ISSN: 3068-1774
Research Article
Journal of Medical Images and Medical Education Research

Dynamic Access Decision Scoring: An Adaptive Framework for Healthcare Data Security and Privacy

Yoram Segal [1*], **& Adi Hod** [2]

[1]*Chief AI Officer (CAIO), 7 Derech Menachem Begin st. Ramat Gan, IL, ISRAEL.*
[2]*CSO Velotix Inc. 1209 Orange St, Wilmington DE 19801, USA.*

[*]**Corresponding author:** Yoram Segal, 1Chief AI Officer (CAIO), 7 Derech Menachem Begin st. Ramat Gan, IL, ISRAEL.

Submitted: 10 April 2025 **Accepted:** 16 April 2025 **Published:** 22 April 2025

https://doi.org/10.63620/MKJMMRR.2025.1008

Citation: *Segal, Y., & Hod, A. (2025). Dynamic Access Decision Scoring: An Adaptive Framework for Healthcare Data Security and Privacy. J of Med Ima & Med Edu Res 2(2), 01-09.*

Abstract

This paper introduces a novel Dynamic Access Decision Scoring (ADS) framework that 1 integrates cognitive computing and big data to address emerging challenges in controlling access 2 to healthcare data systems. Traditional rule-based access control mechanisms lack the cognitive 3 capabilities to process dynamic security requirements, creating vulnerabilities when managing large-4 scale electronic health records (EHRs). Our framework leverages cognitive computing by combining 5 machine learning algorithms, behavioral pattern analysis, and real-time data analytics to create an 6 intelligent security system that safeguards sensitive medical data while maintaining computational 7 efficiency. The core innovation lies in developing a cognitive mathematical template that data 8 scientists and researchers can adapt through deep learning and analytical processing.

The framework 9 introduces a modular formula as an adaptive cognitive pattern, incorporating four computational 10 elements: machine learning predictions, historical pattern recognition, risk analytics, and temporal 11 context processing. Each element employs cognitive algorithms that security architects can calibrate 12 within their specific data ecosystems. The framework's primary contribution demonstrates how 13 cognitive probabilistic approaches can dynamically adapt to complex healthcare environments. 14 This research advances big data security by establishing a cognitive computing foundation for 15 making access control decisions, effectively bridging theoretical data models with practical machine 16 intelligence implementation in healthcare information systems.

Keywords: Access Control; Healthcare Security; Dynamic Decision Scoring; HIPAA Compliance; Machine Learning; Risk Assessment; Data Privacy

Introduction

In today's data-driven world, organizations face the critical challenge of controlling access to their valuable electronic resources while adhering to strict regulations and policies. Chief Data Officers (CDOs) ensure that only authorized users can perform specific actions on sensitive data, including database access, file manipulation, or system-level operations. Traditional rule-based engines have been the predominant solution for enforcing access control policies. These engines operate on a deterministic "if-then-else" principle, where predefined rules dictate whether a request is granted or denied. However, this approach suffers from several inherent limitations. The complexity and incompleteness of rule sets make it virtually impossible to cover every possible scenario, as the real world is full of nuances and unexpected situations. The rigidity and inflexibility of these systems struggle to adapt to changing environments and dynamic requirements, often requiring constant rule updates that can be cumbersome and error-prone. Furthermore, to compensate for their inability to cover all cases, rule-based systems usually resort to overly restrictive policies, blocking access in situations that might be legitimate, thereby hindering productivity and collaboration within the organization. The increasing prevalence of data breaches, driven largely by careless or malicious insiders with legitimate access to sensitive information (approximately 63%), underscores the urgent need for more sophisticated approaches. This need is particularly crucial in healthcare settings, where the transition from paper-based protected health information Version April 9, 2025. (PHI) to electronic protected health information (ePHI) has created new vulnerabilities and security challenges. What's needed is a more continuous and adaptive approach to access control, one that can learn from past behavior, recognize patterns, and make informed decisions even in novel situations. By leveraging machine learning algorithms, we can create a dynamic authorization index that provides a real-time risk assessment for each access request. This index would be a composite score, weighing user identity, resource sensitivity, time of access, historical behavior, and current context.

With this dynamic index, organizations can define authorization thresholds that adapt to changing risk levels. For instance, the threshold could be raised during a suspected cyberattack, requiring a higher score to gain access. This flexibility allows for a more responsive and effective access control system mimicking human decision-making in access control, providing a high probability of correct authorization decisions in real time. This paper presents a comprehensive framework for Dynamic Access Decision Scor- ing (ADS), designed to overcome the limitations of traditional rule-based systems while enabling organizations to protect their valuable resources and foster a collaborative and productive environment. Our approach provides a robust solution for modern access control challenges through machine learning, behavioral analysis, and risk assessment.

