Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.084659

ARTICLE

An AI-Driven and Risk-Aware Digital Identity Protection Framework for Secure IoMT Environments

Joong-Hyun Park[1], **Jiho Choi**[2], **Libor Mesicek**[3] **and Hoon Ko**[2,*]

[1]Software-Oriented University, Sunmoon University, 70, Sunmoon-ro 221 beon-gil, Tangjeong-myeo, Asan-City, Chungcheonnam-do, Republic of Korea

[2]Department of Computer Science & Engineering, Sunmoon University, 70, Sunmoon-ro 221 beon-gil, Tangjeong-myeo, Asan-City, Chungcheonnam-do, Republic of Korea

[3]Faculty of Social and Economic Studies, Jan Evangelista Purkyne University, Pasteurova 1, Usti nad Labem, Czech Republic

*Corresponding Author: Hoon Ko. Email: hoonko21@sunmoon.ac.kr

Received: 27 April 2026; Accepted: 11 June 2026; Published: 23 July 2026

ABSTRACT: With the rapid expansion of the Internet of Medical Things (IoMT), the importance of digital identity–based security has significantly increased. However, conventional static authentication mechanisms are insufficient to effectively address various identity misuse and abuse attacks. In this study, we model digital identity as a dynamic security entity and propose an AI-based framework that integrates a risk scoring model—combining unsupervised anomaly detection with context-aware analysis—and a multi-level risk-adaptive access control mechanism (Permit, Step-Up, Restrict). Experimental results using an extended version of the CERT Insider Threat Dataset tailored for IoMT environments provide proof-of-concept evidence that the proposed method can achieve an AUC of approximately 0.927, orange demonstrating effective discrimination between normal and malicious behavioral patterns. Furthermore, the framework maintains a low False Restriction Rate of around 1.605% while still detecting attacks at a meaningful level, thereby achieving a balance between security and usability. This study highlights the feasibility of a risk-adaptive digital identity protection framework that dynamically evaluates digital identity and adaptively responds based on risk levels in IoMT environments.

KEYWORDS: Digital identity; internet of medical things (IoMT); artificial intelligence (AI); continuous authentication; adaptive risk assessment

1 Introduction

The digital transformation of the healthcare sector has accelerated the adoption of the Internet of Medical Things (IoMT), enabling continuous patient monitoring, remote diagnosis, and data-driven clinical decision-making [1]. Wearable devices, implantable sensors, and intelligent medical equipment continuously generate and exchange sensitive health data in heterogeneous and distributed environments [2]. While these technologies significantly enhance healthcare efficiency and service quality, they also introduce critical cybersecurity and privacy challenges due to the sensitivity of medical data and the heterogeneity of connected devices [3,4]. Recent ransomware incidents targeting hospitals and digital healthcare infrastructures have demonstrated how interconnected healthcare ecosystems can amplify the risks of identity compromise, service disruption, and unauthorized access attacks [5,6]. Recent studies highlight that identity-related threats and access control are major security concerns in IoMT-based healthcare systems, noting that identity compromise can directly impact patient safety and service availability. Digital identity defines

authentication, access control, accountability, and data ownership among patients, healthcare providers, and medical devices. Unlike traditional information systems, the IoMT ecosystem involves diverse entities interacting dynamically under varying contextual conditions, thereby increasing exposure to impersonation, insider misuse, and identity compromise. Despite this, many IoMT security architectures still treat digital identity as a static credential verified through one-time authentication [7]. Existing cybersecurity solutions in healthcare primarily focus on network- and device-level defenses, relying on predefined credentials, rule-based access policies, and reactive security mechanisms. While such static approaches may be effective against known threats, they are limited in detecting identity-centric attacks that evolve gradually through behavioral changes. Consequently, compromised credentials and abnormal identity usage are often detected only after significant operational or safety-related damage has occurred. To enhance trustworthiness and auditability in identity management, blockchain-based digital identity (DI) models have been proposed, offering immutability and transparency that are particularly appealing in healthcare environments. However, many existing DI frameworks implicitly assume that identity trust persists after initial verification and fail to provide mechanisms for continuous behavioral evaluation or adaptive risk assessment. Unlike conventional zero-trust or federated identity frameworks that primarily rely on static trust verification and session-level authentication, the proposed framework continuously evaluates behavioral and contextual identity risks in real time. Meanwhile, Artificial Intelligence (AI) has demonstrated strong potential in cybersecurity through anomaly detection, behavioral analysis, and automated threat response [8]. Nevertheless, AI-based solutions in healthcare security have largely focused on network traffic and malware detection, with limited efforts to explicitly model digital identity itself as a primary and dynamic security asset. These limitations highlight the need for an identity-centric security model that continuously evaluates identity behavior and adapts to evolving threats, while respecting the availability-critical nature of healthcare services. In particular, IoMT environments require a dynamic identity protection model because users, devices, services, and contextual conditions continuously change over time. Therefore, digital identity should not be treated as a fixed credential verified only at login, but as a behavior-aware security entity that must be continuously evaluated throughout interactions. To address this research gap, this paper proposes an AI-based digital identity protection framework for secure IoMT environments and redefines digital identity as a dynamic, behavior-aware security asset. The proposed framework integrates a blockchain-based decentralized identity infrastructure with AI-driven continuous authentication and adaptive risk assessment, thereby transforming the identity protection paradigm into a proactive, context-aware, and risk-adaptive model aligned with IoMT operational requirements. The remainder of this paper is organized as follows. Section 2 reviews the background and related work, while Section 3 analyzes the AI-based Digital Identity Protection Framework. Section 4 presents the experiments and their analysis, and Section 5 concludes the paper.

2 Background and Related Work

2.1 Digital Identity in IoMT Environments

The Internet of Medical Things (IoMT) enables continuous monitoring, remote diagnosis, and data-driven decision-making across heterogeneous environments comprising patients, healthcare providers, medical devices, and cloud services. Within this ecosystem, digital identity provides the basis for authentication, access control, accountability, and data ownership. Compared to traditional information systems, identity management in IoMT is more complex due to the coexistence of human users and autonomous devices and their interactions across organizational and network boundaries [9]. In addition, contextual factors such as time, location, and device state continuously influence identity-related activities [10]. These characteristics highlight the need for adaptive and context-aware identity protection mechanisms in IoMT environments [11]. Furthermore, IoMT environments introduce unique identity management challenges

due to device heterogeneity, interoperability limitations, user and device mobility, and the real-time operational requirements of healthcare services. These characteristics make static credential-based authentication insufficient for detecting gradual identity compromise and abnormal behavioral changes.

2.2 Biometric Identity-Based Security Approaches

Early identity-centric security studies explored biometric methods as a means of secure authentication and strategic data sharing. Ogiela et al. proposed biometric-based mechanisms for advanced strategic data sharing protocols, demonstrating the role of identity verification in secure information exchange. These studies contributed foundational concepts for identity-aware security architectures. However, their focus remained on authentication and secure data sharing, rather than dynamic identity integrity verification or anomaly detection in distributed cyber environments.

2.3 AI in Cybersecurity and Identity Protection

Artificial Intelligence (AI) has emerged as an effective tool in cybersecurity, supporting anomaly detection, behavioral analysis, and automated threat response [12–14]. AI-based techniques have been widely applied to tasks such as intrusion detection, malware classification, and fraud detection [15]. In IoMT environments, authentication and access control must balance security with availability and usability, as overly rigid controls may disrupt healthcare services [16]. Recent studies have explored behavioral analysis and continuous authentication, demonstrating that security systems can move beyond static credential verification [17]. However, most AI-based security solutions primarily focus on network-level signals, and approaches that explicitly model digital identity behavior as a primary security indicator remain limited [18]. In healthcare IoMT environments, AI-driven security mechanisms must carefully balance attack detection capability with operational continuity, since excessive false positives or unnecessary access restrictions may negatively affect clinical workflows and patient care services [19].

