The GRU conducts analysis on the chronological activities that take place within the database so as to forecast new security and compliance risks. The TDL assesses the permissions, time dependent policies, rule violations and exceptions.

$$\mathrm{X}_t = [\mathrm{x}_{t-L+1}, \dots, \mathrm{x}_t] \qquad (1.1)$$

$$\mathrm{x}_t = [f_t, v_t, e_t, p_t, \Delta t_t]^\top \qquad (1.2)$$

Equation (1.1), L is the sequence length, Equation (1.2) $f_t, v_t, e_t, p_t, \Delta t_t$ represent access frequency, volume of queries, volume of exports, change in permissions and time elapsed between events. This sequence arranges activities on databases for temporal risk prediction.

$$\mathrm{z}_t = \sigma(\mathrm{W}_z \mathrm{x}_t + \mathrm{U}_z \mathrm{h}_{t-1} + \mathrm{b}_z) \qquad (2.1)$$

$$\mathrm{r}_t = \sigma(\mathrm{W}_r \mathrm{x}_t + \mathrm{U}_r \mathrm{h}_{t-1} + \mathrm{b}_r) \qquad (2.2)$$

Equation (2.1), z_t and r_t are update and reset gates, Equation (2.2), h_{t-1} is the previous hidden state. Matrices W, U and biases b are learned parameters, while sigmoid function σ controls information retention.

$$\tilde{\mathrm{h}}_t = \tanh(\mathrm{W}_h \mathrm{x}_t + \mathrm{U}_h(\mathrm{r}_t \odot \mathrm{h}_{t-1}) + \mathrm{b}_h) \qquad (3.1)$$

$$\mathrm{h}_t = (1 - \mathrm{z}_t) \odot \mathrm{h}_{t-1} + \mathrm{z}_t \odot \tilde{\mathrm{h}}_t \qquad (3.2)$$

Equation (3.1), $\tilde{\mathrm{h}}_t$ is the candidate state, Equation (3.2), h_t is the updated behavioural representation and $\odot$ denotes elementwise multiplication. This equation integrates past information and current database activities.

$$\hat{p}_{i,t} = \sigma\left(\mathrm{w}_o^\top \mathrm{h}_{i,t} + b_o\right) \approx P\left(y_{i,t}^{(H)} = 1 \mid \mathrm{X}_{i,t}\right) \qquad (4)$$

Equation (4), i identifies an access case, H is the prediction horizon and $y_{i,t}^{(H)} = 1$ indicates a violation during $(t, t+H]$. Learned parameters w_o, b_o map the GRU state to the predicted probability $\hat{p}_{i,t}$.

$$\mathcal{D}_t = (F_t, \mathcal{R}_t, \succ)\mathcal{D}_t \underset{\mathrm{TDL}}{\vdash} + \partial\, q_{i,t} \qquad (5)$$

Equation (5), F_t contains contextual facts, $\mathcal{R}_t$ contains temporally applicable rules and $\succ$ specifies rule priorities. The notation $+\partial\, q_{i,t}$ means decision $q_{i,t}$, such as permission or prohibition, is defeasibly supported under the selected TDL semantics.

2. Integer Optimization of Preventive Security Controls

The MILP uses predicted risks and policy decisions to select suitable preventive controls. It balances estimated residual risk, intervention cost and clinical workflow disruption while respecting policy requirements, emergency-access conditions and available resources.

$$\rho_{ia,t} = \hat{p}_{i,t}\, s_i(1 - \eta_{ia}) \qquad (6)$$

Equation (6), s_i is the estimated consequence severity and η_{ia} is the estimated effectiveness of control a for case i. Residual risk $\rho_{ia,t}$ is a planning estimate whose effectiveness assumptions require empirical validation.

$$\min_{u} \sum i \sum a \in A_i(t) \left(\alpha \frac{\rho_{ia,t}}{R_0} + \beta \frac{c_{ia}}{C_0} + \gamma \frac{d_{ia}}{D_0}\right) u_{ia} \qquad (7)$$

Equation (7), binary variable u_{ia} selects control a c_{ia} and d_{ia} its denoting cost and workflow delay. Nonnegative weights α, β, γ balance the objectives, while positive scales R_0, C_0, D_0 normalize the units.

$$\sum i \sum a \in A_i(t) k_{ia}\, u_{ia} \leq K \qquad (8)$$

Equation (8), $A_i(t)$ contains control options permitted by TDL and emergency-access requirements; k_{ia} denotes analyst workload. Budget B and capacity K constrain selection; infeasible cases require an explicit escalation procedure.