Objective

The primary objective of this research is to develop a comprehensive and adaptive framework for Dynamic Access Decision Scoring (ADS) that addresses the fundamental limitations of traditional access control systems while meeting the unique security require-mints of healthcare environments. Through this framework, we aim to achieve multiple interconnected goals: From a security perspective, our objective is to create a dynamic authorization system that continuously evaluates access requests based on real-time risk assessment, moving beyond the rigid constraints of traditional rule-based approaches. The system must adapt to emerging threats while maintaining operational efficiency and ensuring legitimate access to critical healthcare data. We aim to develop a scoring mechanism for healthcare compliance that inherently aligns with regulatory requirements, particularly HIPAA and related healthcare privacy standards.

The system must provide granular control over protected health information (PHI) while maintaining detailed audit trails for compliance verification. Regarding technical implementation, we aim to establish a mathematical framework combining multiple risk factors into a unified scoring system. The Access Decision Score (ADS) must accurately reflect the risk level of each access request through the following formula: From an operational perspective, we seek to minimize disruption to clinical work- flows while maximizing security effectiveness. The system should identify and prevent unauthorized access attempts while facilitating necessary and legitimate access to patient information, particularly in time-critical healthcare scenarios.

The research also addresses the growing challenge of insider threats in healthcare organizations by incorporating behavioral analysis and pattern recognition into the scoring system. By analyzing historical access patterns and contextual information, the framework should be capable of identifying abnormal behavior that might indicate potential security risks. Ultimately, we aim to create a practical, implementable solution that healthcare or-ganizations can readily adopt to enhance their data security posture while maintaining operational efficiency and regulatory compliance. The framework should provide a foun-dation for future dynamic access control systems developments, particularly as healthcare technologies and security challenges evolve.

Literature Review

The evolution of access control mechanisms has seen a significant shift from traditional role-based approaches to more dynamic systems, driven by the need to address static model limitations in rapidly changing environments [1–3,3,4]. This transition has been particularly crucial in healthcare settings, where protecting electronic health records (EHRs demands sophisticated security measures while maintaining operational efficiency. Our Access Decision Scoring (ADS) system builds upon these advancements by introducing a machine-learning-driven, real-time scoring mechanism that provides a dynamic and context-sensitive evaluation of access requests [5–7].

The ADS system incorporates multiple machine learning models to evaluate access requests, extending beyond conventional approaches that rely primarily on real-time anomaly detection [8–10]. By employing a weighted composite score derived from multiple ML models, the system achieves a 30% reduction in false positives and a 25% decrease in unauthorized access incidents [11]. Unlike traditional implementations that use single-model approaches such as SVM, Random Forest, or Decision Trees, our system integrates various models within the ADS framework, allowing for adaptive weighing of different risk factors based on access request context [12–14]. This integration includes sophisticated risk coefficient matrices and temporal modifiers that ensure secure sharing of sensitive embeddings [15,16].

The mathematical foundation of our ADS model builds upon existing cryptographic techniques and risk coefficients, incorporating these mechanisms into a compre- hensive scoring formula. Drawing inspiration from mesh networks and Moving Target Defense techniques, our system employs a non-linear amplification function that responds dynamically to deviations from historical access patterns [17-19]. The integration of algebraic principles, similar to those used in elliptic curve cryptography, allows for fine-tuning of the risk sensitivity parameter, enabling nuanced risk evaluation that scales based on security needs [19].

Privacy considerations in healthcare access control rely on a continuous risk evaluation system that adapts to varying levels of data sensitivity and regulatory requirements across different jurisdictions [20–24]. The ADS system addresses the human factors gap in health-care data security by incorporating historical user behavior into the risk evaluation process [21]. This approach complements existing technologies like IoT, blockchain, and cloud computing [22] while advancing privacy-preserving access control models through the integration of attribute-based risk coefficient [22,23]s. The system addresses challenges in-tro-duced by AI and ML in healthcare through advanced encryption and temporal context modifiers [24].

The ADS system's ability to evaluate compliance risks continuously strengthens the integration of real-time risk assessment with regulatory compliance [25–29]. By lever-aging blockchain's decentralized architecture and incorporating gradient descent optimization for model weights , the system maintains real-time accuracy in assessing compliance-related risks. Temporal context modifiers dynamically adjust risk assessment based on real-time data, ensuring compliance with health and safety regulations as conditions evolve [27-29].

The ADS system advances beyond traditional access control models in clinical settings by incorporating a real-time risk assessment mechanism [30]. The system's temporal context modifier, inspired by Lagrange interpolation polynomials, adjusts access decision scores based on factors like time of day or specific emergencies. This approach surpasses the NdRAdAC framework by integrating historical pattern analysis for enhanced accuracy in emergency response scenarios [31,32]. The decentralized evaluation system leverages distributed machine learning models to analyze different aspects of access requests while maintaining alignment with formal verification processes, as demonstrated by the ANSI/INCTIS RBAC Reference Model [33, 34].

The ADS system represents a significant advancement in healthcare data security, providing an adaptive and context-aware solution that balances robust security measures with operational efficiency. By integrating machine learning, historical analysis, and real- 145time adaptability, the system offers a comprehensive approach to access control that meets 146 the dynamic demands of modern healthcare environments while ensuring compliance with 147 evolving privacy regulations.

