Journal of Information Systems and Telecommunication
Vol.14, No.4, July-September 2026, 196-213
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Neural Risk-Adaptive Access Control: A Behavior-Context Hybrid Framework for Adaptive Authorization in Dynamic Environments

Donya Piriaei[1], Afshin Rezakhani[2], Hamid Haj Seyyed Javadi[3], Leila Rikhtechi[1]

[1].Department of Computer Engineering, Bo. C., Islamic Azad University, Borujerd, Iran
[2].Department of Computer Engineering, Faculty of Engineering, Ayatollah Boroujerdi University, Borujerd, Iran
[3].Department of Computer Engineering, Shahed University, Tehran, Iran

Received: 08 Jun 2026/ Revised: 04 Aug 2026/ Accepted: 25 Aug 2026

Abstract

We present a risk-adaptive access control framework that integrates dynamic behavioral modeling with Attribute-Based Access Control (ABAC) to enable real-time decision-making in volatile and high-risk environments. The proposed system introduces two novel components: the Attention-based Temporal Unit (ATU) for capturing sequential access behaviors, and the Contextual Scoring Module (CSM) for quantifying contextual and environmental signals. Risk is estimated via a multi-dimensional function that combines behavioral patterns, device and location attributes, and real-time threat indicators. An adaptive decision threshold, continuously refined based on false-accept and false-reject outcomes, ensures a calibrated balance between security and operational usability. Computed risk scores are seamlessly embedded into ABAC policies to support fine-grained enforcement. Evaluation on four domain-relevant datasets—Login Data Set for Risk-Based Authentication (RBA), CERT Insider Threat Test Dataset, CIC-IDS2017, and RT-IoT2022—used to emulate access control scenarios, shows F1-scores up to 0.95 and precision up to 0.94, outperforming strong baselines by up to 12%. The results demonstrate robustness across authentication, insider threat, intrusion, and IoT domains, supporting the framework's applicability in real-time, Risk-Adaptive access systems for wireless communication and IoT environments, particularly in emerging 5G/6G contexts. The modular architecture also separates behavioral, contextual, and environmental evidence so that each source can contribute to the final authorization decision without requiring a single static risk signal.

Keywords: Risk-Adaptive Access Control; Attribute-Based Access Control (ABAC); Temporal Behavior Modeling; Attention-based Temporal Unit (ATU); Contextual Scoring Module (CSM); Real-Time Risk Assessment, Intrusion Detection Datasets.

1-Introduction

The rapid digital transformation fueled by the proliferation of the Internet of Things (IoT), cloud computing, and edge devices has led to unprecedented volumes of distributed, context-sensitive data. This evolution has significantly challenged the adequacy of traditional access control paradigms. While Role-Based Access Control (RBAC) offers structured role hierarchies, it lacks responsiveness to dynamic threats and behavioral variations. Attribute-Based Access Control (ABAC) improves adaptability by incorporating contextual information such as time, location, and device attributes. However, ABAC alone struggles to capture subtle behavioral deviations or synthesize environmental risk signals under real-time constraints [1–3].

To address this gap, Risk-Adaptive Access Control (RAdAC) frameworks have emerged, offering Risk-Adaptive decisions based on estimated security posture. Despite their promise, many RAdAC implementations rely on static rule sets or lightweight statistical models that fail to generalize across dynamic and high-risk environments. Such limitations underscore the need for access control systems that are not only flexible and context-aware but also capable of learning risk from historical interactions and adapting to ongoing environmental shifts. In this work, we introduce a modular risk-adaptive access control architecture that addresses these challenges through two

✉ **Afshin Rezakhani**
Rezakhani@abru.ac.it

specialized components: the Attention-based Temporal Unit (ATU) for modeling behavioral patterns over access sequences, and the Contextual Scoring Module (CSM) for real-time risk evaluation from contextual and environmental inputs. These components operate within a unified ABAC framework to support informed, Risk-Adaptive decisions at runtime. Unlike conventional recurrent architectures such as LSTM and GRU, which were primarily designed for general sequence prediction, the Attention-based Temporal Unit (ATU) is a task-oriented temporal encoder. It employs attention-guided aggregation to extract user behavioral patterns and directly outputs a calibrated behavioral risk probability that can be used by the authorization engine. This design reduces unnecessary recurrent complexity while improving interpretability for access-control decisions. Similarly, the Contextual Scoring Module (CSM) is not a simplified GRU; it performs attribute-level fusion of device, location, and time signals specifically optimized for explainable injection into ABAC policies. This architectural specialization constitutes a core novelty of the present work. The key contributions of our work are summarized as follows:

Modular Risk-Adaptive Architecture: A novel framework that combines the task-oriented Attention-based Temporal Unit (ATU) for behavioral risk modeling with the attribute-level Contextual Scoring Module (CSM) for contextual and environmental scoring, enabling decoupled, interpretable, and real-time risk estimation.

Temporal Behavior Modeling via ATU: Instead of relying on generic recurrent units (LSTM/GRU), the ATU leverages attention-guided sequence encoding specifically designed to detect deviations in user access behavior and produce calibrated risk probabilities suitable for authorization decisions.

Multi-Dimensional Risk Quantification: A composite risk function integrates behavioral, contextual, and environmental factors to provide comprehensive and adaptive assessments.

Feedback-Driven Threshold Adjustment: A dynamic mechanism updates access thresholds based on feedback from past accept/reject outcomes, improving sensitivity to evolving risk conditions.

Seamless ABAC Policy Integration: Computed risk scores are injected into ABAC policies to support context-sensitive, fine-grained enforcement across volatile environments.

The novelty of this research lies in its explicit architectural modularity, sequence-aware behavioral modeling, and adaptive policy coupling, providing a scalable and explainable access control mechanism that outperforms traditional RAdAC and ABAC designs. Furthermore, the proposed framework is directly applicable to critical next-generation infrastructures—such as wireless IoT networks and 5G/6G systems—where secure, real-time, and context-aware access control is a foundational requirement.

The remainder of this paper is organized as follows: Section 2 reviews related work. Section 3 discusses foundational concepts underlying ABAC, RAdAC, and behavioral risk modeling. Section 4 introduces the architecture and components of the proposed system. Section 5 presents empirical results and analysis. Section 6 concludes with key findings and outlines future directions.

2- Related work

In recent years, several intelligent and adaptive access control models have been developed to address the limitations of traditional static systems. These models enhance flexibility, context-awareness, and real-time adaptability by incorporating techniques such as deep learning, blockchain, fuzzy logic, and hybrid approaches. The literature covers domains including healthcare, IoT, cloud computing, and cyber-physical systems, each with specific contributions and challenges. Savinov [7] introduced a dynamic Risk-Adaptive ABAC framework for cyber-physical systems, which accounts for user behavior and environmental context. Zhang [8] proposed an adaptive GRU-based architecture for multivariate time-series forecasting, showcasing high temporal learning capabilities. Islam [9] and Ilyas [10] leveraged blockchain for secure access to forensic and health data, respectively, enhancing data traceability and transparency. Ranga [11] combined CNN and Dual-LSTM to improve anomaly detection in log data. Ensafi [12] evaluated various ML models for seasonal data forecasting, emphasizing the power of hybrid models. Bhatt [13] developed ABAC-CC to secure IoT through access and communication control, while Ayman [14] proposed a policy-driven hybrid RBAC model. Mazzocca [15] introduced a risk-sensitive middleware for healthcare systems. Ma [16] designed a scalable model for text data access combining content analysis and risk assessment. Other significant contributions include Jiang [17] who integrated RAdAC with UCON for large-scale healthcare data, and Ksibi [18] who proposed quantitative and qualitative threat modeling for digital health systems. Sheng [19] and Putra [20] combined ABAC and trust-based blockchain for decentralized IoT security. Alharbe [21] introduced a multi-criteria Risk-Adaptive model for cloud data access. Zhang [22] and Ma [23] developed blockchain-based frameworks for collaborative and secure data sharing. Ganiyau [24] and Ma [27] emphasized semantic and context-aware access control. Atlam [25] and Aliyu [26] explored lightweight and edge-based risk-evaluation mechanisms suitable for constrained IoT devices. Smart environments were addressed by Mansouri [29] and Atlam [30], while Seabe [31] and Malkin [32] tested the predictive performance of LSTM and GRU models. Mohammadi [33] applied

blockchain to P2P energy exchange, and Akbarfam [34] proposed a secure and automated access-control framework combining blockchain and deep learning. Raza [35] used RNN, LSTM, and GRU models to analyze cloud consumers. Fuzzy logic-based approaches were advanced by Athanere [39], Jiang [36], Atlam [40,42,45], and Morid [46]; Jiang [36] proposed a fuzzy trust-prediction and regression-based access-control model for medical big data, and Atlam [43] validated an adaptive risk-based access-control model for IoT systems. Srivastava [37] and Thilagam [47] introduced machine-learning-based risk-adaptive access-control frameworks, while Atlam [38] conducted a systematic review of risk-based access-control models in cloud environments. Outchakoucht [49], Noury [48], and Akhuseyinoglu [50] explored inference-aware and blockchain-enhanced access models. Several surveys and architectural comparisons were provided by Trabelsi [28], Ragothaman [41], and Lee [44], giving broader insights into access control evolution. Rathna et al. [51] present a cross-layer MAC protocol for wireless sensor networks that enhances energy efficiency and packet delivery. Rikhtechi et al. [52] design a secure access control system for SIEMs using structured log analysis and vulnerability-aware policies. Karimi [53] proposed a machine learning-based method for extracting ABAC policies from access logs using clustering techniques, enabling automated policy generation but dependent on log quality. Finally, in a recent publication, we introduced a BERT-LSTM-GRU-based framework (DRCFM) that emphasized semantic embedding and fusion strategies for dynamic Risk-Adaptive access control. The present work builds on that foundation by shifting focus toward lightweight, modular components (ATU and CSM) designed for real-time interpretability and seamless ABAC integration [61].