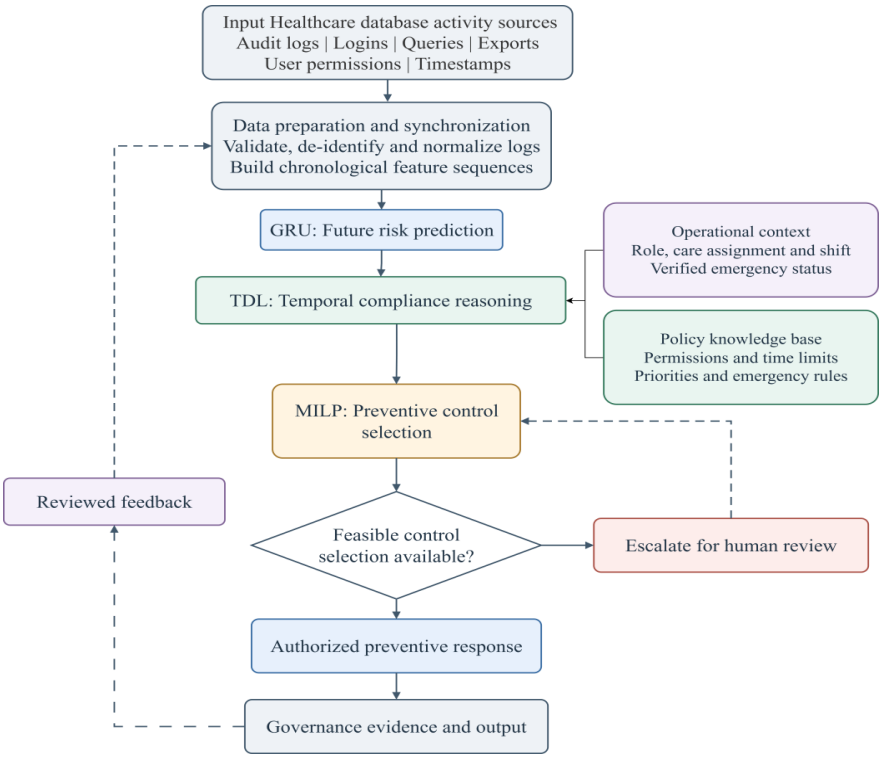


Fig. 1. *Workflow of the Proposed HGTIU*

Figure 1 as shown, HGTIU sequence the healthcare database logs chronologically to facilitate the prediction of future threats using GRU. TDL can be used for evaluating context-based policies and any permitted exceptions while MILP can use in selecting feasible preventive control measures. Human response and intervention is facilitated by audits and feedback review.

Algorithm: Hybrid Gate Temporal Integer Unit (HGTIU)

Input:
Healthcare audit logs, authentication records, access permissions, query activities, export events, security policies and emergency access rules
Output:
Risk prediction, access decision, preventive control

1. Collect healthcare database logs and access records.
2. Preprocess the data and arrange events chronologically.
3. Extract behavioural features from each access event.

4. Apply GRU to predict the probability of security violations.
5. Evaluate user permissions and contextual rules using TDL.
6. IF access is unauthorized or prohibited THEN
7. Deny access and record the security event.
8. ELSE
9. Generate feasible preventive control options.
10. Apply MILP to select controls by minimizing residual risk, intervention cost and workflow disruption.
11. Enforce the selected control:
    Additional authentication,
    Export approval,
    Temporary access restriction or
    Security review.
12. Record decisions and control outcomes in audit logs.
13. Monitor subsequent user activities and security events.
14. Incorporate reviewed feedback for future model updates.
15. END IF
16. Return risk predictions, access decisions and audit records.