Access Decision Scoring (ADS)

The Access Decision Scoring (ADS) formula evaluates whether a specific user (u) request (r) should be granted access to a specific resource (d). This is achieved by calculating the risk score SADS via the following function:

SADS = ADS(r, u, d)

Where:

- User attributes vector (u),
- Resource properties vector (d),
- Context of the access request vector (r),
- Historical patterns of the user's behavior matrix (B).

The system compares the computed ADS score (SADS) against a dynamic threshold (Th) that adapts to the organization's security state (e.g., normal state or under cyberattack).

ADS Preliminaries Preparations

Unified Dimensionality

All vectors representing the request (r), user attributes (u), and resource attributes (d)
must share the same dimensionality:
dim(r) = dim(u) = dim(d) = k,

Where K Is the Number of Components (Features) In Each Vector.

Normalization of Vectors

The Algorithm Normalizes All Vectors to The Unit Norm to Ensure Equal Contribution.

$$\|v\| = \sqrt{\sum_{i=1}^{n} v_i^2}, \quad v_{\text{normalized}} = \frac{v}{\|v\|}.$$

Categorical Data Transformation

Categorical data is converted into numerical form using one-hot encoding. For example, the selected "Admin" option out of the three categorical options {Admin, Group, Others} will be presented with one-hot encoding as follows:

One-hot("Admin") = [1, 0, 0].

Exclusion of Identifiers

The formula omits user ID and resource ID identifiers to evaluate a specific user-
resource pair.

ADS Key Components

Access Request (r)

The access request vector represents the dynamic attributes of the current request. For example:

r = [Normalized Time, Action, Device Type, Trust Level].

Example: At 21:36, the user requests printer access with a face recognition algorithm confidence level of only 0.35.

- Normalized Time: 0.89 (the number of minutes past midnight divided by the daily minutes)
- Action: [Update, Access, Delete] = One-hot(Access) = [0, 1, 0].
- Device Type: [PC, Room, Printer] = One-hot(Printer) = [0, 0, 1].
- Confidence Level: 0.35.

$$r = [0.89, \underline{0\,1\,0}, \underline{0\,0\,1}, 0.35] \Rightarrow r_{\text{normalized}} = \tilde{r} = [0.52, \underline{0.00, 0.59, 0.00,}\underline{0.00, 0.00, 0.59,} 0.21] \in \mathbb{R}^8$$

User Attributes (u)

The User Vector Represents Static Properties:

u = [Role, Clearance Level, Sensitivity Factor].

Example:

$$u = [0, 0, 1, 1, 0, 0, 0.49] \in \mathbb{R}^7$$

Resource Attributes (d)

The resource vector represents the static properties of the resource: d = [Sensitivity Level, Type, Location, Restrictions].
Example:

$$d = [0.83, 0, 1, 0, 0, 0, 1, 0, 0, 1] \in \mathbb{R}^{10}$$

Remark

In this example, the vector d has the largest dimension of 10. Therefore, the vectors r and u will be zero-padded to ensure that all vectors have a uniform dimension of 10.

ADS Formula main components
The definition of the ADS formula is as follows:

SADS = ADS(r, u, d) = ∑(αi Mi(r)) · eβH(r,B) · R(u, d) · T(c),

Where:
- Mi(r): Predictions from individual Machine Learning (ML) models.
- H(r, B): Historical similarity between current and past requests.
- R(u, d): Risk coefficient for the user-resource pair.
- T(c): Temporal context modifier.

Historical Similarity (H(r, B))
Construction of the Historical Matrix B
The system constructs the historical matrix B from a sequence of request vectorsr,
with each r forming a single row in B. Mathematically, B is defined as:

$$B = \begin{bmatrix} r_{t_0} \\ r_{t_1} \\ \vdots \\ r_{t_{n-1}} \end{bmatrix}$$

Where:
- B is the historical matrix.
- rti represents the request vector rat time ti.
- n is the matrix's total number of past requests.
-

Element-wise Representation
If each rti is a vector with k elements:

rti = [rti ,1, rti ,2, , rti ,k],

then B is constructed as:

$$B = \begin{bmatrix} r_{t_0,1} & r_{t_0,2} & \cdots & r_{t_0,k} \\ r_{t_1,1} & r_{t_1,2} & \cdots & r_{t_1,k} \\ \vdots & \vdots & \ddots & \vdots \\ r_{t_{n-1},1} & r_{t_{n-1},2} & \cdots & r_{t_{n-1},k} \end{bmatrix}$$

Size of B
If There Are N Historical Requests and Each Request Vector R Has K Elements, Then the Size of B is:

$$B \in \mathbb{R}^{n \times k}$$

Example
Suppose We Have Three Historical Requests:
rt0 = [0.89, 0.44, 0.35], rt1 = [0.57, 0.71, 0.49], rt2 = [0.83, 0.55, 0.33].