2.4 Blockchain-Based Digital Identity

Blockchain-based digital identity (DI) frameworks aim to provide immutability, transparency, and auditability without relying on a central authority. In healthcare contexts, these properties can enhance identity integrity and traceability while mitigating the single point of failure associated with centralized identity repositories [20–24]. Extensive survey studies on blockchain-based identity management and self-sovereign identity ecosystems have highlighted both the potential benefits and the open challenges of decentralized identity models [25]. However, most existing DI frameworks primarily focus on identity registration and initial verification [26], implicitly assuming that identity trust remains static after verification, and thus fail to adequately support continuous evaluation or adaptive risk assessment. As a result, many existing decentralized identity frameworks have limited capability to dynamically reassess identity trust once authentication has been completed, making continuous behavioral verification and adaptive risk evaluation difficult in rapidly changing IoMT environments.

2.5 Limitations of Existing Digital Identity Protection in IoMT

Most existing digital identity (DI) approaches rely on credential-based authentication and access control mechanisms. However, these approaches do not sufficiently capture the characteristics of IoMT environments, which involve heterogeneous devices, continuous data exchange, and dynamic behavioral patterns that evolve over time. Table 1 summarizes the limitations of current DI approaches.

Table 1: Summary of digital identity (DI) concepts and limitations.

Category	Core Concept	Conventional Approach	Limitations
Static Identity Assumption	Identity is assumed to remain stable and trustworthy after authentication	Trust is established at the time of initial authentication and session key agreement	Fails to reflect behavioral changes over time, contextual variations, and evolving risk levels
Reactive Rule-Based Security Model	Security is based on predefined rules and known attack patterns	Detection and response occur after anomalous behavior is observed	Unable to detect gradual and delayed attacks and lacks proactive defense capability
Lack of Context and Behavioral Awareness	Access control is primarily based on credentials	Evaluation focuses on credential verification at the time of access request	Insufficient for detecting behavior-based anomalies such as access time, device usage, and user patterns
Fragmented Identity Management in IoMT	Identity structures are distributed across multiple entities	Independent identity management systems are maintained for each domain	Causes identity inconsistency and increases the attack surface
Lack of Intelligent Risk Assessment	Identity is treated as a simple binary value	AI-based risk evaluation is used only in a limited manner	Risk scores are not directly integrated into access control policies

Fig. 1 illustrates the differences between existing identity protection mechanisms and AI-driven identity protection. While traditional approaches rely on static credentials and reactive security policies, AI-driven methods incorporate continuous authentication, behavioral analysis, and adaptive risk-based decision-making to address dynamic IoMT threats. The proposed framework further illustrates how behavioral monitoring, AI-driven risk analysis, adaptive access control, and blockchain-based identity verification interact to continuously evaluate identity trust and dynamically respond to evolving security risks in IoMT environments.

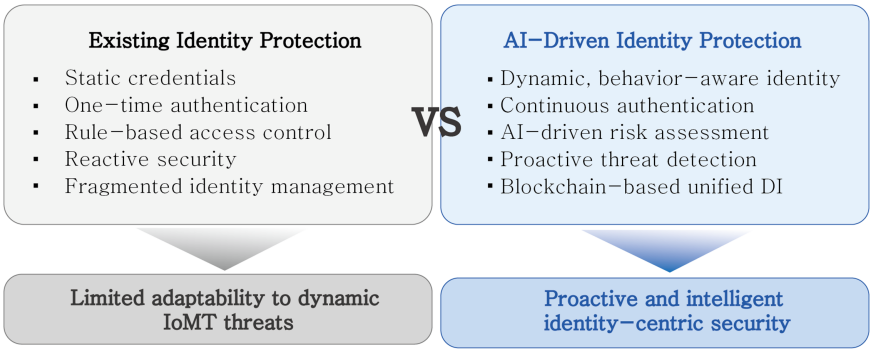

Figure 1: Existing identity protection vs. AI-driven identity protection.

Based on the above limitations, the proposed framework is designed to move beyond static credential-based identity protection by integrating blockchain-based identity anchoring, AI-driven behavioral risk assessment, and adaptive access control.

3 AI-Based Digital Identity Protection Framework

The overall operational process of the proposed framework follows the procedure defined in the Algorithm and can be conceptually summarized as a stepwise workflow as follows:

- **STEP 1: DI Generation and Blockchain Anchoring**
- **STEP 2: Continuous Monitoring of Behavioral and Contextual Information**
- **STEP 3: AI-based Dynamic Identity Risk Assessment**
- **STEP 4: Risk-Based Access Control Execution**
- **STEP 5: Policy Adaptation and Proactive Response**

The proposed framework is designed to provide continuous and adaptive identity protection in dynamic IoMT environments, where static credential-based authentication alone is insufficient [27]. Each stage of the framework contributes to mitigating different identity-related security risks. DI generation and blockchain anchoring establish a tamper-resistant trust foundation for healthcare entities. Continuous monitoring of behavioral and contextual information enables the framework to capture evolving identity activities beyond one-time authentication [28,29]. AI-based dynamic identity risk assessment identifies abnormal behavioral deviations and contextual inconsistencies in real time [30]. Risk-based access control execution adaptively adjusts authentication and authorization decisions according to the calculated identity risk level. Finally, policy adaptation and proactive response enable continuous refinement of security policies and behavioral models to address evolving threats while maintaining healthcare service continuity [31,32]. Each step directly corresponds to the detailed procedures described in the algorithm. Specifically, STEP 1 corresponds to lines 1–5 of Algorithm 1, where a digital identity for IoMT entities is generated and anchored on the blockchain to establish a trust foundation. STEP 2 corresponds to line 6, involving the continuous collection of behavior and contextual information associated with the identity. STEP 3 corresponds to lines 7–9, where the collected behavior is compared against baseline profiles to compute a dynamic risk score for the identity. STEP 4, corresponding to lines 10–22, integrates DI verification with risk assessment results to perform adaptive access control decisions, such as permit, step-up authentication, restrict, or deny. Finally, STEP 5, corresponding to lines 23–25, ensures continuous and proactive identity protection through audit logging, policy updates, and model refinement [33,34].

Algorithm 1: Blockchain-anchored DI with AI-driven continuous identity protection for IoMT

Require: S: Set of IoMT entities (patients, clinicians, devices, services)
1: R: Access request from entity $s \in S$
2: Ctx: Contextual information (time, location, device state, service type)
3: $Policy$: Security policy set
4: VC: Verifiable credentials linked to DI
5: B: Blockchain ledger (trust anchor)
6: M: Trained AI behavior model
7: T_{low}: Lower risk threshold
8: T_{high}: Upper risk threshold
Ensure: D: Access decision $\in$ {Permit, StepUp, Restrict, Deny}
9: $Logs$: Audit logs and updated policy

(Continued)

Algorithm 1 (continued)

function MAIN_WORKFLOW($S, R, Ctx, Policy, VC, B, M$)
  // Layer 1: Blockchain-Based DI (Trust Anchor)
  for all $s \in S$ **do**
    $DI_s \leftarrow$ Generate_Digital_Identity(s)
    $VC_s \leftarrow$ Issue_Verifiable_Credential(s, attributes(s))
    Anchor_On_Blockchain(B, DI_s, hash(VC_s))
  end for
  // Layer 2: AI Intelligence (Continuous Identity Assessment)
  $Obs \leftarrow$ Collect_Identity_Behavior(
    request_pattern,
    device_interaction_sequence,
    temporal_usage,
    contextual_attributes)
  $Profile_s \leftarrow$ Load_Baseline_Profile(M, s)
  $Deviation \leftarrow$ Compare(Obs, $Profile_s$)
  $RiskScore \leftarrow$ Compute_Identity_Risk($Deviation$, Ctx)
  // Layer 3: IoMT Interaction (Adaptive Access Control)
  if Verify_Credential(VC_s, DI_s, B) = False **then**
    $D \leftarrow$ Deny
  else
    if $RiskScore < T_{low}$ **then**
      $D \leftarrow$ Permit
    else if $T_{low} \leq RiskScore < T_{high}$ **then**
      $D \leftarrow$ StepUp
      Trigger_Additional_Authentication(s)
    else
      $D \leftarrow$ Restrict or Deny
      Trigger_Security_Alert(s)
    end if
  end if
  // Layer 4: Feedback & Policy Adaptation
  Update_Audit_Log(s, DI_s, Obs, $RiskScore$, D)
  Adapt_Security_Policy($Policy$, $RiskScore$, Ctx, threat_trends)
  Update_Behavior_Model(M, Obs, feedback_from_decision)
  return D
end function