Among the reviewed works, four studies [54–56] serve as key baselines for comparison. Mohammadi [54] designed a federated deep learning access control framework for healthcare, preserving privacy but introducing scalability constraints. Niu [55] applied BERT to detect anomalies in EHRs with high precision, though with substantial computational demands and reliance on labeled data. Akbarfam [56] presented a hybrid model integrating deep learning and blockchain for automated access control, providing security guarantees at the cost of increased complexity. A comparative review shows that blockchain-based models offer decentralized trust and auditability but often incur latency and energy overhead. Deep learning approaches achieve high accuracy in pattern recognition but require substantial data and often lack interpretability. Fuzzy and hybrid models improve flexibility and adaptability but face scalability and complexity issues. To provide a concise comparison across these approaches, the key characteristics of each referenced work are summarized in Table 1. Overall, integrating context, risk, and adaptive intelligence into access control remains an active research direction. Studies [53–56] illustrate recent advances, including policy automation, privacy-preserving learning, transformer-based anomaly detection, and secure decentralized decision-making. These models highlight trade-offs among accuracy, automation, explainability, and practical feasibility, which serve as the basis for comparison in our evaluation section.

In summary, prior works demonstrate valuable advances in accuracy, security, and adaptability, but none simultaneously address dynamic risk prediction, integration with ABAC, and real-time applicability. This gap highlights the need for a unified framework that leverages deep sequential learning to predict risk adaptively, integrates seamlessly with ABAC policies, and operates efficiently under real-world conditions. Our proposed approach seeks to close this gap and provide a balanced solution across these dimensions. For a structured overview of the reviewed works, their methods, focus areas, and limitations are consolidated in Table 1.

Table 1:Complete Comparative of related works

Ref	*Main Method*	*Model Type*	*Focus*	*Limitation*
7	Risk-Adaptive ABAC	ABAC + Risk	Dynamic access via context	Relies on predefined risk values
8	Adaptive GRU	Deep Learning	Time series prediction	High computation
9	Blockchain log control	Blockchain + MFA	Secure access to logs	Scalability and cost
10	Blockchain for Health IoT	Blockchain AC	EHR data sharing	Overhead and scalability
11	CNN + Dual-LSTM anomaly detection.	Deep Learning	Log anomaly detection	High resources, generalization
12	ML for seasonal forecast	Hybrid ML	Seasonal prediction	Inaccurate under extreme seasonality
13	ABAC-CC	ABAC + Comm Control	Integrated control	Device limitations
14	Hybrid RBAC-policy	RBAC + Policy	Human error reduction	Integration with legacy systems
15	Risk-based middleware	Middleware + Risk	Distributed EHR access	Policy management complexity
16	Semantic + risk-based AC	Semantic + Risk	Content-sensitive access	Semi-structured data challenges
17	RAdAC + UCON	Risk + Usage Control	Scalable medical data access	Infrastructure cost
18	Quantitative threat modeling	Quantitative Risk	Precise threat analysis	Complex in heterogeneous env.
19	Blockchain ABAC	ABAC + Blockchain	Decentralized control	Energy usage
20	Trust-based BC model	Blockchain + Trust	Trust evaluation	Latency, cost

21	Cloud-based RAdAC	Multi-criteria Risk	Adaptive cloud access	Threshold tuning
22	Collaborative blockchain AC	Blockchain	Cooperative secure access	Delay, key management
23	Dynamic BC access	Blockchain	Dynamic sharing	Computation cost
24	Context-aware AC	Context + Risk	Smart access decisions	Privacy and context tracking
25	Lightweight risk eval.	Fuzzy logic	Efficient risk estimation	Manual tuning
26	ad-RACs	ML + Risk	Edge-based adaptive AC	Learning model dependency
27	RTBAC for text	Semantic + Risk	Fine-grained text AC	Compute-intensive
28	IoT AC survey	Survey	Trends in IoT AC	Method diversity
29	Two-level risk AC	Risk-based	Market-aware control	High complexity
30	ANFIS AC	Fuzzy + NN	Real-time adaptive access	Training data quality
31	LSTM/GRU forecast	Deep Learning	Crypto price prediction	Volatility sensitivity
32	Smart home AC	Adaptive Control	Balanced smart access	Monitoring overhead
33	P2P energy AC	Blockchain + Risk	Transaction security	Cost and scale
34	DL + Blockchain	Hybrid	Secure automation	Processing delay
35	Trust analysis in the cloud	GRU/LSTM	Cloud trust/security	Training time
36	Fuzzy trust + regression	Fuzzy + ML	Adaptive EHR AC	Complex logic
37	ML-based smart AC	ML + Risk	Dynamic decision-making	Data dependency
38	Risk-based AC review	Literature Review	Model taxonomy	No experimentation
39	Dynamic AC model	Adaptive Risk	Scalable AC model	Infrastructure requirement
40	Fuzzy IoT AC	Fuzzy logic	Access in uncertainty	Parameter sensitivity
41	IoT AC overview	Survey	Challenge identification	Lack of implementation
42	Neuro-fuzzy IoT AC	NFS	Accurate risk estimation	Tuning and explainability
43	Lightweight IoT AC	Optimized	Fast AC in IoT	Scalability
44	IoT security survey	Review	Security threats	General scope
45	Adaptive IoT AC	Risk-aware	Context-based control	Compute cost
46	DL in Healthcare Time series	LSTM/Transformer	Medical prediction	Privacy and explainability
47	DL-based health IoT AC	Deep Learning	High-security access	Energy usage
48	Inference-aware AC	Policy + Reasoning	Preventing leakage	Complex configuration
49	Blockchain + ML	Hybrid	Dynamic AC	Energy and complexity
50	ABAC for CPS	ABAC + Risk	Real-time secure access	Deployment overhead
51	GRU model comparison	GRU Variants	Performance evaluation	Parameter tuning
52	LSTM review	LSTM-based	Architecture insight	High training need
53	ABAC rule mining	ML + Clustering	Policy automation	Log quality sensitivity
54	Federated Deep AC	FL + DL	Secure distributed AC	Scalability
55	BERT for anomaly detection.	BERT	Pattern detection	Label dependency
56	DL + Blockchain AC	Hybrid	Automated secure access	Resource cost
61	BERT-LSTM-GRU with Risk-Aware Fusion	Deep Hybrid (BERT + RNN)	High accuracy, adversarial robustness, semantic embedding	Limited interpretability, high model complexity, lacks integration with ABAC logic

3- Proposed Framework

This section introduces the proposed risk-adaptive access control framework tailored for dynamic and security-sensitive environments. Prior to describing the architectural components and algorithms, we present concise definitions of the core concepts and modules utilized throughout the framework, including the types of risk and two key analytical components: the Attention-based Temporal Unit (ATU) and the Contextual Scoring Module (CSM). Existing recurrent architectures such as LSTM and GRU were originally developed for general sequential prediction rather than dynamic Risk-Adaptive authorization. In access control, the objective is to extract behavior-sensitive temporal representations that directly support authorization decisions under changing contexts and low-latency requirements. Motivated by this observation, the proposed Attention-based Temporal Unit (ATU) was designed as a task-oriented temporal modeling component that preserves discriminative behavioral patterns while reducing unnecessary recurrent complexity and facilitating integration with contextual risk evaluation.

3-1- Terminology and Core Modules

This subsection defines the fundamental terms and components forming the basis of the proposed access control framework. It introduces the types of risk

considered in the system, as well as the key analytical modules—ATU and CSM—that replace traditional sequential models and enable adaptive, context-aware risk analysis.

Attribute-Based Access Control (ABAC): Attribute-Based Access Control (ABAC) is a dynamic and flexible model that grants permissions based on a set of attributes associated with users, objects, and the environment [1]. Unlike traditional models such as Role-Based Access Control (RBAC), which rely on predefined roles, ABAC defines policies through attributes. These may include user attributes (AU), object attributes (AO), and environmental attributes (AS). In ABAC, access decisions are made by evaluating these attributes against predefined policies. For example, a policy may allow only users above a certain age (AU) or those accessing during specific times (AS) to access a resource (O). Formally, the ABAC model is represented as follows:

$$Auth= \{(u,o,a)|U\ A(u) \supseteq Req_U, O\ A(o) \supseteq Req_O, Perm(a,o) \supseteq Req_A\}$$

Where:

- $A(u)$ denotes the set of user attributes that must satisfy the required attributes Req_U.
- $A(o)$ denotes the set of object attributes that must satisfy the required attributes Req_O.
- *Perm(a,o)* represents the permissions required for an action *a* on object *o*.

The flexibility of this model enables fine-grained access control that adapts to changing conditions and contexts, which is especially useful in environments where access requirements vary frequently.

While ABAC offers fine-grained control, its reliance on static policies limits adaptability under high-risk and dynamic conditions.

Risk-Adaptive Access Control (RAdAC): Risk-Adaptive Access Control (RAdAC) is a dynamic access control model designed to address the limitations of traditional approaches in highly dynamic and mission-critical environments. According to NIST, RAdAC integrates risk assessment and operational needs into access decision-making. Unlike static models such as RBAC or ABAC, RAdAC evaluates security risk and mission impact at runtime when granting or denying access [2,3]. As noted in the NIST Privilege Management Workshop and SP 800-160 Vol.1, the RAdAC decision process usually consists of three interrelated components:

- Trust Evaluation: Estimating the trustworthiness of the subject (e.g., user or device) based on credentials, past behavior, and system reputation.
- Operational Need: Determining the urgency or importance of the requested access, which in mission-critical cases may override risk constraints.
- Risk Assessment: Evaluating potential threats by analyzing contextual factors such as user behavior, device status, environmental conditions, threat intelligence, and the value of the resource.

Our model extends this structure by integrating all three risk dimensions into a unified pipeline. The proposed Risk Determination Engine (RDE) employs time-series access data and domain-specific deep components—the Attention-based Temporal Unit (ATU) and Contextual Scoring Module (CSM)—to dynamically learn and estimate risk scores based on a combination of:

- Historical access logs
- User activity patterns
- Device and network status
- Environmental factors (e.g., location, time of access)
- Active threat signals or detected anomalies

This approach ensures that contextual, behavioral, and system factors are considered in the access decision. A dynamic risk score is computed and compared with a threshold to determine access. If the risk is acceptable, the request is evaluated under ABAC policies. Mathematically, the risk assessment in RAdAC can be expressed as:

$$Access\ Risk = User\ Risk\ Weight \times Resource\ Risk.$$

This method allows RAdAC to provide an adaptive, context-aware approach to access control, which is useful in environments with high security requirements and rapidly changing conditions. By continuously evaluating and adjusting access through real-time risk assessments, RAdAC improves security while preserving operational flexibility [2,3]. RAdAC enhances adaptability but its effectiveness depends on accurate real-time risk estimation, which is challenging in practice.