The Historical Matrix B is Constructed As

$$B = \begin{bmatrix} 0.89 & 0.44 & 0.35 \\ 0.57 & 0.71 & 0.49 \\ 0.83 & 0.55 & 0.33 \end{bmatrix}$$

H(r, B)
The Historical Similarity Compares R with All the Rows Ofb (Historical Requests):

$$H(r, B) = \frac{1}{n} \sum_{i=1}^{n} \frac{r \cdot B_i}{\|r\| \cdot \|B_i\|}.$$

The Weight Β Increases with The Number of Rows (N)
β = log(n + 1).

Risk Coefficient (R(u, d))
The system calculates the risk coefficient using the following formula:
R(u, d) = u . d.

Risk Coefficient Calculation
The Risk Coefficient, R(u, d), quantifies the inherent risk associated with granting access to a resource (d) by a specific user (u). This coefficient depends only on the user and resource attributes, as these are the primary factors in determining the baseline risk of an access request. It ignores the specific request vector (r) since r represents dynamic, situational attributes already accounted for in other components of the scoring process.

Motivation
The motivation for using R(u, d) is to establish a static yet contextually relevant measure of risk based on the user's identity, role, and trustworthiness (u), and the sensitivity, importance, or classification of the resource (d). This separation allows the system to independently assess the intrinsic risk associated with the user-resource pair without conflating it with transient factors.
R(u,d)Formula

$$R(u, d) = \sum_{i=1}^{n} u_i \cdot d_i$$

Where:
- •u=[u1,u2,...,un]: User attribute vector.
- •d=[d1,d2,...,dn]: Resource attribute vector.
- •n:Thenumberof attributes considered.

The risk coefficient is calculated as the dot product of the user vector (u) and the resource vector (d), which combines the corresponding attributes of the user and the resource to evaluate their overall interaction risk.

Importance and Determination of Vector Element Order The question of the order of elements in a vector is critical for calculations such as the scalar product between two vectors u and d, as the scalar product depends on the one-to-one correspondence between the elements of the vectors.

How to Determine the Order of Elements in a Vector? Adaptation to the Business or System Problem: The order of the elements in the vector u (user) and d (resource) is determined based on the specific application of the system. For example:

- If u represents user attributes such as security level, access type, and role, then d should be arranged to include corresponding characteristics of the resource that relate to these attributes (e.g., sensitivity level, required protection type, etc.).

Using a Predefined Convention: Any system that defines vectors of this type must establish a clear predefined convention for the order of elements. For instance:

- The first element always describes the security level.
- The second element always describes the access type.
- The third element describes another attribute, and so on.

Clear Documentation: Document the order of the elements in the vectors clearly in the system or algorithm documentation to prevent misunderstandings.

Solutions to the Problem

- Structural Alignment: Ensure that the order of the elements in the vectors is pre- aligned and consistently maintained across all calculations.
- Automatic Checks: Use functions or automated checks to verify that the order of the vectors matches before performing the computation.
- Using a Matrix: Instead of using separate vectors, define a matrix representing all the relationships between users and resources and perform a more general computation.

Example of Risk Coefficient Calculation

Given:

u = [0.71, 0, 0, 0.57, 0.49], d = [0.83, 0.55, 0.33, 0.55].

Normalize u:

$$\|u\| = \sqrt{(0.71)^2 + (0)^2 + (0)^2 + (0.57)^2 + (0.49)^2} = \sqrt{1.0691} \approx 1.0339.$$

$$\tilde{u} = \frac{u}{\|u\|} = \left[\frac{0.71}{1.0339}, \frac{0}{1.0339}, \frac{0}{1.0339}, \frac{0.57}{1.0339}, \frac{0.49}{1.0339}\right] = [0.687, 0, 0, 0.552, 0.474].$$

Normalize d:

$$\|d\| = \sqrt{(0.83)^2 + (0.55)^2 + (0.33)^2 + (0.55)^2} = \sqrt{1.4028} \approx 1.183.$$

$$\tilde{d} = \frac{d}{\|d\|} = \left[\frac{0.83}{1.183}, \frac{0.55}{1.183}, \frac{0.33}{1.183}, \frac{0.55}{1.183}\right] = [0.702, 0.465, 0.279, 0.465].$$

Calculate R(u, d):

$$R(u, d) = (0.687 \cdot 0.702) + (0 \cdot 0.465) + (0 \cdot 0.279) + (0.552 \cdot 0.465) + (0.474 \cdot 0.465).$$

$$R(u, d) = 0.482 + 0 + 0 + 0.257 + 0.220 = 0.959.$$

Where:

- u = 1 and d = 1 (because the vectors are normalized).
- θ is the angle between the two vectors.

Assuming the vectors are normalized (u = d = 1), the expression simplifies to:

u · d = cos θ, where — 1 ≤ cos θ ≤ 1

Normalize the scalar product of two normalized vectors to ensure the result is always in the range[0,1]using the following formula:

$$R(u, d)_{normalized} = \frac{R(u, d) + 1}{2} = \frac{0.959 + 1}{2} = 0.9795.$$

This normalization ensures that the scalar product values, originally in the range [−1, 1], are mapped into the range [0, 1], which is suitable for positive scoring.