The algorithm summarizes the operational workflow of the proposed framework. First, each IoMT entity is assigned a blockchain-anchored DI and associated verifiable credentials, establishing a tamper-resistant trust anchor. Next, behavioral and contextual observations are continuously collected and compared against the learned baseline profile using an AI model. Based on the resulting dynamic identity risk score, the framework performs context-aware and risk-adaptive access control, ranging from normal access approval to step-up authentication, restriction, or denial. Finally, audit logs, policy updates, and model refinement enable proactive and continuous identity protection in dynamic IoMT environments. In the

proposed framework, the blockchain layer functions as a trust anchor rather than a real-time decision-making component. Specifically, identity-related metadata such as digital identity identifiers and hashes of verifiable credentials are stored on-chain, while detailed behavioral data and real-time analysis remain off-chain to ensure efficiency. This hybrid design balances the trade-off between trust and performance, where blockchain ensures immutability and auditability, while off-chain processing enables low-latency identity risk evaluation required in healthcare environments.

Fig. 2 illustrates the overall architecture of the proposed AI-driven digital identity protection framework for IoMT. The operational data flow can be described as follows. First, IoMT entities generate access requests along with behavioral and contextual information. Second, the AI intelligence layer analyzes these observations to compute a dynamic identity risk score. Third, the blockchain-based DI layer verifies identity credentials and provides a trust anchor. Finally, the framework integrates the risk score with credential verification results to produce an adaptive access control decision. The IoMT interaction layer consists of heterogeneous entities, including patients, healthcare professionals, and medical devices, which generate identity-aware access requests. The AI intelligence layer performs behavioral profiling and risk scoring, enabling dynamic and context-aware decision-making. The blockchain-based digital identity layer provides a trusted foundation by anchoring digital identities and verifiable credentials, ensuring integrity, traceability, and auditability. From a deployment perspective, the proposed framework adopts a hybrid architecture to reduce operational overhead. Blockchain is used exclusively for digital identity anchoring and credential integrity verification, while computationally intensive behavioral analysis and anomaly detection are executed off-chain. This separation minimizes blockchain-induced latency, reduces communication overhead, and improves deployment practicality for healthcare infrastructures. The framework is structured into three interconnected layers. The IoMT interaction layer consists of heterogeneous entities, including patients, healthcare professionals, and medical devices, which generate identity-aware access requests. The AI intelligence layer performs continuous identity assessment through behavioral profiling, continuous authentication, and adaptive risk scoring, enabling dynamic and context-aware decision-making. The blockchain-based digital identity layer provides a trusted foundation by anchoring digital identities and verifiable credentials, ensuring integrity, traceability, and auditability. By integrating these layers, the proposed framework enables proactive and risk-adaptive identity protection, addressing the limitations of static credential-based approaches in dynamic IoMT environments. To empirically validate the effectiveness of the proposed framework, the following section presents the dataset transformation process, risk scoring model, access control policy, and performance evaluation using an IoMT-extended dataset.

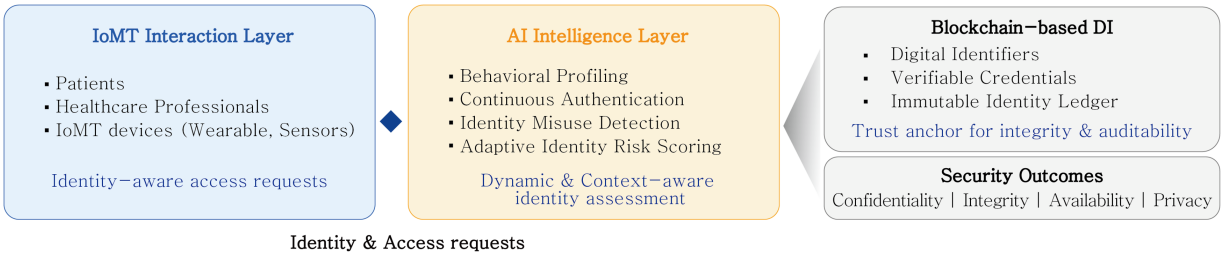

Figure 2: AI-driven digital identity protection framework for IoMT. The framework illustrates the operational data flow from IoMT entities to the AI intelligence layer and the blockchain-based digital identity layer. Behavioral and contextual data generated by patients, healthcare professionals, and medical devices are collected and analyzed by the AI intelligence layer to compute a dynamic identity risk score. The computed risk score is then combined with credential verification results to determine an adaptive access control decision, such as permit, step-up authentication, restrict, or deny.

4 Experiment and Analysis

4.1 Dataset and Experimental Setup

In this study, to analyze DI-based security in IoMT environments, the CERT Insider Threat Dataset—originally containing enterprise user activity logs—was reinterpreted and extended to reflect the relationships among users, devices, and behaviors in IoMT settings. Specifically, users were mapped to healthcare professionals and system users, while devices (e.g., PCs) were mapped to IoMT devices such as wearables and sensors. Log events (e.g., logon, file, and device activities) were transformed into access and usage behaviors in healthcare environments. Furthermore, to capture IoMT-specific characteristics, additional features were designed, including location information, identity type, access frequency, device consistency, and contextual deviation. Due to the limited availability of publicly accessible healthcare cybersecurity datasets containing identity-centric behavioral records, a proxy-based evaluation strategy was adopted in this study. Real healthcare IoMT datasets are often difficult to access because of privacy regulations, ethical constraints, and institutional data governance requirements. Therefore, the CERT Insider Threat Dataset was selected as a structurally analogous benchmark for evaluating identity-related anomaly detection behavior.

Table 2 summarizes the overall composition of the IoMT-extended dataset. The dataset contains over 1.7 million large-scale events and integrates user behavior, device information, and contextual attributes. It is important to note that the CERT Insider Threat Dataset was originally designed for enterprise IT environments rather than IoMT systems. Therefore, the mapping process applied in this study should be interpreted as a proxy-based transformation to approximate identity-related behaviors in IoMT contexts. Although the CERT dataset does not directly contain medical device telemetry, physiological signals, or patient-specific clinical workflows, identity-centric behavioral patterns such as access frequency, device usage consistency, abnormal login timing, and contextual deviation exhibit structural similarities to identity-related interactions in IoMT environments. In addition, the transformed dataset does not fully represent emergency-driven access behaviors, latency-sensitive medical interactions, or device-specific communication characteristics commonly observed in real healthcare IoMT ecosystems. These limitations may affect the direct generalizability of the experimental results to operational clinical environments. In this sense, the transformed dataset provides a proof-of-concept basis for evaluating whether dynamic identity risk can be detected from behavioral and contextual features. Nevertheless, the transformed dataset may not fully capture the physiological, real-time, and device-specific characteristics of real medical IoT environments. Accordingly, this study should be regarded as a proxy-based proof-of-concept validation rather than a full clinical deployment evaluation. Accordingly, the present evaluation should be interpreted as a proof-of-concept validation rather than evidence of immediate clinical deployment readiness. Future work is going to focus on validating the proposed framework using real-world healthcare cybersecurity datasets, IoMT telemetry, digital identity access logs, and dedicated medical IoT simulation environments that better reflect operational clinical workflows.