Deep Learning Models for Time Series : Time-series data, composed of sequences of observations arranged chronologically, are common in domains such as finance, healthcare, and weather forecasting. To model and predict patterns that change over time, deep learning models such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTMs), and Gated Recurrent Units (GRUs) have become essential tools [4–6].

Recurrent Neural Networks (RNNs): RNNs are designed to process sequential data by maintaining a hidden state that captures information from previous time steps. This structure enables RNNs to model temporal dependencies in time-series data. However, standard RNNs face challenges such as the vanishing-gradient problem, which limits their ability to learn long-range dependencies [55].

Long Short-Term Memory Networks (LSTMs): LSTMs, a variant of RNNs, address the limitations of standard RNNs. They introduce a gating mechanism—including input, forget, and output gates—that controls the flow of information through the network. This architecture enables LSTMs to retain and transmit important information over longer sequences, making them effective for tasks that require long-term context, such as language modeling and time-series forecasting [56].

Gated Recurrent Units (GRUs): GRUs are another RNN variant, similar to LSTMs but with a simpler design. GRUs combine the input and forget gates into a single update gate, reducing the model's complexity while still capturing temporal dependencies effectively. In many applications, GRUs perform comparably to LSTMs while requiring fewer computational resources [57].

These deep learning models are widely used for time-series analysis because of their ability to capture temporal patterns and dependencies. They are especially useful when traditional methods, such as autoregressive models, struggle with non-linear and non-stationary data [58]. Although RNN, LSTM, and GRU capture complex temporal dependencies, they require large-scale datasets and often lack explainability, which may hinder adoption in security-critical environments.

- **Behavioral Risk**

Behavioral risk quantifies the likelihood of anomalous or unauthorized behavior based on historical access patterns of a user. It is inferred from temporal sequences of prior access attempts, capturing deviations from a user's established behavioral profile. This form of risk is critical for identifying subtle misuse or insider threats that rule-based systems may overlook.

- **Contextual Risk**

Contextual risk captures the situational threat level of an access attempt, based on attributes such as access time, physical location, and device characteristics. For instance, a request initiated outside normal working hours, from an unrecognized location or an unregistered device, may carry a higher contextual risk.

- **Environmental Risk**

Environmental risk reflects the overall security posture of the system at a given moment. It incorporates signals such as failed login attempts, current system load, active alerts from intrusion detection systems, and external threat intelligence. These factors enable the access control system to respond to broader threat dynamics beyond individual user behavior.

- **Attention-based Temporal Unit (ATU)**

Inspired by the temporal learning capability of Long Short-Term Memory (LSTM), the proposed Attention-based Temporal Unit (ATU) is specifically designed for sequential behavioral risk modeling in dynamic access-control environments. Rather than replicating the complete LSTM architecture, ATU retains only the temporal modeling mechanisms that are essential for extracting behavior-sensitive patterns relevant to authorization decisions. This task-oriented design reduces unnecessary recurrent complexity while maintaining the capability to capture temporal dependencies required for accurate risk estimation. Consequently, ATU provides an effective balance between temporal representation, computational efficiency, and interpretability for risk-adaptive access control.

- **Contextual Scoring Module (CSM)**

Analogous in spirit to Gated Recurrent Units (GRU), CSM is designed to efficiently synthesize real-time contextual information—such as device trust level, geolocation, and time of access—into a unified risk representation. Unlike general-purpose GRUs, CSM prioritizes attribute-specific encoding, enabling adaptive fusion of contextual cues with behavioral signals. This modular structure supports explainability and fine-grained policy integration within ABAC frameworks. The Contextual Scoring Module (CSM) draws inspiration from GRU architectures but is redesigned to prioritize attribute-level fusion of contextual cues such as device, location, and time. It offers a lightweight and modular alternative that better aligns with the explainability and performance requirements of risk-adaptive access policies. The notations and abbreviations used throughout the paper are summarized in Table 2 for clarity.

Table 2: Symbols and Notations

Abbreviation	**Full Form**
ABAC	Attribute-BasedAccessControl
RAdAC	Risk-Adaptive Access Control
ATU	Attention-based temporal unit
CSM	Contextual scoring module
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
GRU	Gated Recurrent Unit
RDE	Risk Determination Engine
PEP	Policy Enforcement Point
PDP	Policy Decision Point
FRR	False Rejection Rate
FAR	False Acceptance Rate
F1-Score	Harmonic mean of precision and recall
AUC	Area Under the ROC Curve
AU	User Attributes (ABAC)
AO	Object (Resource) Attributes (ABAC)
AS	Environmental Attributes (ABAC)
U	Set of Users
O	Set of Objects (Resources)
S	Set of Sessions
OP	Set of Operations
Mathematical Symbols and Notation	
$\boldsymbol{u, r, t}$	User, resource, and current time step
$\boldsymbol{R(u, r, t)}$	Overall (composite) risk score for user u accessing resource r at time t (Eq. 1)
$\boldsymbol{H_{u(t)}}$	Behavioral risk (predicted by ATU at time t (Eq. 6)
$\boldsymbol{C(u, r, t)}$	Contextual risk (device, location, time) (Eq. 2)
$\boldsymbol{\mathcal{E}(t)}$	Environmental risk (system/network conditions) (Eq. 3)

$\lambda_1, \lambda_2, \lambda_3$	Weights for behavioral, contextual, and environmental risk in Eq. (1)
$C^{dev}(u,t)$	Device-related contextual risk component
$C^{loc}(u,t)$	Location-related contextual risk component
$C^{time}(u,t)$	Time-based contextual risk component
$w_{dev}, w_{loc}, w_{time}$	Weights for contextual risk components in Eq. (2)
$F(t), S(t), A(t), E_{ext}(t)$	Failed logins, system load, security alerts, and external signals
w_f, w_s, w_a, w_e	Weights for environmental factors in Eq. (3)
τ	Adaptive decision threshold
α	Learning rate for adaptive threshold update (Eq. 5)
$X_u^{t-k:t}$	Sequence of user u's most recent k access events (model input)
f_θ	ATU/CSM model function with parameters θ
σ	Sigmoid activation function mapping outputs to [0,1]
$L(\theta)$	Binary cross-entropy loss (Eq. 4)
N	Number of training samples
θ	Trainable model parameters
X	Encoded input sequence (access vectors)
y	Ground-truth labels (0 = safe, 1 = risky)
ŷ	Predicted risk probability
TP, TN, FP, FN	Confusion-matrix counts used in metrics

3-2- Risk-Based Intelligent Access Control

In modern digital environments characterized by rapidly evolving threats and dynamic contexts, traditional static access control schemes such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) prove insufficient. RBAC enforces fixed, role-based permissions, and ABAC introduces greater flexibility by leveraging contextual attributes, but neither model can adapt in real time to changing risk conditions. Risk-Adaptive Access Control (RAdAC) frameworks attempt to address this by incorporating dynamic risk evaluation into access policies; however, many existing RAdAC solutions rely on static rules or simplistic models that fail to capture complex user behaviors and evolving threat landscapes.

To address these gaps, we propose a hybrid Risk-Adaptive access control framework that integrates deep learning techniques with ABAC, enabling dynamic risk estimation and adaptive decision-making. Specifically, our model employs an Attention-based Temporal Unit (ATU) and a Contextual Scoring Module (CSM) to analyze user behavior and contextual factors, respectively. The ATU learns temporal patterns in historical access sequences, enabling the system to detect subtle anomalies in user behavior. Simultaneously, the CSM evaluates real-time contextual and environmental information—such as unusual access times, unrecognized devices, or active threat alerts—to ensure the computed risk reflects the system's current security state. As illustrated in Figure 1, the architecture comprises five interconnected modules that collectively support data-driven, real-time access decisions:

1. Access Request Collector: Captures metadata from each access request (user ID, requested resource, timestamp, device ID, and location).
2. Access History Analyzer: Stores structured logs of past access activities to build detailed behavioral profiles.
3. Risk Evaluation Engine: Computes a composite risk score by integrating behavioral risk (from historical patterns), contextual risk (based on factors like anomalous access times or device trust levels), and environmental risk (reflecting system-wide threat conditions).
4. Deep Risk Predictor (ATU/CSM-based): Leverages the Attention-based Temporal Unit (ATU) and Contextual Scoring Module (CSM) to learn long-term dependencies and detect behavioral anomalies in historical data, thereby refining the risk evaluation.
5. Access Decision Module: Enforces ABAC policies augmented by the dynamic risk score, making fine-grained allow/deny decisions for each access request.

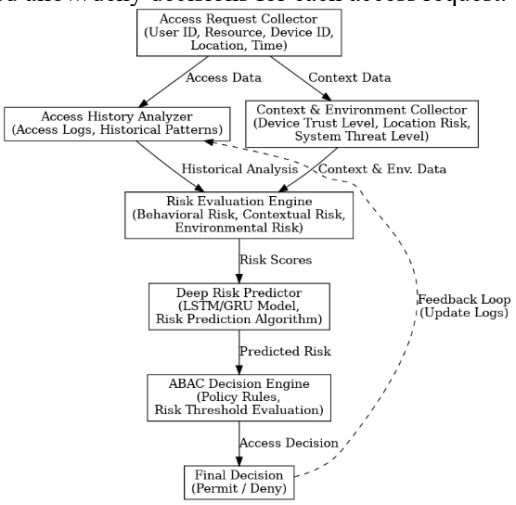


Fig.1 Architecture of the Proposed Risk-Adaptive Access Control System

3-3- Risk Quantification Based on Access History

Our framework computes risk scores based on access history, with particular attention to user behavior derived from historical data. Unlike conventional RAdAC models that focus mainly on contextual factors, our approach combines historical, contextual, and environmental risks within a single risk function.