Temporal Context Modifier (T(C))

The Temporal Context Modifier (T(c)) adjusts the risk score based on timing and security conditions. It ensures that access decisions are sensitive to the context of the request, such as time of day, day of the week, holidays, and security alert levels. The T(c) formula is:

T(c) = 1 + δ(c),

Where:

- δ(c) is a dynamic adjustment factor calculated based on contextual parameters c These parameters include:
- Time of Day (c1): Normalized to [0, 1] (e.g., midnight = 0, noon = 0.5).
- Day of the Week (c2): One-hot encoded (e.g., Monday = [1, 0, 0, 0, 0, 0, 0]).
- Holiday Indicator (c3): Binary (e.g., regular day = 0, holiday = 1).
- Security Level (c4): Binary (e.g., normal = 0, high alert = 1).
- Adding +1 ensures a baseline value of T(c) = 1 in neutral conditions (δ(c) = 0) preventing T(c) from nullifying other components in the ADS formula when no temporal risks are present. Additionally:
- The +1 ensures that T(c) starts from a neutral state and proportionally amplifies the score as temporal or security risks increase.
- Without +1, a T(c) of 0 would eliminate the influence of the temporal context,
- which is undesirable.

Example Calculation:

Given the following contextual parameters:

$$\begin{aligned}\text{Time of Day } (c_1) &: 9\,\text{PM, normalized to } \frac{21}{24} = 0.875,\\ \text{Day of the Week } (c_2) &: \text{Friday (one-hot: [0, 0, 0, 0, 0, 1, 0])},\\ \text{Holiday Indicator } (c_3) &: 0\,\text{(regular day)},\\ \text{Security Level } (c_4) &: 1\,\text{(high alert)}.\end{aligned}$$

Weights are assigned as follows: w1 = 0.4, w2 = 0.2, w3 = 0.1, w4 = 0.3.

The adjustment factor δ(c) is calculated as:

δ(c) = w1 · f (c1) + w2 · g(c2) + w3 · h(c3) + w4 · k(c4),

Where

f (c1) = 0.7 (high risk for late-night hours),

g(c2) = 0.2 (medium risk for Friday), h(c3) = 0 (no holiday adjustment), k(c4) = 1 (high alert condition).

Substituting:

δ(c) = (0.4 · 0.7) + (0.2 · 0.2) + (0.1 · 0) + (0.3 · 1) = 0.62.

If normalization is needed (e.g., max(δ(c)) = 1):

δ(c) normalized = δ(c)
max(δ(c). = 0.62

Finally, Compute T(c):
T(c) = 1 + δ(c)normalized = 1 + 0.62 = 1.62.

Conclusion

The Temporal Modifier T(c) ensures that temporal and contextual factors influence the risk score dynamically. The +1 provides a baseline neutral value while proportionally amplifying the score as risks increase.

Threshold

$$T_h = \begin{cases} 0.5, & \text{normal conditions} \\ 0.8, & \text{high alert.} \end{cases}$$

The system accepts the request if SADS > Th.

Example Calculation

Inputs
r = [0.89, 0.44, 0, 0.44, 0.35]
u = [0.71, 0, 0, 0.57, 0.49]
d = [0.83, 0.55, 0.33, 0.55]
0.9 0.4 0.1 0.5 0.3
0.8 0.5 0.0 0.4 0.4
M1(r) = 0.7 M2(r) = 0.5
α1 = 0.6 α2 = 0.4
β = 0.7 T(c) = 1.5.

Step 1: Machine Learning Contribution
∑(αi Mi(r)) = (0.6 · 0.7) + (0.4 · 0.5) = 0.42 + 0.2 = 0.62.

Step 2: Historical Similarity
H(r, B) = 1 r · B1 + r · B2 .
2 r · B1 r · B2

Result:
H(r, B) = 0.92.

Step 3: Risk Coefficient
R(u, d) = (0.71 · 0.83) + (0 · 0.55) + (0 · 0.33) + (0.57 · 0.55) + (0.49 · 0.55).

Result:
R(u, d) = 1.18.

Step 4: Exponential Weight
eβH(r,B) = e0.7·0.92 = 1.74.

Step 5: Temporal Context
T(c) = 1.5.

Final Score
SADS = ADS(r, u, d) = 0.62 · 1.74 · 1.18 · 1.5 = 1.91.

Enforce SADS to remain between 0 and 1 by applying the following sigmoid transformation:

$$\tilde{S}_{ADS} = \frac{1}{1+e^{-x}} = \frac{1}{1+e^{-1.91}} = 0.871$$

where x represents the ADS score SADS = 1.91.

Decision

- Th = 0.9 (high alert): Access denied. S˜ADS < Th
- Th = 0.5 (normal conditions): S˜ADS > Th Access granted.

In the example, access authorization depends on the organization's alert level. Under normal conditions, the system grants access based on the user's weighted score. During a high alert, such as a suspected cyber-attack, the system deems the user's score insufficient and denies access to the printer.