4.1.1 Transformation of the CERT Dataset for IoMT

The key columns of the CERT dataset (user, pc, date, and activity) were transformed to align with the digital identity (DI) structure in IoMT environments. In addition, supplementary features were designed to integratively capture user behavior and contextual information. The transformation from enterprise user activity to IoMT identity behavior is grounded in the assumption that identity-centric security threats share common structural patterns across domains. For example, unauthorized login events correspond to abnormal access attempts in healthcare systems, while device inconsistencies reflect potential device

hijacking scenarios. This abstraction enables the modeling of identity misuse behaviors despite domain differences. This transformation is not intended to imply that enterprise IT logs and IoMT logs are identical. Rather, it is designed as a structural alignment between enterprise identity events and IoMT identity interactions. In both domains, identity misuse can be observed through abnormal access frequency, unusual access timing, device inconsistency, and deviations from a user's historical behavior. Thus, the transformation focuses on abstract identity-behavior relationships rather than domain-specific medical measurements.

Table 2: Summary of IoMT-extended dataset.

Category	Description
Original Dataset	CERT Insider Threat Dataset
Data Extension	Extended to reflect IoMT environment characteristics
Total Events	1,705,820
Number of Users	1000
Log Types	Logon, file, device
Number of Features	14
Key Features	Time, location, identity type, access count, device match, context deviation
Data Ordering	Chronological order (time-based sorting)
Data Split	Time-based split (Train/Test)
Training Data	1,184,162 events
Test Data	511,746 events
Learning Approach	Unsupervised learning based on normal data
Label Configuration	Normal/Attack (three attack scenarios)

Table 3 presents the transformation of the CERT dataset into an IoMT-oriented feature set. The original columns, such as *user*, *pc*, *date*, and *activity*, were reinterpreted to align with the IoMT environment. In addition, supplementary features were generated to capture temporal patterns, user behavioral characteristics, and contextual information. In particular, identity-aware features such as *device_match* and *context_deviation* were designed to model the relationships among users, devices, and contextual conditions.

Table 3: Transformation from CERT dataset to IoMT-extended features.

Original (CERT)	Derived Feature (IoMT)	Feature Type	Description
User	user_id	Identity	Unique identifier of user (clinician/system user)
pc	device_id	Device	Identifier mapped to IoMT device (e.g., wearable, sensor)
Date	Timestamp	Temporal	Event occurrence time
Activity	Activity	Behavioral	Activity type (logon, file, device)
Date	Hour	Temporal	Hour of day (0–23)
Date	day of week	Temporal	Day of the week
Date	is_weekend	Temporal	Weekend indicator

(Continued)

Table 3 (continued)

Original (CERT)	Derived Feature (IoMT)	Feature Type	Description
Date	is_night	Temporal	Night-time access indicator
User + timestamp	access_count_24h	Behavioral	Number of accesses within the past 24 h
pc + user	device_match	Identity-aware	Registered device matching indicator (0/1)
N/A	Location	Contextual	Access location (e.g., hospital, remote)
N/A	identity_type	Contextual	User type (e.g., clinician)
User behavior history	context_deviation	Identity-aware	Deviation from baseline behavior
Derived	Label	Ground Truth	Normal (0)/Attack (1)

4.1.2 Attack Scenario

Table 4 defines three representative identity-based attack scenarios in IoMT environments, as summarized in that Table. Each scenario is constructed by reinterpreting the CERT Insider Threat Dataset to reflect diverse identity misuse situations in IoMT settings. In particular, credential theft and device hijacking exhibit clear anomalous patterns, whereas insider misuse closely resembles normal behavior but is characterized by subtle deviations. Each attack scenario was simulated by introducing abnormal behavioral and contextual deviations into the transformed IoMT identity features. Credential theft scenarios were characterized by unusual login timing, unfamiliar access locations, and previously unseen device usage patterns. Device hijacking scenarios were simulated through inconsistent device-user relationships, mixed access sequences, and abrupt contextual mismatches between identity and device behavior. Insider misuse scenarios were modeled using gradual increases in access frequency, subtle deviations from historical behavioral profiles, and abnormal activity patterns occurring during otherwise legitimate operational periods. Unlike explicit attacks such as credential theft, insider misuse intentionally preserves partial similarity to normal behavior, making detection more difficult and requiring continuous behavioral risk assessment rather than simple rule-based anomaly detection.

Table 4: Attack scenarios in IoMT environment.

Scenario	Description	Key Characteristics
Credential Theft	Unauthorized access using compromised credentials	Unusual access time, remote location, new device
Insider Misuse	Increased abnormal activities by internal users	Increased access during normal hours, subtle behavioral changes
Device Hijacking	Access through compromised IoMT devices	Device mismatch, mixed or inconsistent access patterns

4.2 Feature Set and Risk Scoring Model

In this study, Isolation Forest was selected as the anomaly detection model due to its computational efficiency and suitability for unsupervised learning in large-scale environments. Unlike deep learning-based time-series models such as LSTM or Transformer architectures, which require substantial computational resources and training data, Isolation Forest provides a lightweight alternative that is well-suited for resource-constrained IoMT environments. Given that IoMT systems often operate on edge devices with strict latency and availability requirements, the use of a computationally efficient model is critical to ensure real-time risk assessment and uninterrupted healthcare services. The features used in this study were designed as shown in Table 5 to reflect user behavior, device usage, and contextual information. Behavioral features capture user activity patterns such as time and access frequency, while contextual features represent environmental information including location and user type. Identity-specific features model the relationship between users and devices as well as deviations in behavior. In particular, *context_deviation* was designed to quantify the difference between an individual user's current behavior and their normal behavioral patterns. This feature plays a critical role in detecting stealthy attacks, such as insider misuse or abuse.

Table 5: Description of extracted features.

Feature	Description
user_id	User identifier
device_id	Device used for access
timestamp	Event occurrence time
activity	Type of activity
hour	Time of day (hour)
day of week	Day of the week
is_weekend	Whether it is a weekend
is_night	Whether it is nighttime
Location	Access location
identity_type	Type of user
access_count_24 h	Number of accesses in the last 24 h
device_match	Whether it is a registered device
context_deviation	Deviation from normal behavior
Label	Normal/Attack

Risk Scoring Model

In this study, a risk score is computed by combining unsupervised learning-based anomaly detection with contextual information. First, the anomaly score for each event is calculated using the Isolation Forest algorithm,

$$A(x_t) \in [0,1] \tag{1}$$

Here, $A(x_t)$ represents the anomaly score of event x_t, where a higher value indicates a greater likelihood that the event deviates from normal patterns. Next, to reflect the difference between a user's normal behavioral pattern and the current activity, a context deviation is defined as follows,

$$D(x_t) = \frac{|x_t - \mu_b|}{\sigma_b + \epsilon} \tag{2}$$

In this equation, the deviation from the user's average behavioral pattern is normalized using the standard deviation, resulting in a scaled value. A higher value indicates a greater deviation from the normal pattern. The term $D(x_t)$ is a deviation-based metric designed to be combined with the anomaly score. Here, μ_b denotes the mean of the user's normal behavior pattern, and σ_b represents the standard deviation of that behavior. Finally, the risk score is defined by combining the anomaly score and the context deviation as follows:

$$R(x_t) = \alpha \cdot A(x_t) + \beta \cdot D(x_t) \tag{3}$$

The parameters α and β are weighting factors that reflect the relative importance of anomaly detection and contextual information. In this study, they are set to $\alpha = 0.7$ and $\beta = 0.3$ to emphasize the contribution of the anomaly score. The values of α and β were determined based on the objective of emphasizing anomaly-driven behavioral deviations while still incorporating contextual deviation information. Since identity misuse in IoMT environments often appears as abnormal behavioral patterns, a higher weight was assigned to the anomaly score. To examine the robustness of this setting, we conducted a sensitivity analysis using different combinations of α and β, including $(0.5, 0.5)$, $(0.7, 0.3)$, and $(0.9, 0.1)$. The results showed that the setting of $\alpha = 0.7$ and $\beta = 0.3$ provided a balanced trade-off between attack detection performance and false restriction control.