3-3-1- Formal Definition of Risk Function

Let u denote a user, r a resource, and t the request time. The risk function *R(u,r,t)* in Eq. (1) is formally defined as:

$$R(u,r,t) = \lambda 1 \cdot Hu(t) + \lambda 2 \cdot Cu(u,r,t) + \lambda 3 \cdot E(t) \quad (1)$$

where:

- $Hu(t)$: Historical behavior risk from prior access sequences.
- $Cu(u,r,t)$: Contextual risk based on real-time attributes (device, location, time).
- $E(t)$: Environmental risk reflecting current system threats.
- $\lambda1, \lambda2, \lambda3 \in [0,1]\ and\ \lambda1 + \lambda2 + \lambda3 = 1$.

3-3-2- Behavioral Risk Score from Access History

To compute H$u(t)$, we define a structured access history sequence:

$$Su = [(a_1, t_1, d_1, l_1, p_1), \ldots, (a_n, t_n, d_n, l_n, p_n)]$$

Where each tuple represents a historical access attempt, with:

- ai: Resource or action requested,
- ti: Timestamp,
- di: Device used,
- li: Location of access,
- $pi \in \{0,1\}$: Decision outcome ($deny = 0, permit = 1$).

This sequence is encoded and processed by a trained Attention-based Temporal Unit and Contextual Scoring Module network to estimate the probability of anomalous behavior. The procedure for computing the risk score from access history is outlined in Algorithm 1.

Algorithm 1 Computing Historical Risk
***procedure ComputeHistoricalRisk($Su, f\theta$)*:**
V ← []
for each (ai, ti, di, li, pi) in Su in temporal order do
vi ← Encode(ai, ti, di, li, pi)
append vi to V
end for
z ← fθ(V) # network logit or score
H ← σ(z) # if fθ outputs logits; else H ← z if already probabilistic
return H # equals Hu(t)
end procedure

3-3-3- Contextual Risk Evaluation

The contextual risk $Cu(t)$ is assessed using real-time attributes such as device type, physical location, and time of access. Each attribute influences the risk score according to predefined profiles or learned patterns:

- Device Risk: Known and managed devices are assigned lower risk, while unknown or unmanaged devices are assigned higher risk.
- Location Risk: Access from within organizational premises or trusted networks carries lower risk, while access from public or unverified locations carries higher risk.
- Time Risk: Access during regular working hours is considered lower risk, while access at unusual times may suggest anomalous behavior.

The total contextual risk in Eq (2) is calculated as:

$$C(u,r,t) = w_{dev}\ C^{(dev)}(u,t) + w_{loc}\ C^{(loc)}(u,t) + w_{time}\ C^{(time)}(u,t) \quad (2)$$

Equation (2) decomposes the contextual risk into device-, location-, and time-based components. The weights w_{dev}, w_{loc}, w_{time} reflect the relative importance of each factor, and can be tuned to match the security requirements of a particular environment. For example, in high-security settings, the device attribute may be assigned greater weight, while in location-sensitive systems, the location factor may dominate. Contextual risk is highly sensitive to organizational policies; misconfigured weights may lead to biased decisions, such as over-restricting remote users.

3-3-4- Environmental Risk Evaluation

The environmental risk E(t) represents the current security state of the system and includes factors such as:

- Failed Login Attempts: A large number of failed logins may indicate a brute-force attack.
- System Load: Elevated system load can suggest a denial-of-service attack or other anomalies.
- Active Security Alerts: Current incidents or alerts reported by intrusion detection systems.
- External Threat Intelligence: Information on ongoing threats or vulnerabilities that could affect the system.

The total environmental risk in Eq (3) is calculated as:

$$E(t) = w_f \cdot F(t) + w_s \cdot S(t) + w_a \cdot A(t) + w_e \cdot E_{ext}(t) \quad (3)$$

Equation (3) models the environmental risk as a weighted combination of system- and environment-related factors. Specifically, $F(t)$ denotes failed login attempts, $S(t)$ represents system load, $A(t)$ captures security alerts, and $E_{ext}(t)$ refers to external signals such as network anomalies or third-party threat feeds. The weights w_f, w_s, w_a, w_e, w can be configured depending on the operational environment. For example, in cloud-based infrastructures, system load may play a dominant role, while in mission-critical settings, external threat intelligence may be prioritized.

3-4- Deep Learning-based Risk Predictor

Our risk predictor uses recurrent neural networks (Attention-based Temporal Unit and Contextual Scoring Module) to learn long-term behavioral patterns. The model captures temporal relationships in access sequences, improving predictive accuracy and sensitivity to behavioral anomalies. The Attention-based Temporal Unit and

Contextual Scoring Module are trained on historical access data and optimized using the following binary cross-entropy loss:

$$L(\theta) = -\frac{1}{N}\sum_{i=1}^{N}\left[w_{+}y_i\, log(\hat{y}_i) + \left(w_{-}(1-y_i)\right) log(1-\hat{y}_i)\right] \quad (4)$$

Equation (4) defines the weighted binary cross-entropy loss used to optimize the Attention-based Temporal Unit and Contextual Scoring Module models. Here, y_i is the ground-truth label, $\hat{y}_i$ is the predicted probability, and w_+ and w_- are inverse-frequency weights for the risky and safe classes, respectively. These weights are computed from the training-label ratio as specified in Algorithm 2, so errors in the minority class contribute more strongly to the loss. The logarithmic terms continue to penalize confident incorrect predictions, while the weighting addresses class imbalance and preserves probabilistic interpretation.

To keep the predictor effective against changing user behaviors and emerging threats, the model can be updated periodically with new access data or through online learning techniques. This helps the system stay adaptive to recent patterns. The training process of the Deep Risk Predictor is outlined in Algorithm 2.

Algorithm 2 Training the Deep Risk Predictor
procedure TrainDeepRiskPredictor(D, RNN_type∈{ATU,CSM e.g., LSTM, GRU}):
split D into train/val
initialize fθ (RNN_type), optimizer (e.g., Adam), early-stopping
compute class weights w_+, w_- from train label ratio
for epoch = 1..E do
for each minibatch (X, y) in train do
z ← fθ(X)
y_pred ← σ(z)
L ← BCE(y, y_pred; weights = {w_+, w_-})
backpropagate L and update θ
end for
monitor val_AUC, val_F1
if no improvement for P epochs: break
end for
return θ
end procedure

3-5- Adaptive Access Decision Process

The final access decision is based on dynamic risk thresholds that are updated from ongoing system feedback. These thresholds are adjusted according to risk prediction accuracy and compliance with security policies, allowing automatic policy adaptation. The adaptive threshold is denoted by $\tau(t)$ and updated periodically as in Eq. (5):

$$\tau(t+1) = \tau(t) + \alpha \cdot (FRR - FAR) \quad (5)$$

Equation (5) provides the adaptive update rule for the decision threshold τ. The threshold is adjusted based on the observed difference between the False Rejection Rate (FRR) and the False Acceptance Rate (FAR), with learning rate α. If FRR exceeds FAR, the threshold is raised to reduce unnecessary denials; conversely, if FAR is higher, the threshold is lowered to tighten security. This dynamic mechanism allows the system to balance usability and security over time, in contrast to static thresholds used in traditional RAdAC systems.

Unlike static thresholds, the adaptive mechanism reduces bias over time, but frequent threshold shifts may increase system instability if FRR/FAR estimates are noisy. The procedure for updating the adaptive threshold is outlined in Algorithm 3.

Algorithm 3 Updating the Adaptive Threshold
procedure UpdateThreshold(τ, window W, α, β, τmin, τmax):
(FRR, FAR) ← EstimateRates(W) # on last m decisions
τ' ← clamp(τ + α · (FRR − FAR), τmin, τmax)
τ+1 ← (1 − β) · τ + β · τ' # EMA smoothing to avoid oscillations
return τ+1
end procedure

3-6- Integration with ABAC

Our framework seamlessly integrates computed risk into ABAC policies, thereby enhancing their adaptability. In this model, ABAC policies evaluate a combination of user, resource, environmental, and risk-related attributes to determine access rights. The framework further enables the specification of distinct risk thresholds (τ) for different resources or user roles, supporting fine-grained control over authorization. For instance, highly confidential resources may be assigned stricter thresholds, demanding stronger evidence of low risk before access is granted, whereas less sensitive resources can operate under more relaxed thresholds. The complete Risk-ABAC decision-making process is described in Algorithm 4, and an illustrative policy rule demonstrates how risk scores directly shape access outcomes.

$$IF\ (User.role = "Manager")\ AND\ (Resource.type = "Confidential")\ AND\ (Risk \leq \tau)$$
$$THEN\ PERMIT$$
$$ELSE\ DENY$$

Algorithm 4 Integrated Risk-ABAC Decision
procedure RiskABACDecision(q, Π, τ_map):
(u, r, t, ctx) ← Parse(q)
H ← ComputeHistoricalRisk(Su_recent(u), fθ)
C ← ComputeContextRisk(u, r, t, ctx) # Eq.(2)
E ← ComputeEnvRisk(t) # Eq.(3)
R ← λ1·H + λ2·C + λ3·E # Eq.(1)
τ ← τ_map[role(u), r] # resource/role-specific threshold
if MissingRequiredAttrs(u, r, ctx): return DENY
if R ≤ τ and EvaluateABAC(Π, u, r, ctx) = TRUE:
LogDecision(u, r, t, R, τ, "PERMIT")

return PERMIT
else:
LogDecision(u, r, t, R, τ, "DENY")
return DENY
end procedure

Compared with prior works (e.g., [7, 13, 21, 56]), our framework introduces a unified integration of behavioral, contextual, and environmental risks, optimized with recurrent deep models. This ensures finer granularity than blockchain-only models and greater adaptability than fuzzy or rule-based approaches.