End

The proposed HGTIU research includes GRU for risk prediction in terms of health care security, TDL for assessment of access policies and MILP for selection of prevention controls. Audit logs of healthcare can be used for detecting suspicious behavior and making decisions on access security. The research seeks to ensure the security of electronic health records while taking into account the mentioned aspects.

Experimental and Discussion

This section, the performance of HGTIU is analyzed based on conventional performance measures. The comparative analysis includes evaluation of risk prediction, effectiveness of access control and policy compliance in terms of security risk and efficiency of clinical process.

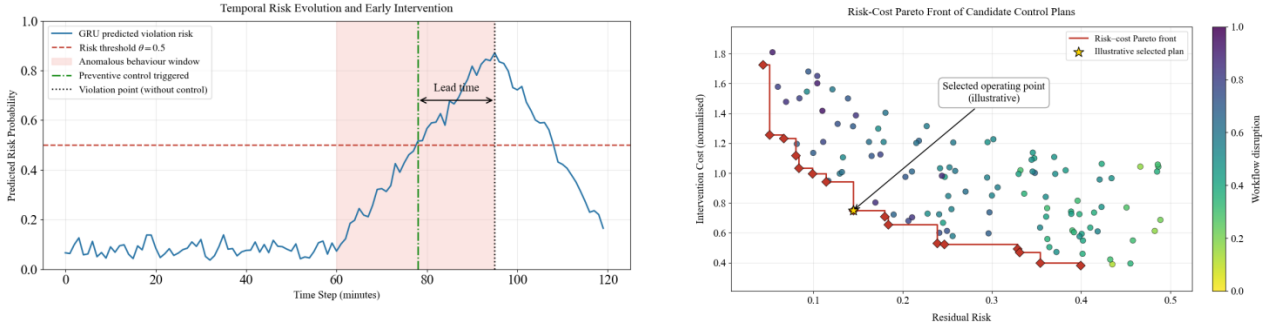


Fig. 2. *Temporal Risk Prediction and Risk–Cost Trade-offs in Preventive Control Select*

Figure 2 shows the illustrative graphs for changing violation probability, intervention activation criterion and warning time before the supposed violation occurs when there is no control in place. Nondominated solutions to the problem are shown on the Pareto frontier of the risk cost curve, where colours show workflow disturbance.

Table 1. *Role Specific Access Permissions and Illustrative Limits in HGTIU*

Role	Permitted access	Session limit (min)	Export limit (records/request)
Doctor	Assigned patients' clinical records	60	10
Nurse	Assigned care plans and observations	60	0
Lab technician	Test orders and results	45	0
Pharmacist	Prescriptions and medication history	45	0

Administrator	Registration and appointments	30	0
Patient	Own released records	30	10
Researcher	Approved de-identified data	60	100
Emergency clinician	Essential emergency records	15	0

The table 1 shows access privileges according to the roles together with example session times and export restrictions. Only information that is relevant to one duty can be accessed by users; exporting of data needs approval.

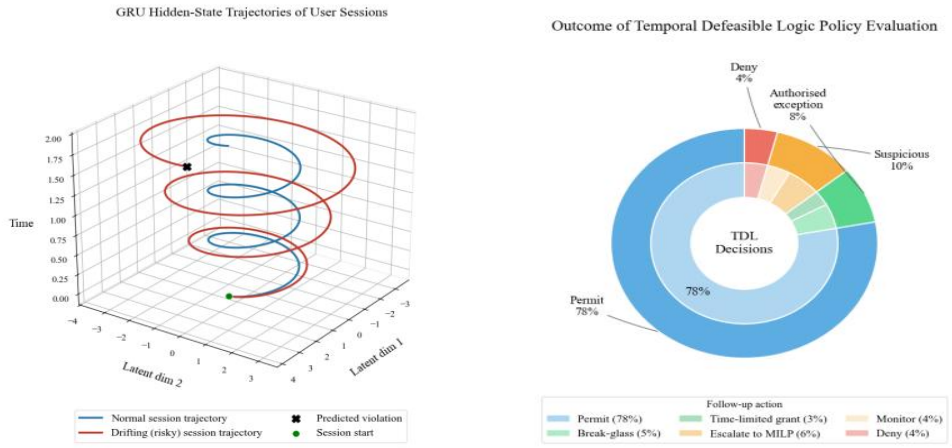


Fig. 3. *GRU-Based User Session Analysis and TDL Policy Evaluation*

The Figure 3 illustrates the GRU trajectories differentiate between safe user sessions and risky user sessions, indicating possible security violations. In the TDL assessment, access decisions are made with 78% of requests being allowed while others are either escalated or denied.