4.3 Risk-Aware Access Control Policy

4.3.1 Risk-Based Policy Framework

In this study, three levels of access control policies are defined based on the computed risk score $R(x)$, as follows:

- Permit: Access is allowed when the risk is assessed as low (normal level).
- Step-Up Authentication: Additional authentication is required when the risk is assessed as moderate.
- Restrict: Access is restricted when the risk is assessed as high.

Each policy is designed to provide a progressive response according to the level of risk. The definition of the access control policy is formulated as shown in (4).

$$Decision(x_t) = \begin{cases} \text{Permit}, & R(x_t) < T_{\text{low}} \\ \text{Step-Up}, & T_{\text{low}} \le R(x_t) < T_{\text{high}} \\ \text{Restrict}, & R(x_t) \ge T_{\text{high}} \end{cases} \tag{4}$$

4.3.2 Threshold Setting

The risk score-based policy is defined by two thresholds, T_{low} and T_{high}, which are described as follows.

- $R(x_t) < T_{\text{low}}$: Normal behavior → Permit
- $T_{\text{low}} \le R(x_t) < T_{\text{high}}$: Suspicious behavior → Step-Up
- $R(x_t) \ge T_{\text{high}}$: High likelihood of attack → Restrict

Normal behavior tends to cluster in the low-risk score region, whereas attack behavior is predominantly distributed in the high-risk score region. A distinguishable separation between the two distributions is observed. Based on the empirical distribution of risk scores, the thresholds are set to $T_{low} = 0.3$ and $T_{high} = 0.65$. The threshold values were selected based on the empirical distribution of risk scores observed in the training and validation results. Threshold candidates were iteratively evaluated using validation data to balance attack detection effectiveness and unnecessary access restrictions on legitimate healthcare

users. Specifically, T_{low} was set near the upper boundary of the normal behavior distribution to minimize unnecessary restrictions on legitimate users, while T_{high} was set in the high-risk region where attack samples were more concentrated. This configuration supports a progressive policy structure in which low-risk events are permitted, intermediate-risk events trigger step-up authentication, and high-risk events are restricted. Additional threshold sensitivity analysis confirmed that overly low thresholds increased false restrictions, whereas overly high thresholds reduced attack blocking performance.

4.3.3 Significance of Policy Design

The proposed access control policy has the following characteristics:

- Overcomes the limitations of single-threshold-based blocking approaches.
- Provides a progressive response mechanism based on risk levels.
- Maintains a balance between security and service availability.
- Supports continuous authentication and adaptive security responses required in IoMT environments.

4.4 Performance Evaluation

4.4.1 Overall Detection Performance Analysis

Table 6 presents the performance results on the test dataset. An AUC of 0.927 indicates that the model effectively distinguishes between normal and attack behaviors. The Precision of 0.313 and Recall of 0.476 imply that approximately half of the attack events are successfully detected. Although the precision and recall values indicate that certain attack events remain difficult to detect, particularly subtle insider misuse behaviors, healthcare IoMT environments require a balanced security strategy that minimizes unnecessary service disruption while maintaining practical attack mitigation capability. Therefore, the proposed framework prioritizes progressive risk-aware responses and low false restriction rates rather than aggressive blocking policies that could negatively affect clinical operations and patient care continuity. In addition, the False Restriction Rate is as low as 1.605%, indicating that unnecessary restrictions on legitimate users are minimized, thereby ensuring both availability and user convenience in IoMT environments. Furthermore, the Block Rate is measured at 47.646%, demonstrating that the risk-based access control policy is effective in blocking actual attacks.

Table 6: Overall performance of the proposed framework.

Metric	Value
AUC	0.927
Precision	0.313
Recall	0.476
F1-score	0.378
False Restriction Rate	1.605%
Block Rate	47.646%

4.4.2 Performance Analysis by Attack Scenario

Table 7 presents the detection performance by attack type. Credential theft and device hijacking attacks achieve high detection performance, with AUC values of 0.948 and 0.954, respectively. In particular, credential theft shows a detection delay (MTTD) of 0, indicating that immediate detection is possible. This result suggests that abrupt behavioral changes are effectively reflected in the risk score. In contrast, insider

misuse exhibits a relatively lower AUC (0.826) and a higher MTTD (27 events), indicating that detection is more challenging due to its tendency to mimic normal behavior patterns. Nevertheless, a certain level of increase in the risk score is still observed, suggesting that progressive response strategies, such as Step-Up authentication, are more appropriate than complete restriction. This limitation can be attributed to the use of a lightweight anomaly detection model, which prioritizes efficiency over the ability to capture long-term temporal dependencies. In addition, the performance of Isolation Forest may be sensitive to the quality and representativeness of engineered behavioral features, since the model does not explicitly learn hierarchical temporal relationships or semantic feature interactions. Consequently, insufficient or poorly designed behavioral and contextual features may reduce anomaly discrimination capability in highly dynamic healthcare environments. In particular, insider misuse remains challenging because malicious behavior may gradually emerge while still resembling normal user activity. Unlike credential theft or device hijacking, insider misuse does not always produce abrupt changes in access time, device consistency, or contextual attributes. Therefore, additional temporal and relational features may be required to capture long-term behavioral drift. Future work will investigate time-series models such as LSTM and Transformer-based architectures, as well as graph-based behavioral analysis, to better model sequential identity interactions and subtle deviations over time.

Table 7: Performance by attack scenario.

Attack Type	AUC	MTTD (Events)	Block Rate	False Restriction
Credential Theft	0.948	0	0.589	0.016
Device Hijacking	0.954	6	0.539	0.016
Insider Misuse	0.826	27	0.066	0.016

4.4.3 Risk Score Distribution Analysis

Fig. 3 shows the distribution of risk scores by attack type. The risk score distributions are clearly distinguishable across attack types. Credential theft and device hijacking are concentrated in the high-risk region, whereas insider misuse exhibits a lower and more dispersed distribution. Insider misuse tends to follow patterns similar to normal behavior, making it more difficult to distinguish from conventional attack types. The presence of several low-risk outliers in credential theft and device hijacking scenarios suggests that certain malicious behaviors may partially overlap with legitimate operational patterns, potentially resulting in false negatives or delayed detection. These overlaps may occur when compromised identities imitate normal access timing, familiar devices, or expected contextual conditions. Nevertheless, the proposed framework reduces the impact of such cases through progressive risk-aware responses rather than relying solely on binary anomaly classification. Future improvements may be achieved through additional contextual features, richer temporal behavior modeling, and adaptive threshold optimization to improve discrimination between benign and malicious identity interactions.

Fig. 4 illustrates the distribution of risk scores for normal and attack data. Normal data are predominantly concentrated in the low-risk score region, whereas attack data are distributed in relatively higher risk score regions. A certain level of separation is observed between the two distributions, indicating that the proposed risk scoring model can effectively distinguish between normal and anomalous behavior. Furthermore, the thresholds are determined based on these distribution characteristics and are utilized as criteria for performing progressive access control according to the level of risk.