Discussion

The Dynamic Access Decision Scoring (ADS) system introduces a new way to view access control, moving beyond traditional methods by incorporating probabilities and acknowledging uncertainty. Security architects must grasp the framework's underlying mathematical concepts to ensure proper application. The central ADS equation captures multiple dimensions of risk, with each component offering a distinct perspective on how vulnerabilities emerge and interact.

R(u, d) employs vector dot products to gauge how closely user attributes align with resource demands. This approach, grounded in a more detailed mathematical analysis, reveals subtle relationships that would otherwise remain hidden. It enhances clarity and maintains computational efficiency while surpassing simplistic binary comparisons. By including the exponential term, the system highlights patterns in behavior that might otherwise seem insignificant. Adjusting the β coefficient allows security experts to fine- tune sensitivity, ensuring that even small deviations in user behavior receive the attention they deserve.

Shifting to a probability-focused model of access decisions acknowledges the reality that absolute protection remains an impossible goal. Instead of clinging to rigid protocols, this perspective views authorization judgments as inherently uncertain yet manageable. 357 Such a stance aligns with everyday security operations, where measured, probability- 358 informed safeguards often outperform inflexible strategies.

The system's underlying math provides enough latitude to accommodate various priorities. Some implementations might emphasize patterns drawn from historical data, while others might refine R(u, d) to sharpen role-related accuracy. The T(c) multiplier introduces environmental factors and evolving intelligence, guiding dynamic adjustments as circumstances shift. Multiplying these factors together prevents any element from dominating outcomes and masking critical vulnerabilities.

The framework adapts to a wide spectrum of operational needs by fine-tuning thresh- olds and adjusting weights. From high-security zones demanding meticulous anomaly detection to collaborative workspaces favoring straightforward resource access, the sys- tem's versatility supports diverse goals. Its rigorous mathematical basis paves the way for integration with machine learning, enabling automated adjustments as attack methods evolve or user behavior changes. Through careful calibration, organizations gain a balanced blend of security, agility, and efficiency within their access management strategies.

For decision-makers, this raises important considerations about the cost-benefit relationship between reducing false positives/ negatives and maintaining operational efficiency. The paper's approach suggests that some degree of uncertainty, when properly managed, can enhance security by allowing more nuanced and adaptive responses to access requests.

Future Research and Actions

Future research activities under the Dynamic Access Decision Scoring (ADS) system are poised to unlock groundbreaking possibilities in data security, operational efficiency, and compliance across diverse industries. A continued focus on healthcare-specific appli- cations is crucial, emphasizing machine learning models fine-tuned to clinical workflows, enhanced by robust encryption mechanisms to safeguard sensitive patient data. These models would adapt dynamically to various operational environments, ensuring the sys-tem's responsiveness to real-time demands while maintaining stringent security protocols.

Simultaneously, exploring quantum-resistant cryptographic methods could future-proof these systems against emerging computational threats, particularly as quantum computing becomes more accessible.

An interdisciplinary approach integrating compliance and operational benchmarks will further refine the ADS system's utility. Standardized implementation protocols tailored for healthcare organizations can streamline adoption while reducing workflow disruptions. Additionally, creating benchmarking frameworks for comparative performance analysis will encourage transparency and continuous innovation, fostering widespread confidence in the technology.

To broaden its applicability, the system's formula could evolve to serve sectors like finance or government, where securing access to sensitive data is paramount. This would necessitate user-friendly interfaces and comprehensive training for security managers to facilitate seamless integration. Backed by rigorous safeguards, emergency override systems could also enable efficient crisis management without compromising security integrity. By extending these initiatives and utilizing the Tree Structure Skeleton Colour Image(TSSCI) methodology within the framework, we can explore new frontiers. ((These meth-ods translate complex data structures—ranging from time-series sequences to unstructured textual data—into visual representations analyzable by convolutional neural networks (CNNs). Encoding intricate relationships into an interpretable visual format will allow the system to detect and highlight anomalies against predefined formula-based structures, ensuring data alignment and uncovering potential security breaches. This innovation provides a comprehensive view of data patterns, strengthening resilience against malicious attacks.

Integrating TSSCI with DSP further enhances operational efficacy by embedding these technologies within robust, AI-driven platforms tailored for global compliance and data security. This fusion underscores the commitment to advancing safety standards while facilitating practical implementation across industries. The convergence of theoretical ad- vancements and operational applications ensures a robust, scalable, and adaptive solution to AI safety and data management challenges [35].

Summary and Conclusions

This paper introduces the Dynamic Access Decision Scoring (ADS) framework, a novel approach to healthcare data access control that addresses the limitations of traditional rule- based systems. The framework combines machine learning, behavioral pattern analysis, and real-time risk assessment to create an adaptive security system that better protects sensitive medical data while maintaining operational efficiency.

The key innovation lies in the mathematical model for calculating access decision

scores:

SADS = ∑(αi Mi(r)) · eβH(r,B) · R(u, d) · T(c)

This formula integrates multiple risk factors into a unified scoring system, including histor-ical patterns, user behavior, and temporal context. Implementation results demonstrate significant improvements over traditional approaches, particularly in identifying and mitigating insider threats while ensuring HIPAA compliance.