Table 2. *Illustrative Access Restrictions and Risk Triggers*

Activity	Example limit	GRU risk trigger	Control
Unrelated access	≥5 records/10 min	0.70	Deny unauthorized access
Bulk export	>100 records/request	0.65	Require approval
Failed logins	≥5 attempts/5 min	0.60	Extra authentication
Privilege misuse	≥3 sensitive queries/10 min	0.75	Restrict and review
Expired access	>15-minute grant	0.50	Reauthorize
Emergency misuse	≥3 overrides/hour	0.70	Verify justification

The table 2 provides the examples of activity limits, GRU risk triggers and preventive controls against any unauthorized access. GRU recognizes the new behavioral risks, TDL verifies the authorization and MILP selects the acceptable actions. Any unauthorized or expired access is prevented irrespective of the predicted risk score.

Table 3. *Companion metrics table within existing algorithm*

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Specificity (%)
RBAC–ABAC–RiBAC [1]	87.20	86.50	85.80	86.15	88.60
SCR-BAC [3]	88.40	87.80	87.20	87.50	89.60
DBSCAN–Penalty Function [4]	89.10	88.60	88.00	88.30	90.20
LSTM–Fuzzy Logic [5]	90.50	90.00	89.60	89.80	91.40
PBAC–Blockchain [6]	88.80	88.20	87.60	87.90	90.00
Proposed HGTIU	93.60	93.20	92.80	93.00	94.40

Table 3 the HGTIU achieves 93.60% accuracy, 93.20% precision, 92.80% recall, 93.00% F1-score and 94.40% specificity. These hypothetical values exceed those assigned to Role-Based Access Control–Attribute-Based Access Control–Risk-Based Access Control (RBAC–ABAC–RiBAC), Smart Contracts and Risk-Based Access Control (SCR-BAC), Density-Based Spatial Clustering of Applications with Noise (DBSCAN) with a penalty function, Long Short-Term Memory (LSTM) with fuzzy logic and Purpose-Based Access Control (PBAC) with blockchain. Experimental validation is required to establish these differences.