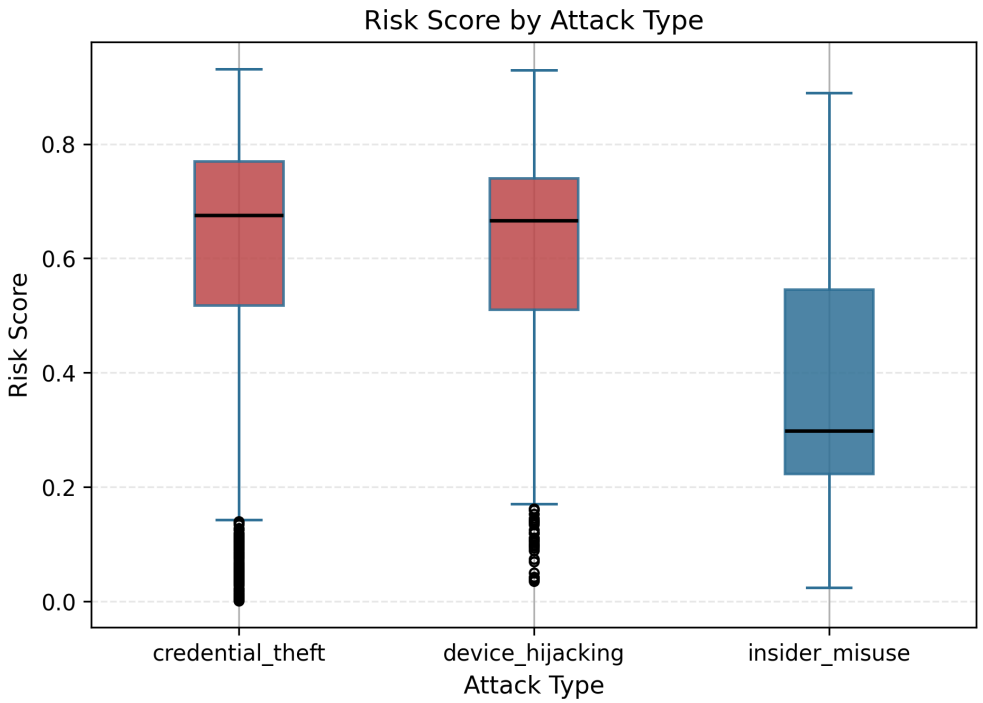

Figure 3: Risk score by attack type.

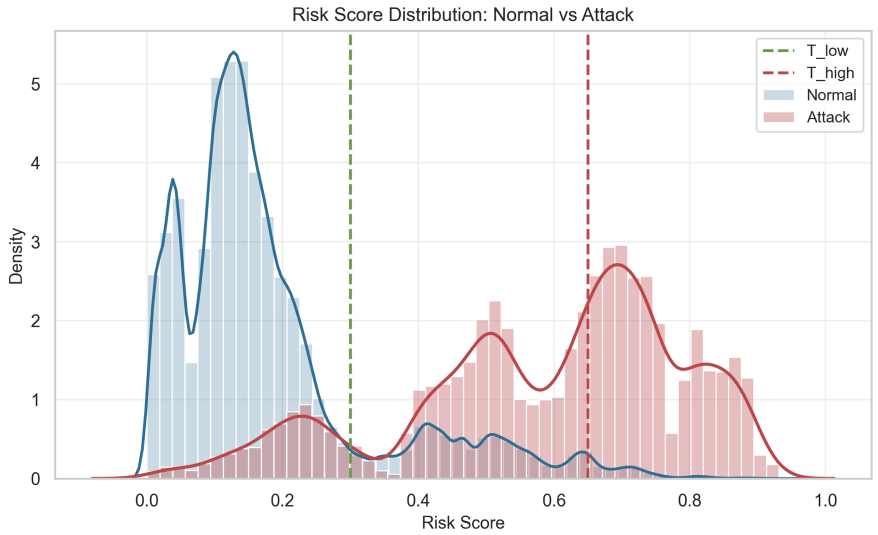

Figure 4: Risk score distribution: normal vs. attack.

4.4.4 Time-Based Risk Variation Analysis

Fig. 5 illustrates the dynamic variation of risk scores over time. During normal periods, the risk score remains relatively stable at a low level, whereas during attack periods, a sharp increase is observed. In particular, the attack intervals are highlighted with pink shading, within which the risk scores clearly tend to exceed the predefined thresholds. These results suggest that the proposed model can dynamically assess risk by incorporating temporal context. In other words, beyond evaluating anomalies at a single point in time, the

model enables more precise detection based on behavioral changes over time. Furthermore, the risk levels are categorized based on the thresholds T_{low} and T_{high}, and the corresponding policies—Permit, Step-Up, and Restrict—are applied appropriately according to the situation.

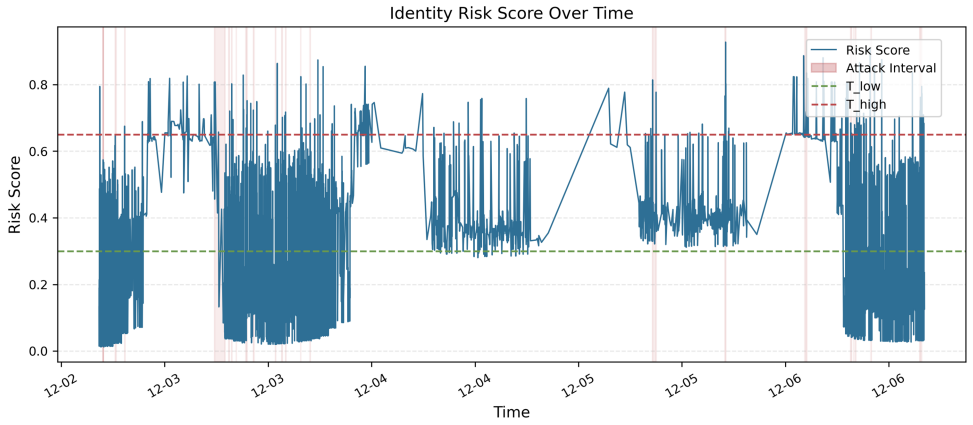

Figure 5: Identity risk score over time.

4.4.5 Policy Distribution Analysis

To evaluate the effectiveness of the risk-based access control policy, the distribution of policy decisions by attack type was analyzed, and the results are summarized in Table 8. According to Table 8, approximately 84.8% of normal behavior is classified as Permit, while the Restrict rate remains very low at 1.6%, indicating that unnecessary access restrictions on legitimate users are minimized. In contrast, for credential theft and device hijacking, the Restrict rates are relatively high at 58.9% and 53.9%, respectively, demonstrating that explicit anomalous behaviors are actively blocked. For insider misuse, the Permit rate is relatively higher and the Restrict rate is lower compared to other attack types, while the Step-Up rate is notably higher. This indicates that insider attacks, due to their similarity to normal behavior patterns, are more appropriately handled through progressive responses such as additional authentication rather than complete restriction. Overall, these results demonstrate that the proposed framework effectively connects dynamic identity risk assessment with progressive access control decisions, thereby addressing the static identity protection limitations discussed in Section 2.

Table 8: Policy decision distribution by attack type.

Attack Type	Permit (%)	Step-Up (%)	Restrict (%)
Credential Theft	3.8%	37.2%	58.9%
Device Hijacking	5.5%	40.6%	53.9%
Insider Misuse	50.3%	43.0%	6.5%
Normal	84.8%	13.6%	1.6%

4.4.6 Comparative Evaluation with Sequential Deep Learning Baseline

To address the limitation of relying solely on a lightweight anomaly detection model, an additional comparative experiment was conducted using a sequential deep learning baseline. Specifically, a Long Short-Term Memory Autoencoder (LSTM-AE) was implemented to model temporal identity behavior sequences. The LSTM-AE was trained under the same unsupervised anomaly detection setting as the proposed

framework, using only normal behavioral sequences extracted from the IoMT-extended dataset. To ensure a fair comparison, identical feature assumptions and anomaly detection conditions were maintained across both methods. A sliding temporal window of 20 consecutive identity events was used to capture sequential behavioral dependencies, and reconstruction error was employed as the anomaly score with threshold optimization based on validation performance. Table 9 summarizes the comparative performance between the proposed Isolation Forest-based framework and the LSTM-AE baseline.

Table 9: Comparative evaluation with sequential deep learning baseline.