Some of the architectural elements proposed in this framework—specifically the Attention-based Temporal Unit (ATU) and the Contextual Scoring Module (CSM)—originate from our earlier work [61], where they were designed and validated as independent components for behavior modeling and context-aware risk analysis. In the present study, these modules are systematically integrated into a cohesive access control framework, extended with real-time policy coupling, adaptive thresholding, and multi-domain evaluation. This integration allows us to demonstrate not only their individual effectiveness but also their synergy in supporting robust, risk-adaptive access decisions under dynamic and heterogeneous conditions.

4- Experimental Evaluation

To evaluate the effectiveness and robustness of the proposed Risk-Adaptive Access Control Framework, we conducted experiments on four widely used real-world and benchmark time-series datasets: RBA, CERT Insider Threat, CIC-IDS2017, and RT-IoT2022. The goal of these experiments was to examine the model's capability to derive risk scores from access histories, contextual information, and environmental factors, thereby ensuring accurate and timely access control decisions.

Table 3: Description of datasets used in the evaluation

Dataset	Description	Samples	Reference
Login Data Set for Risk-Based Authentication (RBA)	Synthesized login attempts from a large-scale online service, including IP, location, device, user agent, RTT, timestamp, success/failure for risk-based authentication evaluation.	>33,000,000 login attempts (>3.3M users)	[57]
CERT Insider Threat Test	Synthetic enterprise logs (logon, device, file, email) with benign and malicious insider scenarios for behavioral anomaly detection in access control.	Millions of log records (e.g., r6.2: ~135M events for 4,000 users)	[58]
CIC-IDS2017	Labeled network flows from realistic enterprise simulation, including benign traffic and attacks (brute force, DoS, infiltration) as proxy for unauthorized access risks.	~2,830,000+ labeled flows	[59]
RT-IoT2022	Real-time bidirectional IoT network flows from diverse devices, with normal patterns and attacks (DoS, brute force, scans) for anomaly detection in dynamic IoT access.	123,117 instances	[60]

4-1-Datasets and Experimental Setup

To ensure domain relevance and methodological validity, we evaluate the proposed framework on four publicly available datasets specifically related to access control, authentication, insider threats, network intrusions, and IoT security: (1) Login Data Set for Risk-Based Authentication (RBA Dataset), providing large-scale login attempts with contextual features for risk-based decisions; (2) CERT Insider Threat Test Dataset, simulating enterprise access logs with anomalous behaviors; (3) CIC-IDS2017, containing labeled network flows with attacks proxying unauthorized access; and (4) RT-IoT2022, capturing real-time IoT traffic including normal and adversarial patterns. Each dataset was preprocessed into sequential access-like records: temporal sequences for behavioral risk (ATU input), device/location/IP/time for contextual risk (CSM), failed attempts/alerts/attacks for environmental risk. Synthetic or derived permit/deny labels were used where necessary (e.g., benign vs. attack flows in CIC-IDS2017 mapped to safe/risky access). This approach enables direct evaluation of risk-adaptive mechanisms in realistic scenarios. A summary of the datasets is provided in Table 3. Each dataset was carefully mapped to the access-control decision problem. Specifically, user identifiers, resources/actions, timestamps, device/IP information, and location attributes were treated as the standard ABAC attributes (subject, object, environment). Attack or anomalous records were labeled as high-risk (deny) access attempts, while benign records were labeled as low-risk (permit). This mapping is justified because the resulting binary decision task is isomorphic to risk-adaptive authorization: the model must distinguish legitimate from

anomalous access patterns under realistic contextual and environmental conditions. The RBA dataset directly reflects risk-based authentication scenarios, the CERT dataset captures insider behavioral anomalies, CIC-IDS2017 provides network-level intrusion patterns that proxy unauthorized access, and RT-IoT2022 supplies real-time IoT traffic with both normal and adversarial behaviors. Consequently, performance on these datasets provides a meaningful evaluation of the framework's ability to support Risk-Adaptive access decisions across authentication, insider threat, intrusion, and IoT domains. To ensure full reproducibility, all experiments were conducted with the following fixed configuration unless otherwise stated: Adam optimizer with learning rate 1×10^{-3}, batch size 64, sequence length k = 10, embedding dimension 64, binary cross-entropy loss with inverse-frequency class weights, early-stopping patience of 8 epochs based on validation AUC, and random seed 42 for all weight initializations and data shuffling. The complete source code, pre-processed data splits, and configuration files will be publicly released upon acceptance of the paper. The implementation was carried out in TensorFlow with the Keras backend. ATU/CSM modules map access patterns into behavioral risk probabilities $H_u(t)$ (Eq. (6)). The overall risk function is given in Eq. (1), with default weights $\lambda_1 = 0.6$, $\lambda_2 = 0.3$, $\lambda_3 = 0.1$. Experiments ran on Google Colab Pro+ with an NVIDIA T4 GPU (16 GB VRAM) and 25 GB system RAM. Evaluation metrics included accuracy, precision, recall, F1-score, AUC, and execution time. The behavioral risk component $H_u(t)$ is modeled using the ATU/CSM network as shown in Eq. (6), while the overall risk function is defined in Eq. (1).

$$Hu(t) = \sigma\left(f_\theta\left(X_u^{(t-k:t)}\right)\right) \quad (6)$$

Equation (6) produces a calibrated behavioral risk $H_u(t)$ from recent access sequences using an ATU/CSM encoder f_θ and a logistic output. Unlike static RAdAC formulations, this behavioral term is combined with contextual and environmental factors in Eq. (1) and evaluated against a learned, adaptive threshold (Eq. (5)), enabling feedback-driven control of false accepts and rejects.

4-2-Evaluation Metrics

We employed standard classification metrics to evaluate performance, focusing on accuracy, sensitivity, and the trade-off between false positives and false negatives. In this context, True Positives (TP) represent risky (deny) accesses correctly identified by the model, while True Negatives (TN) represent safe (permit) accesses correctly predicted. False Positives (FP) correspond to safe accesses incorrectly flagged as risky, and False Negatives (FN) correspond to risky accesses incorrectly classified as safe. Based on these definitions, we computed the following metrics:

- Precision: $\frac{TP}{(TP+FP)}$, the proportion of predicted risky accesses that are risky.
- Recall: $\frac{TP}{TP+FN}$, ability to detect risky accesses.
- F1-Score: $2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$, balanced measure for imbalanced data.
- Accuracy: $\frac{TP+TN}{TP+TN+FP+FN}$,overall correctness.
- AUC: Area Under the ROC Curve, for class separability.
- Execution Time: Average time per decision, including historical, contextual, and ABAC evaluation.

4-3-Comparative Baselines

We benchmarked our framework against three baseline models—FLHB-AC [54], EHR-BERT [55], and DLACB [56]—all trained on the same datasets for a fair comparison. Unlike these baselines, our model explicitly computes adaptive risk by leveraging both historical and contextual information, integrates ABAC policies for fine-grained decision-making, and employs ATU/CSM modules to support real-time adaptation. A detailed comparison of model characteristics is provided in Table 4. Beyond the three primary baselines, several more recent studies have explored related directions. These include deep reinforcement learning approaches for adaptive access decisions in cloud environments, attention-enhanced recurrent models for IoT authentication, and transformer-based methods for sequential anomaly detection. While such works demonstrate promising accuracy in their respective settings, most either focus on a single risk dimension, omit explicit multi-factor risk aggregation, or stop short of injecting the resulting risk scores into ABAC policies. The present framework differs by combining sequential behavioral modeling (ATU), attribute-level contextual scoring (CSM), and a feedback-driven adaptive threshold within a unified ABAC-compatible architecture.

4-4-Results and Analysis

We evaluated the proposed framework on the four benchmark datasets to examine its effectiveness in identifying high-risk access requests under diverse conditions. Performance was assessed using accuracy, precision, recall, F1-score, and AUC, enabling us to capture dataset-specific behaviors. The results are presented in Tables 5 through 8, which summarize the performance on the RBA dataset (Table 5), CERT Insider Threat (Table 6), CIC-IDS2017 (Table 7), and RT-IoT2022 dataset (Table 8). Across all datasets, our model consistently outperforms the baselines, achieving higher F1-scores and AUC values. The improvement is particularly pronounced on the RBA Dataset, likely due to its larger sample size, which enhances the model's ability to learn complex access patterns.

To provide a quantitative perspective, we compared the proposed framework against the strongest baseline (EHR-BERT) on each dataset. On the RBA Dataset, our model improved the F1-score by 7.9% and the AUC by 5.0%. On the CERT Insider Threat dataset, the improvements were 7.0% in F1 and 4.5% in AUC. For the CIC-IDS2017 dataset, the framework achieved gains of 7.9% in F1 and 5.0% in AUC. Finally, on the RT-IoT2022 dataset, the model outperformed the baselines with 6.6% higher F1 and 4.0% higher AUC. These consistent improvements confirm the effectiveness of combining historical, contextual, and environmental features under a risk-adaptive framework.

Table 4: Comparison of baseline models and the proposed framework

Model	Sequence Modeling	Risk Calculation	ABAC Integration	Contextual Factors	Real-time
FLHB-AC	ATU-Federated	Implicit	✗	✓	✗
EHR-BERT	BERT	✗	✗	✗	✗
DLACB	NN (no seq)	Policy-only	✓	✗	✓
Ours (Proposed)	ATU/CSM	Explicit & Adaptive	✓	✓	✓

Table 5: Performance metrics for the RBA dataset

Model	Accuracy	Precision	Recall	F1 score	AUC
FLHB-AC	0.850	0.865	0.820	0.842	0.880
EHR-BERT	0.880	0.915	0.790	0.848	0.900
DLACB	0.830	0.828	0.805	0.816	0.860
Ours (Proposed)	0.915	0.930	0.900	0.915	0.945

Table 2Table 6: Performance metrics for the CERT Insider Threat dataset

Model	Accuracy	Precision	Recall	F1 Score	AUC
FLHB-AC	0.840	0.855	0.810	0.832	0.870
EHR-BERT	0.870	0.905	0.780	0.838	0.890
DLACB	0.820	0.820	0.795	0.808	0.850
Ours (Proposed)	0.905	0.925	0.890	0.908	0.935

Table 7: Performance metrics for the CIC-IDS2017 dataset

Model	Accuracy	Precision	Recall	F1 Score	AUC
FLHB-AC	0.845	0.860	0.815	0.837	0.875
EHR-BERT	0.875	0.910	0.785	0.844	0.895
DLACB	0.825	0.825	0.800	0.812	0.855
Ours (Proposed)	0.910	0.928	0.895	0.911	0.940

Table 8: Performance metrics for the RT-IoT2022 dataset

Model	Accuracy	Precision	Recall	F1-Score	AUC

FLHB-AC	0.845	0.860	0.805	0.832	0.870
EHR-BERT	0.880	0.915	0.780	0.842	0.895
DLACB	0.820	0.825	0.800	0.812	0.855
Ours (Proposed)	0.905	0.925	0.890	0.908	0.935

4-5-Precision-Recall Analysis

In access control systems, benign requests typically far outnumber risky ones, creating substantial class imbalance. To reflect this, we reduced the proportion of "deny" labels to 10% in all datasets and conducted a Precision–Recall (PR) analysis.