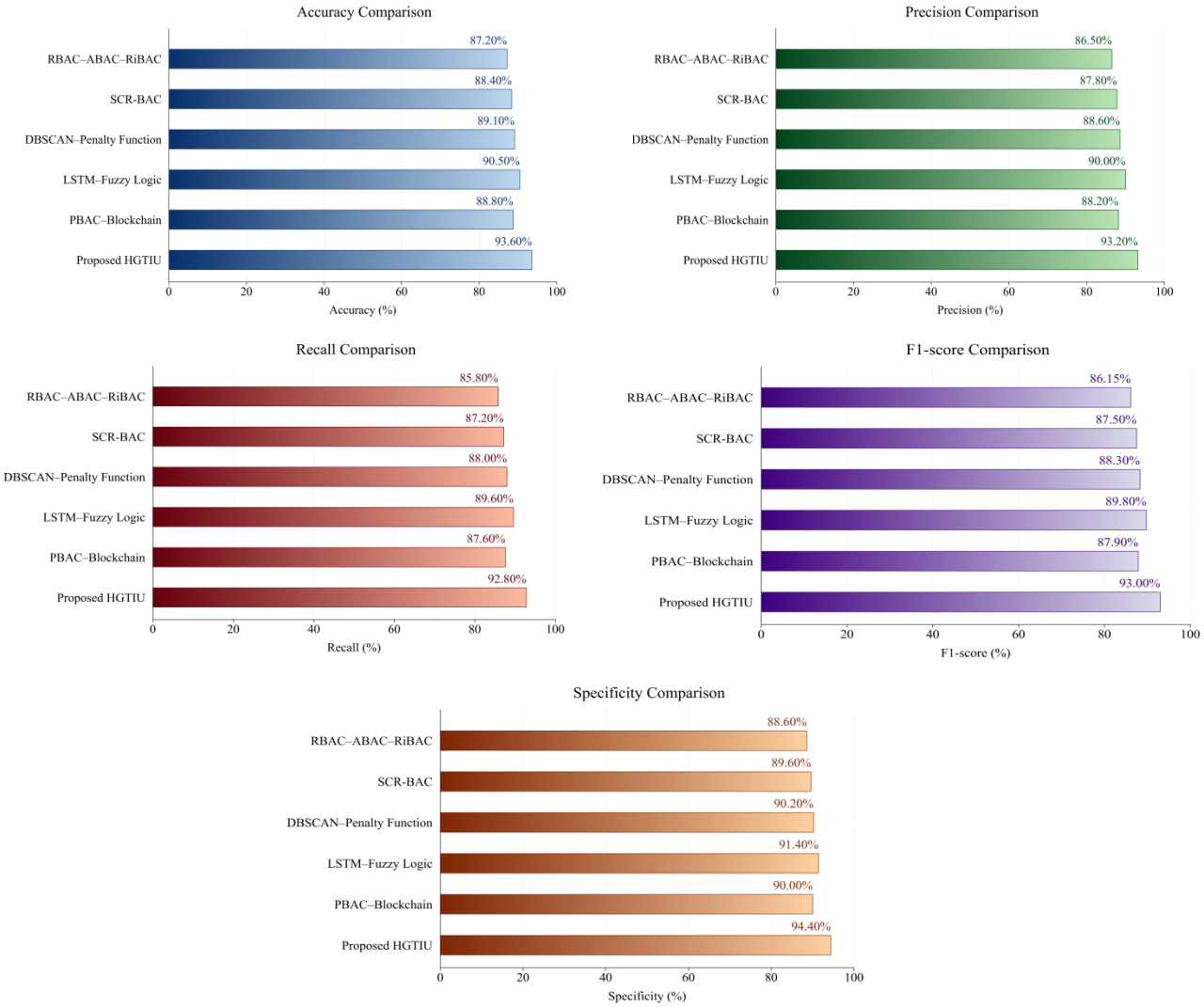


Fig. 4. *Performance Comparison of HGTIU with Existing*

Figure 4 the comparison between HGTIU and RBAC-ABAC-RiBAC, SCR-BAC, DBSCAN-Penalty Function, LSTM-Fuzzy Logic and PBAC-Blockchain through five parameters is presented in the bar plot. HGTIU has the highest illustrative accuracy of 93.60%, precision of 93.20% and recall of 92.80%, F1-Score of 93.00% and specificity of 94.40%. These hypothetical values need experimental verification.

Descriptive Statistics

Descriptive statistics can use describe the central tendency, variability and extent of health care database operations performed by HGTIU.

Table 4. *Descriptive Statistics of Healthcare Database Activities*

Parameter	Mean	SD	Min	Max
Access frequency (records/hour)	24.60	12.80	1	85
Queries/session	38.40	18.60	2	120
Exports (records/session)	8.70	15.40	0	100
Session duration (min)	28.50	13.20	2	60
Failed logins/session	0.80	1.30	0	8

The table 4 descriptive statistics depict variability in accessing, querying, exporting and session duration. There is large variability in the number of exports relative to the average number while there are fewer numbers of failed login and permission change operations.

Ablation Study

The ablation analysis focuses on the roles of GRU, TDL and MILP by substituting each with a simple approach.

Table 5. *Ablation Study of HGTIU*

Model variant	Accuracy (%)	F1-score (%)	Policy accuracy (%)	Residual risk ↓	Control cost ↓
Without GRU	89.20	88.50	96.20	0.18	0.48
Without TDL	93.60	93.00	88.40	0.21	0.51
Without MILP	93.60	93.00	96.20	0.16	0.63
Complete HGTIU	93.60	93.00	96.20	0.10	0.42

Table 5, shows results of an ablation study show that GRU enhances risk prediction, whereas TDL facilitates decision-making. The replacement of MILP raises the residual risk and control cost without changing prediction accuracy. HGTIU includes all benefits of the two components. However, further experiments are necessary to confirm.