Model	Learning Type	AUC	Precision	Recall	F1-Score
Proposed Framework (Isolation Forest)	Unsupervised	0.927	0.313	0.476	0.378
LSTM Autoencoder	Unsupervised	0.861	0.184	0.291	0.225

The comparative results indicate that the proposed lightweight framework outperformed the LSTM-AE baseline under the current experimental setting. Although the LSTM-AE benefited from temporal dependency modeling and achieved reasonably competitive anomaly detection performance, its overall precision, recall, and F1-score remained lower than those of the proposed framework. These findings suggest that while sequential modeling can improve anomaly sensitivity, lightweight ensemble-based anomaly detection remains more effective for highly imbalanced and structurally heterogeneous IoMT identity data. Table 10 presents the attack-specific comparison between the proposed framework and the LSTM-AE baseline.

Table 10: Attack-specific comparison between proposed framework and LSTM-AE.

Attack Type	Model	AUC	Block Rate	MTTD (Events)
Credential Theft	Proposed	0.948	0.589	0
Credential Theft	LSTM-AE	0.891	0.412	2
Device Hijacking	Proposed	0.954	0.539	6
Device Hijacking	LSTM-AE	0.903	0.381	4
Insider Misuse	Proposed	0.826	0.066	27
Insider Misuse	LSTM-AE	0.874	0.214	11

Attack-specific analysis revealed complementary detection characteristics between the two approaches. The proposed framework achieved stronger overall performance for credential theft and device hijacking attacks, whereas the LSTM-AE demonstrated improved sensitivity to insider misuse scenarios, where malicious behavior evolves gradually over time and exhibits temporal continuity. This suggests that sequence-aware deep learning models may offer advantages for behaviorally progressive attack patterns, although such benefits come at the cost of increased model complexity and computational overhead. These results suggest a practical trade-off between detection effectiveness and deployment efficiency. While sequential deep learning models provide richer temporal behavioral modeling capability, they require substantially greater computational resources, longer inference latency, and more extensive tuning. By contrast, the proposed Isolation Forest-based framework provides stronger overall detection effectiveness with a simpler and more deployment-friendly architecture, making it more suitable for latency-sensitive healthcare IoMT environments.

4.4.7 Scalability, Deployment Overhead, and Real-Time Applicability Analysis

The practical applicability of the proposed framework in healthcare IoMT environments depends on scalability, deployment overhead, and real-time operational feasibility. From a scalability perspective, the computational burden of the proposed framework primarily depends on the volume of identity-related event streams rather than the complexity of deep sequential model inference. Since Isolation Forest relies on tree-based anomaly scoring rather than high-parameter neural architectures, the inference workload remains comparatively lightweight and suitable for large-scale monitoring scenarios involving numerous users, devices, and access interactions. Regarding deployment overhead, the framework adopts a hybrid architecture in which blockchain is used exclusively for digital identity anchoring and credential integrity verification, while behavioral monitoring, anomaly detection, and risk scoring are executed off-chain. This design reduces blockchain transaction dependency during runtime decision making, thereby minimizing communication latency, storage overhead, and unnecessary cryptographic processing in latency-sensitive healthcare environments. For real-time applicability, healthcare IoMT systems require rapid access control decisions to avoid disrupting patient monitoring, emergency response, and clinical workflows. The proposed lightweight anomaly detection architecture is intentionally designed for near real-time identity risk evaluation, prioritizing fast anomaly scoring over computationally intensive temporal sequence modeling. Although full deployment-level latency benchmarking remains future work, the architectural design supports practical operational feasibility in real healthcare access control scenarios.

4.4.8 Adversarial Robustness Considerations

Adversarial robustness is an important practical consideration for AI-driven identity protection systems, particularly in healthcare IoMT environments where attackers may deliberately attempt to evade anomaly detection mechanisms. Several adversarial threat scenarios are relevant to the proposed framework. First, evasion attacks may occur when adversaries intentionally imitate legitimate behavioral patterns, such as normal access timing, familiar device usage, or expected contextual attributes, to reduce anomaly scores. Second, poisoning attacks may arise if malicious behavioral data are introduced into the training process, causing abnormal identity patterns to be incorporated into the normal behavioral baseline. Third, behavioral mimicry attacks are particularly relevant in digital identity protection, where attackers may gradually adapt their behavior to resemble legitimate users and thereby avoid triggering risk-based access control responses. Although the current study does not experimentally evaluate these adversarial scenarios, the proposed framework architecture provides several conceptual defense opportunities. Progressive access control policies, contextual verification, and multi-factor step-up authentication can partially mitigate simple evasion attempts. Nevertheless, robust protection against sophisticated adversarial manipulation remains an open research challenge. Future work will investigate adversarially robust anomaly detection, ensemble behavioral monitoring, adversarial training strategies, and graph-based identity behavior modeling to improve resilience against intelligent attack adaptation.

4.4.9 Implementation Feasibility and Security Implications

The practical deployment of the proposed framework in healthcare IoMT environments would require integration with existing hospital identity and access management infrastructures. In realistic deployment scenarios, the framework could operate as an identity-aware security layer positioned between authentication services and healthcare application access control mechanisms. For example, clinician authentication workflows, electronic medical record (EMR) access requests, remote telemedicine access sessions, and IoMT device communication requests could be continuously evaluated using dynamic identity risk assessment. From a cybersecurity perspective, the framework is particularly relevant to identity-centric attack scenarios

frequently observed in connected healthcare environments. Credential theft attacks may be detected through abnormal access timing, unfamiliar device usage, and contextual deviations. Insider misuse may be identified through gradual behavioral drift and unusual access frequency patterns. Device hijacking scenarios may be detected through device inconsistency and identity-context mismatch. Beyond attack detection, the proposed framework supports progressive security responses rather than rigid binary access control decisions. This characteristic is especially important in healthcare environments where immediate service denial may disrupt patient care or clinical workflows. Instead, moderate-risk situations may trigger step-up authentication, while high-risk situations may result in access restriction or alert generation. These characteristics position the proposed framework as a practical identity-aware cybersecurity architecture capable of improving operational resilience, identity trust management, and adaptive threat response in real-world healthcare IoMT environments.

5 Conclusion

The proliferation of the Internet of Medical Things (IoMT) is increasing the need for more adaptive and intelligent digital identity protection mechanisms in healthcare environments. Conventional identity management approaches based on static credentials and one-time authentication have limitations in effectively addressing identity-centric threats such as credential theft, insider misuse, and device compromise. In this study, digital identity is redefined as a dynamic security entity that evolves over time. Based on this perspective, we propose an AI-based digital identity protection framework that integrates a behavior-driven risk scoring model with a progressive access control policy. The proposed framework effectively captures the dynamic security requirements of IoMT environments through continuous authentication, adaptive risk assessment, and risk-based access control. Experimental results demonstrate that the proposed model effectively distinguishes between normal behavior and various attack scenarios, achieving an AUC of over 0.92. In particular, abrupt attacks such as credential theft and device hijacking are detected with high accuracy and low detection delay. For stealthy attacks such as insider misuse, the framework maintains a balance between security and usability through progressive response strategies. Furthermore, by maintaining a low False Restriction Rate for legitimate users, the framework ensures both service continuity and user convenience, which are critical in healthcare environments. These results suggest that modeling digital identity as a dynamic, risk-based entity—rather than a static attribute—and applying progressive response strategies based on risk scores can serve as an effective security approach in IoMT environments. However, this study relies on experiments conducted using extended public datasets, which may not fully capture the complex behavioral patterns present in real-world IoMT environments. This limitation is primarily due to the reliance on a proxy dataset, highlighting the need for domain-specific IoMT behavioral datasets. Future work should focus on validation using real healthcare data, comparative evaluation with advanced sequential deep learning models, robustness enhancement against adversarial behavioral manipulation, and tighter integration with blockchain-based digital identity systems to further improve practical deployment feasibility and scalability. Comparative evaluation with an LSTM-based sequential anomaly detection baseline further confirmed the trade-off between temporal behavioral modeling capability and lightweight deployment feasibility. While sequential deep learning models improved detection sensitivity for gradual insider misuse scenarios, the proposed framework remained more suitable for practical low-latency IoMT deployment.