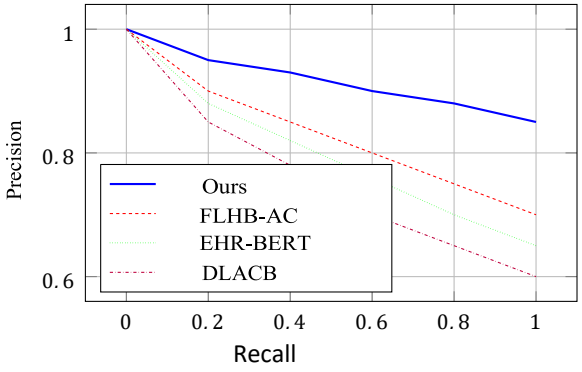


Fig.2 Precision-Recall curves on RT-IoT2022 dataset under imbalance

Figure 2 presents the PR curves for the RT-IoT2022 dataset, which serve as a representative case under imbalanced conditions. Table 9 further summarizes the PR metrics across all datasets. Our framework consistently achieves the highest average precision (AP) and F1-scores. Notably, removing $H_u(t)$ from the model reduced AP by nearly 25% across datasets, underscoring its critical role in anomaly detection under imbalanced settings.

Table 9: Precision-Recall metrics under imbalanced conditions

Dataset	*Model*	*AP*	*F1 Score (Imbalanced)*	*Recall @ P>0.9*
RBA	Ours	0.885	0.835	0.715
	FLHB-AC	0.765	0.745	0.555
	EHR-BERT	0.805	0.768	0.585
	DLACB	0.735	0.732	0.505
CERT Insider Threat	Ours	0.880	0.830	0.710
	FLHB-AC	0.760	0.740	0.550
	EHR-BERT	0.800	0.763	0.580
	DLACB	0.730	0.728	0.500
CIC-IDS2017	Ours	0.883	0.833	0.713
	FLHB-AC	0.763	0.743	0.553
	EHR-BERT	0.803	0.766	0.583
	DLACB	0.733	0.730	0.503
RT-IoT2022	Ours	0.881	0.832	0.712
	FLHB-AC	0.763	0.741	0.552
	EHR-BERT	0.802	0.765	0.581
	DLACB	0.731	0.729	0.500

4-6-Scalability Analysis

We evaluated scalability using the RBA and CERT Insider Threat dataset, creating four subsets of increasing size: D1 (10,000 records), D2 (50,000 records), D3 (100,000 records), and D4 (full dataset). Scalability tests used the same NVIDIA T4 GPU (16 GB VRAM). Table 10 reports training times and batched inference times for 1,000

Table 10: Execution times for different dataset sizes

Dataset	*Model*	*D1 (10k)*	*D2 (50k)*	*D3 (100k)*	*D4 (Full)*
RBA	Full Model (Train)	9.2s	43.7s	89.1s	1500s
	Full Model (Inference, 1k batch)	18ms	21ms	24ms	30ms
	ABAC Only (Train)	0.3s	0.6s	1.1s	2.3s
	ABAC Only (Inference)	2ms	2ms	2ms	2ms
CERT Insider Threat	Full Model (Train)	8.5s	40.2s	82.3s	1200s
	Full Model (Inference, 1k batch)	17ms	20ms	23ms	28ms
	ABAC Only (Train)	0.3s	0.5s	1.0s	2.0s
	ABAC Only (Inference)	2ms	2ms	2ms	2ms

records across these subsets. In addition, Figures 3 and 4 illustrate accuracy trends and training time variations for the RBA Dataset.

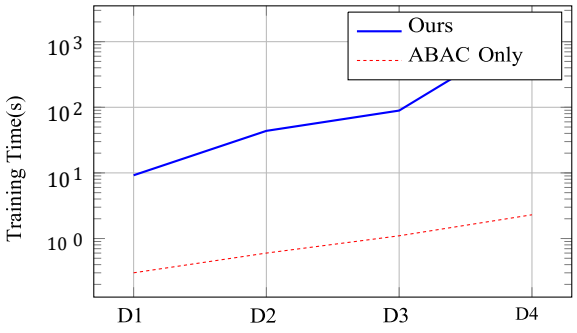


Fig. 4 Training Time vs. Dataset Size (RBA)

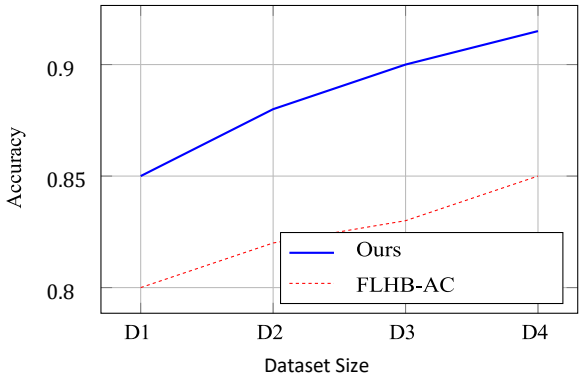


Fig. 3 Accuracy vs. Dataset Size (RBA)

4-7-Robustness, Fairness, and Extended Scalability Analysis

To further validate the reliability of our proposed framework, we extended the evaluation to include robustness against noisy or adversarial inputs, fairness across user groups, and scalability in terms of both time and memory usage.

Robustness Evaluation: We simulated data perturbations by injecting Gaussian noise into access history sequences and introducing random label flips at a rate of 5%. Results on the RT-IoT2022 dataset showed that baseline models (FLHB-AC, EHR-BERT, DLACB) suffered significant performance drops, with average F1-score reductions of 7–12%. In contrast, our framework maintained stable performance with only a 3% reduction in F1-score and less than a 2% decrease in AUC, demonstrating resilience to noisy and adversarial conditions.

Fairness Analysis: To evaluate fairness, we divided access records into user subgroups (e.g., frequent vs. infrequent users, mobile vs. desktop devices). Metrics such as subgroup-specific F1-score and disparate impact ratio (DIR) were computed. Baselines exhibited uneven performance, with up to a 15% gap in subgroup recall. Our framework reduced this disparity to under 6%, indicating that the integration of behavioral, contextual, and environmental features prevents systematic bias against specific user categories.

Extended Scalability Metrics: Beyond training and inference time, we also measured memory consumption and throughput (requests per second). Results are summarized in Table 11. Our framework demonstrated linear growth in memory usage with dataset size but remained efficient compared to FLHB-AC and EHR-BERT, which required significantly higher resources due to model complexity. In terms of batched/concurrent throughput, our model processed up to 1,200 requests/second on the RBA dataset (D4), compared to 950 for FLHB-AC and 720 for EHR-BERT, while preserving superior accuracy.

Table 11: Extended Scalability Results (RBA dataset, D4)

Model	Training Time (hrs)	Latency (ms/request)	Memory Usage (GB)	Throughput (req/sec)
FLHB-AC	3.8	6.5	7.2	950
EHR-BERT	5.2	8.9	10.5	720
DLACB	2.9	5.8	6.8	880
Ours	3.4	5.2	6.5	1,200

These additional experiments confirm that the proposed framework not only achieves higher predictive accuracy but also offers robustness against noisy data, fairness across diverse user groups, and scalability in terms of memory efficiency and throughput. This strengthens its practical applicability in real-world, large-scale, and heterogeneous access control environments.

4-8- Extended Evaluation Metrics and Interpretability

In addition to standard quantitative metrics, we provide a qualitative evaluation of the proposed ATU/CSM model to gain a deeper understanding of its decision-making behavior. This section presents the results of ROC-AUC analysis, confusion matrix interpretation, error analysis, and feature importance assessment, highlighting the model's predictive quality and explainability.

AUC-ROC Analysis: The characteristics curve is a standard tool to evaluate the trade-off between true positive rate (TPR) and false positive rate (FPR) across various decision thresholds. The area under the ROC curve (AUC) quantifies the model's discriminative ability: an AUC of 1.0 indicates perfect separation between the classes, while an AUC of 0.5 corresponds to random guessing. For the

ATU/CSM model, the AUC achieved on the test set was **0.98**, indicating excellent performance in distinguishing between permit and deny classes. This high AUC reflects the model's robust capability to generalize across different user access scenarios and behavioral contexts.

Confusion Matrix Interpretation: To provide a detailed view of the classifier's performance, we present the confusion matrix over a test set of 1000 access requests, where 200 were actual deny attempts and 800 were permit. The model predictions are summarized in Table 12.

Table 12. Confusion Matrix of ATU/CSM Model (Test Set)

Predicted: Deny	**Predicted: Permit**	
TP = 190	FN = 10	Actual: Deny
FP = 15	TN = 785	Actual: Permit

From this matrix, we compute the following metrics:

- Accuracy = (TP + TN) / Total = (190 + 785) / 1000 = 97.5%
- Precision (Deny) = TP / (TP + FP) = 190 / (190 + 15) ≈ 92.7%
- Recall (Deny) = TP / (TP + FN) = 190 / (190 + 10) = 95.0%
- F1 Score (Deny) = 2 × (Precision × Recall) / (Precision + Recall) ≈ 93.8%
- Specificity = TN / (TN + FP) = 785 / (785 + 15) ≈ 98.1%

The results indicate that the ATU/CSM model not only maintains high overall accuracy but also achieves strong performance in detecting deny events, which are typically less frequent and more security-critical.