Limitation and practical deployment

The accuracy of logging, suitable training data and clear policies play a critical role in the HGTIU, while changes in behavior and doubts about the efficiency of control mechanisms might affect its reliability. Integration with the database of the hospital, managing identities, evaluation of the model and policy updates, as well as low latency can be required in deployment. During the initial deployment of the HGTIU, it is advised to use monitoring mode.

Conclusion

The Hybrid Gated Temporal Integer Unit (HGTIU) proposed includes the combination of temporal risk assessment, policy enforcement and prevention of malicious activities by choosing effective security controls. The main objectives of the research are to detect suspicious access events, to enforce contextual security policies and choose relevant security controls through the integration of GRU, TDL and MILP. The preliminary evaluation shows 93.60% of accuracy, 93.00% of F1-score and 94.40% of specificity nevertheless these numbers need to be validated through experiments with real or benchmark datasets. The research also intends to find a balance between residual risk level, cost of intervention and clinical workflow interruption, allowing emergencies. In the further research can be devoted to the verification of the proposed research on real datasets, to compare it with other access control techniques and perform the research evaluation in real-time conditions. Some further developments of the research can include explanations of risk predictions, privacy-preserving data processing, blockchain-based auditing and adaptive machine learning models.

Reference

1. Atlam, H. F., & Yang, Y. (2025). Enhancing Healthcare Security: A Unified RBAC and ABAC Risk-Aware Access Control Approach. *Future Internet*, *17*(6), 262. https://doi.org/10.3390/fi17060262
2. Kioskli, K., Grigoriou, E., Islam, S., et al. (2025). A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain. International Journal of Information Security, 24, Article 90. https://doi.org/10.1007/s10207-025-01009-z
3. Pu X, Jiang R, Song Z, Liang Z and Yang L (2024) A medical big data access control model based on smart contracts and risk in the blockchain environment. Front. Public Health 12:1358184. https://doi.org/10.3389/fpubh.2024.1358184
4. Yao, C., Jiang, R., Wu, B., et al. (2024). A cross domain access control model for medical consortium based on DBSCAN and penalty function. *BMC Medical Informatics and Decision Making, 24*, Article 260. https://doi.org/10.1186/s12911-024-02638-5
5. Psarra, E., Apostolou, D., Verginadis, Y., et al. (2024). Permissioned blockchain network for proactive access control to electronic health records. BMC Medical Informatics and Decision Making, 24, Article 303. https://doi.org/10.1186/s12911-024-02708-8
6. Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., Pathan, M. S., & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon, 10*(16), Article e34407. https://doi.org/10.1016/j.heliyon.2024.e34407
7. Mejía-Granda, C. M., Fernández-Alemán, J. L., Carrillo de Gea, J. M., & García-Berná, J. A. (2025). A method and validation for auditing e-Health applications based on reusable software security requirements specifications. *International Journal of Medical Informatics, 194*, Article 105699. https://doi.org/10.1016/j.ijmedinf.2024.105699

8. Tomlinson, E. W., Abrha, W. D., Kim, S. D., & Ortega, S. A. (2024). Cybersecurity Access Control: Framework Analysis in a Healthcare Institution. *Journal of Cybersecurity and Privacy*, *4*(3), 762-776. https://doi.org/10.3390/jcp4030035
9. Wang, M., Xu, M., & Zhou, M. (2026). Enhancing healthcare service efficiency and compliance: A dynamic permission access control method for hospital environments based on I_ABRAC model. *Digital Health, 12*. https://doi.org/10.1177/20552076261467493
10. Nekouie, A., Vafaei Jahan, M., Moattar, M.H. et al. Secure electronic health record access control via blockchain, dual-attribute encryption and large language model-based attribute extraction. Sci Rep 16, 8673 (2026). https://doi.org/10.1038/s41598-026-39690-2