Acknowledgement: The authors would like to thank Sun Moon University for its support of this research.

Funding Statement: This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the National Program for Excellence in SW, supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation) in 2026 (Project No. 2024-0-00023).

Author Contributions: Joong-Hyun Park: Writing & editing, Validation, Resources, Investigation. Jiho Choi: Formal analysis, Investigation. Libor Mesicek: Methodology, Conceptualization. Hoon Ko: Investigation, Validation, Supervisor. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The original data used in this study are publicly available through the CERT Insider Threat Dataset. The IoMT-extended dataset was generated through feature transformation and contextual mapping of the original CERT dataset. The processed dataset and supporting materials are available from the corresponding author upon reasonable request.

Ethics Approval: Not applicable.

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

References

1. Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak K-S. The internet of things for health care: a comprehensive survey. IEEE Access. 2015;3:678–708. doi:10.1109/ACCESS.2015.2437951.
2. Farahani B, Barzegari M, Shams Aliee F, Shaik K. Towards fog-driven IoT eHealth: promises and challenges. Future Gener Comput Syst. 2018;78(7):659–76. doi:10.1016/j.future.2017.04.036.
3. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput Netw. 2015;76(15):146–64. doi:10.1016/j.comnet.2014.11.008.
4. Alsubaei F, Abuhussein A, Shiva S. Security and privacy in the internet of medical things: taxonomy and risk assessment. In: Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops). Piscataway, NJ, USA: IEEE; 2017. p. 112–20. doi:10.1109/LCN.Workshops.2017.72.
5. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digit Med. 2019;2(1):98. doi:10.1038/s41746-019-0161-6.
6. Morse, Amyas, Investigation: WannaCry cyber attack and the NHS. Report by the National Audit Office. [cited 2026 Feb 5]. Available from:https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/.
7. Cameron K. The laws of identity. Microsoft Corporation. Technical Report. 2005 [cited 2026 Feb 5]. Available from: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.
8. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2016;18(2):1153–76. doi:10.1109/COMST.2015.2494502.
9. Prajapat S, Kumar P, Kumar D, Das AK, Hossain MS, Rodrigues JJPC. Quantum secure authentication scheme for internet of medical things using blockchain. IEEE Internet Things J. 2024;11(23):38496–507. doi:10.1109/JIOT.2024.3448212.
10. Wang Z, Guo Y, Guo Y. A blockchain-based medical IoT authentication scheme resistant to combined attacks. Comput Netw. 2025;263(16):111241. doi:10.1016/j.comnet.2025.111241.
11. Ferdous MS, Chowdhury F, Alassafi MO. In search of self-sovereign identity leveraging blockchain technology. IEEE Access. 2019;7:103059–79. doi:10.1109/ACCESS.2019.2931173.
12. Sommer R, Paxson V. Outside the closed world: on using machine learning for network intrusion detection. In: Proceedings of the IEEE Symposium on Security and Privacy. Piscataway, NJ, USA: IEEE; 2010. p. 305–16. doi:10.1109/SP.2010.25.
13. Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. ACM Comput Surv. 2009;41(3):15. doi:10.1145/1541880.1541882.
14. Patcha A, Park J-M. An overview of anomaly detection techniques. Comput Netw. 2007;51(12):3448–70. doi:10.1016/j.comnet.2007.02.001.
15. Apruzzese G, Colajanni M, Ferretti L, Guido A, Marchetti M. On the effectiveness of machine and deep learning for cyber security. In: Proceedings of the 10th International Conference on Cyber Conflict (CyCon); 2018 May 29–Jun 1; Tallinn, Estonia. p. 371–89. doi:10.23919/CYCON.2018.8405026.
16. Ksibi S, Jaidi F, Bouhoula A. MLRA-Sec: an adaptive and intelligent cyber-security-assessment model for internet of medical things (IoMT). Int J Inf Secur. 2025;24(1):21. doi:10.1007/s10207-024-00923-y.

17. Fridman L, Weber S, Greenstadt R, Kam M. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. IEEE Syst J. 2017;11(2):513–21. doi:10.1109/JSYST.2015.2472579.
18. Xiang X, Cao J, Fan W, Xiang S, Wang G. Blockchain-enabled dynamic trust management for the internet of medical things. Decis Support Syst. 2024;180(6):114184. doi:10.1016/j.dss.2024.114184.
19. Health Sector Coordinatiing Council Cybersecurity Working Group. Operational Continuity—Cyber Incident (OCCI), Version 1.1. Health Industry Cybersecurity; 2022. [cited 2026 Jun 30]. Available from: https://healthsectorcouncil.org/wp-content/uploads/2022/05/Operational-Continuity-Cyber-Incident-OCCI.pdf.
20. Jacobovitz O. Blockchain for identity management. Technical Report 16-02, Ben-Gurion University of the Negev. 2016 [cited 2026 Feb 5]. Available from: https://www.cs.bgu.ac.il/$\sim$frankel/TechnicalReports/2016/16-02.pdf.
21. Conti M, Dehghantanha A, Franke K, Watson S. Internet of things security and forensics: challenges and opportunities. Future Gener Comput Syst. 2018;78(6):544–6. doi:10.1016/j.future.2017.07.060.
22. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017;24(6):1211–20. doi:10.1093/jamia/ocx068.
23. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. In: Proceedings of the IEEE Open Big Data Conference. Piscataway, NJ, USA: IEEE; 2016. p. 25–30. doi:10.1109/BigData.2016.7840958.
24. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of the IEEE Security and Privacy Workshops. Piscataway, NJ, USA: IEEE; 2015. p. 180–4. doi:10.1109/SPW.2015.27.
25. Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Choo K-KR. Blockchain-based identity management systems: a review. J Netw Comput Appl. 2020;166(15):102731. doi:10.1016/j.jnca.2020.102731.
26. Jena SK, Barik RC, Priyadarshini R. A systematic state-of-the-art review on digital identity challenges with solutions using the conjugation of IoT and blockchain in healthcare. Internet of Things. 2024;25(10):101111. doi:10.1016/j.iot.2024.101111.
27. ISO/IEC 27799:2016. Health informatics—information security management in health using ISO/IEC 27002. Geneva, Switzerland: International Organization for Standardization; 2016.
28. U.S. Department of Health & Human Services. Health insurance portability and accountability act (HIPAA) security rule. 2013 [cited 2026 Feb 5]. Available from: https://www.hhs.gov/hipaa.
29. European Union. General data protection regulation (GDPR), regulation (EU) 2016/679. 2016 [cited 2026 Feb 5]. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
30. World Health Organization. Ethics and governance of artificial intelligence for health. Geneva, Switzerland: World Health Organization; 2021 [cited 2026 Feb 5]. Available from: https://www.who.int/publications/i/item/9789240029200.
31. Khan MA, Din IU, Almogren A. Securing access to internet of medical things using a graphical-password-based user authentication scheme. Sustainability. 2023;15(6):5207. doi:10.3390/su15065207.
32. Ameer S, Praharaj L, Sandhu R, Bhatt S, Gupta M. ZTA-IoT: a novel architecture for zero-trust in IoT systems and an ensuing usage control model. ACM Trans Priv Secur. 2024;27(3):1–36. doi:10.1145/3671147.
33. Kalaria R, Kayes ASM, Rahayu W, Pardede E, Shahraki AS. Adaptive context-aware access control for IoT environments leveraging fog computing. Int J Inf Secur. 2024;23(4):3089–107. doi:10.1007/s10207-024-00866-4.
34. Bhuva DR, Kumar S. A novel continuous authentication method using biometrics for IoT devices. Internet of Things. 2023;24(9):100927. doi:10.1016/j.iot.2023.100927.