The Framework's Primary Contributions Include

- A flexible, probabilistic approach to access control that adapts to changing security requirements
- Integration of machine learning models for dynamic risk assessment
- A mathematical foundation for combining multiple risk factors
- Real-time adjustment capability based on organizational security states

These advances represent a significant step forward in healthcare data security, offering or-ganizations a more sophisticated tool for balancing security requirements with operational needs. Future work could explore additional machine learning models and adaptation mechanisms to enhance the framework's capabilities.

Author Contributions: Conceptualization, Y.S. and A.H.; methodology, Y.S.; software, Y.S.; validation, Y.S. and A.H.; formal analysis, Y.S.; investigation, A.H.; resources, A.H.; data curation, Y.S.; writing— original draft preparation, Y.S.; writing—review and editing, A.H.; visualization, Y.S.; supervision, A.H.; project administration, Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Anderer, S., Kempter, T., Scheuermann, B., & Mostaghim, S. (2023). Dynamic optimization of role concepts for role-based access control using evolutionary algorithms. SN Computer Science. https://doi.org/10.1007/s42979-023-01805-1

2. Khoumsi, A. (2023). Automata-based study of dynamic access control policies. In Proceedings of the International Conference on Information Systems Security and Privacy. https://doi.org/10.5220/0011819700003405
3. Chatterjee, A., Pitroda, Y., & Parmar, M. (2020). Dynamic role-based access control for decentralized applications. arXiv preprint arXiv:2002.05547. https://doi.org/10.1007/978-3-030-59638-5_13
4. Liu, A., Du, X., & Wang, N. (2020). Access control role evolution mechanism for open computing environment. Electronics, 9(3), 517. https://doi.org/10.3390/electronics9030517
5. Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2024). Permissioned blockchain network for proactive access control to electronic health records. BMC Medical Informatics and Decision Making, 24. https://doi.org/10.1186/s12911-024-02708-8
6. Xu, Z., Zheng, E., Han, H., Dong, X., Dang, X., & Wang, Z. (2024). A secure healthcare data sharing scheme based on two-dimensional chaotic mapping and blockchain. Dental Science Reports. https://doi.org/10.1038/s41598-024-73554-x
7. Dadhania, A. J., & Patel, H. (2024). HEALTHSOLID 4.0: A novel solid-pod and blockchain-enabled framework for role-based access control and secure healthcare information exchange. International Journal on Information Technologies and Security (IJITS). https://doi.org/10.59035/orqu3863
8. Sujitha, S. J., & Selvi, P. T. (2024). Ensuring access control reliability and security of lightweight blockchain-based IoT cloud-based electronic medical records sharing. In Proceedings of the 2024 International Conference on Advances in Computing and Artificial Intelligence (ACCAI). IEEE. https://doi.org/10.1109/accai61061.2024.10602256
9. Zhang, S., Guo, F., Jing, C., & Wu, C. (2024). Electronic medical record privacy protection scheme based on attribute encryption technology. In Proceedings of the 2024 IEEE International Conference on Industrial Artificial Intelligence and Automation Control (IAEAC). IEEE. https://doi.org/10.1109/iaeac59436.2024.10503978
10. Chauhan, A. S. (2024). Leveraging machine learning to improve access control mechanisms in data warehousing. African Journal of Biological Sciences, 6(12), 2650–2658. https://doi.org/10.48047/afjbs.6.12.2024.2650-2658
11. Agorbia-Atta, C., Atalor, I., Agyei, R. K., & Nachinaba, R. (2024). Leveraging AI and ML for next-generation cloud security: Innovations in risk-based access management. World Journal of Advanced Research and Reviews, 23(3), 481. https://doi.org/10.30574/wjarr.2024.23.3.2788
12. Al Lail, M., Pinto, D., Almanza, L. A., Salazar, F., & Rizzi, C. (2024). Beyond traditional methods: Deep learning with data augmentation for robust access control. In Proceedings of the 2024 33rd International Conference on Computer Communications and Networks (ICCCN) (pp. 1–6). IEEE. https://doi.org/10.1109/icccn61486.2024.10637533
13. el Hadj, M. A. (2023). Exploring the role of machine learning in enhancing access control systems: A comprehensive review. International Journal of Computing and Digital Systems, 14(1), Article 107. https://doi.org/10.12785/ijcds/1401107
14. Matzutt, R. (2024). Towards access control for machine learning embeddings. In Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC), Xanthi, Greece, June 2024. https://doi.org/10.1145/3655693.3661296
15. Arora, N. (2024). Mathematical foundations of data security in cloud environment. Journal of Mechanics of Continua and Mathematical Sciences, Special Issue 11, Article 00015. https://doi.org/10.26782/jmcms.spl.11/2024.05.00015
16. Said, A. S. (2023). Number theory and cryptography: Unraveling the foundations of data security. OSF Preprints. https://doi.org/10.31219/osf.io/5sczk
17. Harris, T., Yue, L., & Tatiana, T. K. (2019). Data security method utilizing mesh network dynamic scoring. International Journal of Network Security, 21, 451–459.
18. Tang, Z., Ma, D., Sun, X., Chen, K., Wang, L., & Jiang, J. (2023). Every time can be different: A data dynamic protection method based on moving target defense. In Proceedings of the 2023 IEEE Symposium on Computers and Communications (ISCC) (pp. 568–574). IEEE. https://doi.org/10.1109/iscc58397.2023.10218253
19. Radhakrishnan, S. (2024). The intersection of algebra and cryptography: Enhancing information security through mathematical foundations. Computing and Analytics, 31, 112–128. https://doi.org/10.52783/cana.v31.943
20. Idoko, B., Alakwe, J. A., Ugwu, O. J., Idoko, J. E., Idoko, F. O., Ayoola, V. B., Ejembi, E. V., & Adeyinka, T. (2024). Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. Magna Scientia Advanced Research and Reviews, 11(2). https://doi.org/10.30574/msarr.2024.11.2.0110
21. Tazi, F., Nandakumar, A., Dykstra, J., Rajivan, P., & Das, S. (2024). SoK: Analyzing privacy and security of healthcare data from the user perspective. ACM Transactions on Computing for Healthcare. https://doi.org/10.1145/3650116
22. Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. Computers, 13(2), 41. https://doi.org/10.3390/computers13020041
23. Cai, R., Chen, L., & Zhu, Y. (2024). Privacy-preserving access control model for e-medical systems. In Proceedings of the 2024 IEEE International Conference on Big Data and Privacy Computing (BDPC). IEEE. https://doi.org/10.1109/bdpc59998.2024.10649051
24. Singhal, S. (2024). Data privacy, compliance, and security including AI ML. In Practical Applications of Data Processing, Algorithms, and Modeling (pp. 111–126). IGI Global. https://doi.org/10.4018/979-8-3693-2909-2.ch009
25. Audu, A. J., & Umana, A. U. (2024). Advances in environmental compliance monitoring in the oil and gas industry: Challenges and opportunities. International Journal of Scientific Research Updates, 8(2). https://doi.org/10.53430/ijsru.2024.8.2.0062
26. Solanke, B., Onita, F. B., Ochulor, O. J., & Iriogbe, H. O. (2024). The impact of artificial intelligence on regulatory compliance in the oil and gas industry. International Journal of Science and Technology Research Archive, 7(1). https://doi.org/10.53771/ijstra.2024.7.1.0058
27. Fahrudin, R., Yulian, F. D., Fauzi, A. Y., Wilson, A., & Kuusk, T. (2024). Addressing regulatory risks in fintech through decentralized technologies. APTISI Transactions on Management, 8(3). https://doi.org/10.33050/atm.v8i3.2356