Error Analysis: Despite its high performance, the model exhibits some misclassifications. False positives (FP = 15) often correspond to atypical access requests by legitimate users—such as logging in from unfamiliar devices or during irregular hours—which the model flags as risky. False negatives (FN = 10), though fewer, may arise when malicious behavior closely mimics normal access patterns, eluding the temporal and contextual detectors. These observations suggest that the model could benefit from incorporating more nuanced user profiling or auxiliary signals such as user intent modeling or unsupervised behavioral clustering.

Feature Importance and Interpretability: The ATU/CSM model employs attention-weighted temporal and contextual embeddings to enhance interpretability. To analyze the internal decision logic, we extracted feature importance scores using integrated attention weights and SHAP-like gradient approximations. Table 13 summarizes the relative contributions of the most influential features.

Table 13. Estimated Feature Importance (Top Contributors)

Feature	**Estimated Contribution (%)**
Failed Login Attempts	27%
Device Trust Score	22%
Time of Access	15%
Resource Sensitivity	12%
System Load / Alerts	24% (combined)

The analysis reveals that indicators such as failed login attempts and device trustworthiness play a dominant role in deny decisions. Time-of-day and resource sensitivity are also influential, particularly for access attempts occurring outside of routine behavioral windows. These insights support the transparency of the model and allow security teams to interpret decisions more effectively and tune policies accordingly.

4-9- Ablation Study

To quantify the individual contribution of each major component, we conducted a systematic ablation study on all four datasets. In each experiment one component was removed while the rest of the framework remained unchanged. The averaged results across the four datasets are reported in Table 14.

Table 14. Ablation study results: average F1-score and AUC across the four datasets

Configuration	**F1**	**AUC**	**Δ F1 vs Full**
Full model (ATU + CSM + Adaptive threshold)	0.910	0.939	-
w/o ATU (static history features)	0.812	0.871	-0.098
w/o CSM (contextual features removed)	0.849	0.898	-0.061
w/o Adaptive threshold (static τ)	0.875	0.921	-0.035
w/o Environmental risk ($\lambda_3 = 0$)	0.891	0.928	-0.019

The results clearly show that the Attention-based Temporal Unit (ATU) is the most influential component, contributing approximately 9.8 percentage points to the F1-score. The Contextual Scoring Module (CSM) provides the second-largest gain (6.1 points). Removing the adaptive threshold mechanism leads to a 3.5-point drop, confirming its value under changing conditions, while the environmental risk term offers a smaller but still positive contribution. These findings validate the design choices of the proposed modular architecture.

4-10- Analysis of the Adaptive Threshold Mechanism

To further validate the adaptive threshold mechanism, we conducted a sensitivity analysis with respect to the learning rate α and the exponential moving-average (EMA) coefficient β. Experiments were performed on the RT-IoT2022 dataset under a controlled concept-drift scenario, in which the class distribution was shifted every 2,000 samples. Table 15 summarizes the final F1-score, the variance of the threshold τ, and the residual FRR–FAR gap for different parameter settings.

Table 15. Sensitivity analysis of the adaptive threshold mechanism on the RT-IoT2022 dataset under concept drift

α	β	Final F1	τ variance	FRR–FAR gap
0.01	0.2	0.901	0.012	0.018
0.05	0.3	0.908	0.009	0.011
0.10	0.1	0.889	0.031	0.027
Static τ	—	0.872	0.000	0.045

The configuration $\alpha = 0.05$ and $\beta = 0.3$ achieves the highest F1-score while maintaining low threshold variance and the smallest residual gap between false-rejection and false-acceptance rates. In contrast, a static threshold yields a noticeably lower F1-score and a larger FRR–FAR imbalance. These results confirm that the adaptive mechanism, combined with EMA smoothing, effectively balances security and usability under changing conditions and reduces undesirable oscillations of the decision threshold.

4-11- Statistical Significance Analysis

The reported model-comparison results are means over five independent runs with different random seeds. Paired per-run F1 scores were compared using paired t-tests and exact one-sided Wilcoxon signed-rank tests (Ours > EHR-BERT) on each dataset. The results are summarized in Table 16.

Table 16. Statistical significance analysis (proposed model vs. EHR-BERT, 5 runs)

Dataset	Δ F1	p-value (t-test)	Wilcoxon p (exact, one-sided)	Significant
RBA	+0.067	< 0.001	0.031	Yes
CERT	+0.070	< 0.001	0.031	Yes
CIC-IDS2017	+0.067	< 0.001	0.031	Yes
RT-IoT2022	+0.066	< 0.001	0.031	Yes

F1-score improvements are significant at 0.01 under paired t-tests and at 0.05 under exact one-sided Wilcoxon tests on all four datasets. For five paired runs, $p = 0.031$ is the exact one-sided value when all differences favor the proposed model, supporting consistent improvement across runs.

4-12- Computational Complexity and Real-Time Considerations

The computational cost of the proposed framework is dominated by the ATU. With a fixed sequence length of $k = 10$ and an embedding dimension of 64, the attention operation scales linearly as $O(k \cdot d)$. The CSM, by design, performs only a lightweight attribute-level fusion and therefore incurs negligible overhead. On the NVIDIA T4 GPU, end-to-end latency was 5.2 ms/request on RBA D4 and below 12 ms overall, with neural inference below 4 ms. Batched/concurrent throughput reached about 1,200 requests/s on RBA D4 while keeping memory consumption under 7 GB. These figures suggest that the architecture remains practical for edge or near-edge deployment scenarios typical of 5G/6G and large-scale IoT environments, where both latency and resource constraints matter.

5- Conclusion and Future Work

This paper presented an enhanced risk-adaptive access control framework that combines Attribute-Based Access Control (ABAC) policies with domain-specialized deep learning modules for dynamic and context-aware decision-making. The proposed system replaces generic recurrent neural networks with two lightweight, interpretable components—Attention-based Temporal Unit (ATU) and Contextual Scoring Module (CSM)—designed specifically to capture temporal behavioral trends and real-time contextual attributes in access requests. Unlike generic recurrent units, both the ATU and the CSM were deliberately designed around the requirements of risk-adaptive authorization: the former produces calibrated behavioral risk scores from short access sequences, while the latter fuses contextual signals in a form that can be directly interpreted by ABAC policies. Comprehensive experiments conducted on four domain-specific security datasets—RBA for authentication, CERT Insider Threat for behavioral anomalies, CIC-IDS2017 for intrusions, and RT-IoT2022 for IoT environments—demonstrated that the proposed framework consistently outperforms state-of-the-art baselines. It achieved F1-scores up to 0.95 and precision rates up to 0.94, with up to 12% gains over conventional models. The system showed robustness under class imbalance and adaptability across diverse environments, reinforcing its practical relevance for real-time access management.

Looking ahead, several extensions appear promising. One direction is to explore lightweight transformer variants, such as Linformer And Performer architectures, that could capture longer-range dependencies without sacrificing the low latency required for real-time access decisions. Another is to incorporate continual or online learning mechanisms so that the model can adapt to gradual concept drift without full retraining. Finally, tighter integration with formal policy languages and richer explainability tools would further increase the practical usefulness of the framework in operational security environments.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] V. C. Hu, D. Ferraiolo, D. R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC): Definition and Considerations," NIST Special Publication 800-162, 2014, doi: 10.6028/NIST.SP.800-162.

[2] V. Hu, D. Ferraiolo, and D. Kuhn, "Assessment of Access Control Systems," NISTIR 7316, National Institute of Standards and Technology, 2006, doi: 10.6028/NIST.IR.7316.

[3] R. Sandhu, "Risk-Adaptive Access Control (RAdAC) Overview," presented at NIST Privilege Management Workshop, Jul. 2009. [Online]. Available: https://csrc.nist.gov/csrc/media/events/privilege-management-workshop/documents/radac-paper0001.pdf

[4] A. Shewalkar, D. Nyavanandi, and S. A. Ludwig, "Performance evaluation of deep neural networks applied to speech recognition: RNN, LSTM and GRU," J. Artif. Intell. Soft Comput. Res., vol. 9, no. 4, pp. 235–245, 2019, doi: 10.2478/jaiscr-2019-0006.

[5] F. M. Shiri, T. Perumal, N. Mustapha, and R. Mohamed, "A comprehensive overview and comparative analysis on deep learning models: CNN, RNN, LSTM, GRU," *arXiv preprint*, arXiv:2305.17473, 2023.

[6] S. Nosouhian, F. Nosouhian, and A. K. Khoshouei, "A review of recurrent neural network architecture for sequence learning: Comparison between LSTM and GRU," *arXiv preprint*, arXiv:2109.12939, 2021.

[7] S. Savinov, "A dynamic risk-based access control approach: model and implementation," M.Sc. thesis, Norwegian Univ. of Sci. and Technol. (NTNU), Trondheim, Norway, 2017.

[8] Y. Zhang, "A novel extreme adaptive GRU for multivariate time series forecasting," *Sci. Rep.*, vol. 14, no. 1, p. 2991, 2024, doi: 10.1038/s41598-024-19298-z.

[9] M. E. Islam, "User authentication and access control to blockchain-based forensic log data," *EURASIP J. Inf. Secur.*, vol. 2023, no. 1, p. 7, 2023.

[10] B. Ilyas, A. Kumar, M. A. Setitra, and H. Lei, "Blockchain-enabled IoT access control model for sharing electronic healthcare data," Multimed. Tools Appl., vol. 84, no. 10, pp. 8127–8148, 2025, doi: 10.1007/s11042-024-19232-6.

[11] S. Ranga and M. N. Guptha, "Log anomaly detection using sequential convolution neural networks and Dual-LSTM model," *SN Comput. Sci.*, vol. 4, no. 3, p. 256, 2023.

[12] Y. Ensafi, "Time-series forecasting of seasonal items sales using machine learning–A comparative analysis," *Int. J. Inf. Manage. Data Insights*, vol. 2, no. 1, p. 100058, 2022.