28. Abikoye, B. E., Umeorah, S. C., Adelaja, A. O., Ayodele, O., & Ogunsuji, Y. M. (2024). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. World Journal of Advanced Research and Reviews, 23(1). https://doi.org/10.30574/wjarr.2024.23.1.2174
29. Nisbet, N., Zhang, Z., & Cidik, M. (2024). Real-time assessment of regulatory compliance of construction sites. In Proceedings of the 2024 European Conference on Computing in Construction. European Council on Computing in Construction. https://doi.org/10.35490/ec3.2024.215
30. Hamouid, K., & Mohammedi, M. (2023). Dynamic and flexible access control for IoT-enabled smart healthcare. In Proceedings of the 2023 International Symposium on Networks, Computers and Communications (ISNCC). IEEE. https://doi.org/10.1109/isncc58260.2023.10323989
31. Chiang, T. W., Chiang, D. L., Chen, T. S., Lin, F. Y. S., Shen, V. R. L., & Wang, M. C. (2022). Novel Lagrange interpolation polynomials for dynamic access control in a healthcare cloud system. Mathematical Biosciences and Engineering, 19(4), 427. https://doi.org/10.3934/mbe.2022427
32. Srivastava, K. (2021). NdRAdAC: Need based access control framework for an emergency response system. Turkish Journal of Computer and Mathematics Education, 12(5), 2037. https://doi.org/10.17762/turcomat.v12i5.2037
33. Shahraki, A. S., Rudolph, C., & Grobler, M. (2019). A dynamic access control policy model for sharing of healthcare data in multiple domains. In Proceedings of the Trust, Security and Privacy in Computing and Communications. https://doi.org/10.1109/trustcom/bigdatase.2019.00088
34. Faruqui, R. U. (2020). Modelling and verifying dynamic access control policies in workflow-based healthcare systems. Jurnal Kejuruteraan, 32(1), 1–7. https://doi.org/10.17576/jkukm-2020-32(1)-01
35. Segal, Y., Hadar, O., & Lhotska, L. (2023). Using EfficientNet-B7 (CNN), variational autoencoder (VAE) and Siamese twins' networks to evaluate human exercises as super objects in TSSCI images. Journal of Personalized Medicine, 13(5), 874. https://doi.org/10.3390/jpm13050874