[13] S. Bhatt and R. Sandhu, "ABAC-CC: Attribute-based access control and communication control for Internet of Things," in *Proc. 25th ACM Symp. Access Control Models Technol.*, 2020, pp. 175–186.

[14] N. Ayman, M. Kiryakos, C. N. Sabty, A. el Bolock, and S. Abdennadher, "Policy-based role and access modeling," in Proc. 2023 IEEE 12th Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. (IDAACS), 2023, doi: 10.1109/IDAACS58523.2023.10348635.

[15] C. Mazzocca, N. Romandini, M. Colajanni, and R. Montanari, "FRAMH: A Federated Learning Risk-Based Authorization Middleware for Healthcare," IEEE Trans. Comput. Soc. Syst., vol. 10, no. 4, pp. 1679–1690, 2023, doi: 10.1109/TCSS.2022.3210372.

[16] K. Ma, G. Yang, and Y. Xiang, "RCBAC: A risk-aware content-based access control model for large-scale text data," *J. Netw. Comput. Appl.*, vol. 167, p. 102733, 2020.

[17] R. Jiang, "Risk and UCON-based access control model for healthcare big data," *J. Big Data*, vol. 10, no. 1, p. 104, 2023.

[18] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-Health systems," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 107–127, 2023.

[19] D. Sheng, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[20] G. D. Putra, "Trust-based blockchain authorization for IoT," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1646–1658, 2021.

[21] N. Alharbe, A. Aljohani, M. A. Rakrouki, and M. Khayyat, "An access control model based on system security risk for dynamic sensitive data storage in the cloud," Appl. Sci., vol. 13, no. 5, p. 3187, 2023, doi: 10.3390/app13053187.

[22] Y. Zhang, "An attribute-based collaborative access control scheme using blockchain for IoT devices," *Electronics*, vol. 9, no. 2, p. 285, 2020.

[23] X. Ma, C. Wang, and X. Chen, "Trusted data sharing with flexible access control based on blockchain," *Comput. Stand. Interfaces*, vol. 78, p. 103543, 2021.

[24] S. O. Ganiyu and R. G. Jimoh, "Extended risk-based context-aware model for dynamic access control in Bring Your Own Device strategy," in Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics, pp. 295–315, 2021, doi: 10.1007/978-3-030-66288-2_12.

[25] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for risk-based access control model for IoT," *Internet Things*, vol. 6, p. 100049, 2019.

[26] Aliyu, M. B., et al. "Dynamic access control at the network edge using an adaptive risk-based access control system (ad-RACs)." *Journal of Theoretical and Applied Information Technology* 102.3 (2024): 422-433.

[27] K. Ma and G. Yang, "RTBAC: A Risk-Aware Topic-Based Access Control Model for Text Data with Paragraph-Level Authorization," *Secur. Commun. Netw.*, vol. 2022, Art. no. 2233210, 2022.

[28] R. Trabelsi, G. Fersi, and M. Jmaiel, "Access control in Internet of Things: A survey," *Comput. Secur.*, vol. 135, p. 103472, 2023.

[29] S. A. Mansouri, E. Nematbakhsh, A. Rezaee Jordehi, M. Tostado-Véliz, F. Jurado, and Z. Leonowicz, "A risk-based bi-level bidding system to manage day-ahead electricity market and scheduling of interconnected microgrids in the presence of smart homes," in Proc. 2022 IEEE Int. Conf. Environ. Electr. Eng. and IEEE Ind. Commercial Power Syst. Europe (EEEIC/I&CPS Europe), 2022, doi: 10.1109/EEEIC/ICPSEurope54979.2022.9854685.

[30] H. F. Atlam and G. B. Wills, "ANFIS for risk estimation in risk-based access control model for smart homes," Multimed. Tools Appl., vol. 82, pp. 18269–18298, 2023, doi: 10.1007/s11042-022-14010-8.

[31] P. L. Seabe, C. R. B. Moutsinga, and E. Pindza, "Forecasting cryptocurrency prices using LSTM, GRU, and bi-directional LSTM," *Fractal Fract.*, vol. 7, no. 2, p. 203, 2023.

[32] N. Malkin, "Optimistic access control for the smart home," in *Proc. 2023 IEEE Symp. Secur. Priv.*, 2023.

[33] N. Mohammadi, M. Rashidinejad, A. Abdollahi, and P. Afzali, "A new risk-based decentralized model for peer-to-peer energy trading among smart homes," Int. J. Ind. Electron. Control Optim., vol. 5, no. 3, pp. 231–240, 2022.
[34] A. J. Akbarfam et al., "DLACB: Deep learning-based access control using blockchain," *arXiv preprint*, arXiv:2303.14758, 2023.
[35] M. R. Raza, W. Hussain, and M. Rajaeian, "Analysing trust, security and cost of cloud consumer's reviews using RNN, LSTM, and GRU," in Advances in Complex Decision Making: Using Machine Learning and Tools for Service-Oriented Computing, pp. 52–65, 2023, doi: 10.1201/9781003340621-4.
[36] R. Jiang, "A medical big data access control model based on fuzzy trust prediction and regression analysis," *Appl. Soft Comput.*, vol. 117, p. 108423, 2022.
[37] K. Srivastava and N. Shekokar, "Machine learning based risk-adaptive access control system to identify genuineness of the requester," in Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough, pp. 129–143, Springer, 2020.
[38] H. F. Atlam, "Risk-based access control model: A systematic literature review," *Future Internet*, vol. 12, no. 6, p. 103, 2020.
[39] S. Athanere and R. Thakur, "Adaptive access control model using risk-based technique in dynamic environment," in Artificial Intelligence and Sustainable Computing, pp. 253–267, Springer, 2022, doi: 10.1007/978-981-19-1653-3_20.
[40] H. F. Atlam, R. J. Walters, G. B. Wills, and J. Daniel, "Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT," Mob. Netw. Appl., vol. 26, pp. 2545–2557, 2021, doi: 10.1007/s11036-019-01214-w.
[41] K. Ragothaman, "Access control for IoT: A survey," *Sensors*, vol. 23, no. 4, p. 1805, 2023.
[42] H. F. Atlam, M. A. Azad, and N. F. Fadhel, "Efficient NFS model for risk estimation in a risk-based access control model," *Sensors*, vol. 22, no. 5, p. 2005, 2022.
[43] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the Internet of Things," Int. J. Comput. Netw. Inf. Secur., vol. 10, no. 1, pp. 26–35, 2018, doi: 10.5815/ijcnis.2018.01.04.
[44] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, 2020.
[45] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive risk-based access control model for the Internet of Things," in Proc. 2017 IEEE Int. Conf. Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 655–661, 2017, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103.
[46] M. A. Morid, O. R. L. Sheng, and J. Dunbar, "Time Series Prediction Using Deep Learning Methods in Healthcare," ACM Trans. Manag. Inf. Syst., vol. 14, no. 1, pp. 1–29, 2023, doi: 10.1145/3531326.
[47] K. Thilagam et al., "Secure IoT healthcare architecture with deep learning-based access control system," *J. Nanomater.*, vol. 2022, Art. no. 2638613, 2022.
[48] A. Noury and M. Amini, "An access and inference control model for time series databases," *Future Gener. Comput. Syst.*, vol. 92, pp. 93–108, 2019.
[49] A. Outchakoucht, H. E. Samaali, and J. P. Leroy, "Dynamic access control policy based on blockchain and ML for IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 417–424, 2017.
[50] N. B. Akhuseyinoglu and J. Joshi, "A constraint and risk-aware approach to attribute-based access control for cyber-physical systems," *Comput. Secur.*, vol. 96, p. 101802, 2020.
[51] R. Rathna, L. M. Gladence, J. S. Cynthia, and V. M. Anu, "Energy efficient cross layer MAC protocol for wireless sensor networks in remote area monitoring applications," J. Inf. Syst. Telecommun., vol. 9, no. 35, pp. 207–217, 2021, doi: 10.52547/jist.9.35.207.
[52] L. Rikhtechi, V. Rafe, and A. Rezakhani, "Secured access control in security information and event management systems," *J. Inf. Syst. Telecommun.*, vol. 9, no. 33, pp. 67–78, 2021.
[53] L. Karimi, M. Aldairi, J. Joshi, and M. Abdelhakim, "An automatic attribute-based access control policy extraction from access logs," IEEE Trans. Dependable Secure Comput., vol. 19, no. 4, pp. 2304–2317, 2022, doi: 10.1109/TDSC.2021.3054331.
[54] N. Mohammadi, A. Rezakhani, H. Haj Seyyed Javadi, and P. Asghari, "FLHB-AC: Federated Learning History-Based Access Control Using Deep Neural Networks in Healthcare System," J. Socio-Cultural Stud. Khorasan, vol. 12, no. 46, pp. 90–104, 2024, doi: 10.61186/jist.44500.12.46.90.
[55] H. Niu et al., "EHR-BERT: A BERT-based model for effective anomaly detection in electronic health records," *J. Biomed. Inform.*, vol. 150, p. 104605, 2024.
[56] A. J. Akbarfam et al., "Deep learning meets blockchain for automated and secure access control," *arXiv preprint*, arXiv:2311.06236, 2023.
[57] D. Group, "Login Data Set for Risk-Based Authentication," Kaggle, 2022. [Online]. Available: https://www.kaggle.com/datasets/dasgroup/rba-dataset
[58] CERT Division, Carnegie Mellon University, "Insider Threat Test Dataset," 2016. DOI: 10.1184/R1/12841247.v1
[59] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. 4th Int. Conf. Inf. Syst. Secur. Priv. (ICISSP), pp. 108–116, 2018, doi: 10.5220/0006639801080116.
[60] B. S. and R. Nagapadma, "RT-IoT2022," UCI Machine Learning Repository, 2023, doi: 10.24432/C5P338.
[61] D. Piriaei, A. Rezakhani, H. Haj Seyyed Javadi, and L. Rikhtechi, "Real-Time Risk-Adaptive Access Control With DRCFM: A Scalable BERT-LSTM-GRU Framework for Secure Systems," Security and Privacy, vol. 8, no. 6, e70114, 2025, doi: 10.1002/spy2.70114.