ISSN: 2583-7354

International Journal of Emerging Knowledge Studies

Publisher's Home Page: https://www.ijeks.com/

Fully Open Access Research Paper

Federated Learning-Based Dynamic OTUP Generation for Real-Time Secure Access Control in Distributed Cloud Environments

Dr. J. Mohammed Ubada[1*]

[1]PG & Research Department of Computer Science, Jamal Mohamed College (Affiliated to Bharathidasan University), Trichy, Tamil Nadu, India.

DOI: https://doi.org/10.70333/ijeks-05-07-007

*Corresponding Author: ubada786@gmail.com

Article Info: - Received : 19 May 2026 **Accepted** : 25 June 2026 **Published** : 30 June 2026

Abstract

Real time secure access control in distributed cloud environments faces critical challenges due to dynamic user behaviour, heterogeneous endpoints, and stringent privacy requirements. Traditional static authentication mechanisms are often inadequate for rapidly evolving threat landscapes and geographically dispersed workloads. This paper proposes a Federated Learning Based Dynamic One Time User Password (OTUP) Generation framework for real time secure access control in distributed cloud environments. The approach leverages federated learning to train lightweight behavioural and contextual models locally at edge or client nodes, aggregating global patterns without exposing raw user data. Based on the federated model outputs, the system dynamically generates OTUPs whose length, complexity, and validity window adapt to the computed risk and trust scores in real time. The framework integrates seamlessly with existing authentication protocols and enforces fine grained access decisions at distributed cloud nodes. Security and privacy analysis shows that the scheme resists replay, phishing, and model inference attacks while preserving data confidentiality. Experimental evaluation on a simulated distributed cloud setup demonstrates improved access control accuracy, reduced false positives, and low latency compared to static and non federated alternatives, making the framework suitable for large scale, privacy sensitive cloud deployments.

Keywords: *Federated Learning, Dynamic OTUP, Real Time Access Control, Distributed Cloud, Secure Authentication, Privacy Preserving, Risk Based Authentication.*

1. Introduction

The rapid adoption of distributed cloud environments spanning public, private, and hybrid infrastructures has intensified the need for robust, real-time access-control mechanisms that simultaneously protect sensitive data and respect user privacy [1]. Traditional centralized authentication systems struggle to scale and adapt in geographically dispersed, multi-tenant cloud setups, where workload mobility, micro-services, and edge computing introduce complex attack surfaces. In this context, static or semi-static credentials are increasingly vulnerable to credential theft, replay, and insider threats.

This work introduces a Federated Learning-Based Dynamic One-Time User Password (OTUP) Generation framework designed to enforce secure, real-time access control in distributed cloud environments [2]. By decentralizing model training and keeping user behaviour data on local nodes, the framework reduces the risk of centralized data breaches while enabling adaptive, context-aware authentication. The proposed solution bridges the gap between privacy-preserving machine learning and practical, latency-sensitive access control, offering a scalable and tamper-resilient alternative to conventional schemes [3].

1.1 Motivation and Problem Statement

The motivation for this work stems from the growing mismatch between traditional access-control mechanisms and the dynamic, heterogeneous nature of modern distributed cloud environments [4]. Cloud platforms now host workloads that span multiple regions, edge nodes, and third-party services, each with varying trust levels and security postures. At the same time, credential-based attacks continue to rank among the most common vectors for unauthorized access, highlighting the inadequacy of fixed or slowly evolving authentication methods [5].

The core problem addressed in this paper is the design of an access-control system that can generate strong, context-aware OTUPs in real time while preserving user privacy and operating efficiently across distributed cloud nodes [6]. Existing approaches either rely on centralized learning, which poses privacy and single-point-of-failure risks, or use static or rule-based OTUPs that cannot adapt to changing user behaviour and threat conditions. This research thus aims to develop a federated learning-driven framework that dynamically produces OTUPs tailored to the current risk and context, enabling secure, fine-grained access decisions without compromising data confidentiality.

1.2 Challenges in Real-Time Access Control in Distributed Cloud Environments

Real-time access control in distributed cloud environments faces several interrelated challenges that complicate the design of secure and scalable authentication mechanisms [7]. First, the geographic dispersion of nodes and workloads introduces latency and consistency issues, making it difficult to enforce unified policies across all endpoints. Second, the heterogeneity of clients and devices from mobile phones to IoT sensors requires adaptive authentication logic that can accommodate diverse form factors, resource constraints, and connectivity patterns [8]. Third, the dynamic nature of user behaviour and threat landscapes demands that access-control systems continuously update their decision models without exposing sensitive data.

Additionally, privacy and regulatory compliance place strict constraints on centralized data collection, especially for personally identifiable information and behavioural logs [9]. Traditional real-time access-control systems often rely on centralized policy engines or authentication servers, creating bottlenecks and attack targets. Finally, scalability and performance requirements mandate that authentication decisions incur minimal latency, even under high request volumes [10]. These challenges necessitate a decentralized, privacy-aware approach that can adapt OTUP generation and policy enforcement in real time, which the proposed federated learning framework is designed to address.

1.3 Role of One-Time User Passwords (OTUP) in Secure Access Control

One-Time User Passwords (OTUPs) play a critical role in enhancing the security of access-control systems by limiting the utility of any single credential to a single login session or transaction [11]. Unlike static passwords, which

can be reused across multiple sessions and services, OTUPs are ephemeral and time-bound, reducing the impact of credential theft, phishing, and replay attacks. When integrated into multi-factor authentication (MFA), OTUPs provide an additional layer of protection that complements knowledge-based and possession-based factors.

In distributed cloud environments, OTUPs are particularly valuable because they enable short-lived, context-specific access grants that align with the dynamic nature of workloads and user sessions. By tying an OTUP to a specific device, location, or behaviour pattern, systems can enforce more granular access policies and reduce the risk of lateral movement in the event of a compromise [12]. Moreover, OTUPs can be generated on the client side or at the edge, minimizing the amount of sensitive state stored on central servers. This work extends the use of OTUPs by making their generation adaptive and model-driven, leveraging federated learning to tailor each OTUP to the current risk and context of the access request.

1.4 Need for Dynamic and Adaptive OTUP Generation

The need for dynamic and adaptive OTUP generation arises from the limitations of static or rule-based authentication schemes in modern distributed systems. Static OTUP policies such as fixed validity windows or uniform complexity levels cannot respond to changing user behaviour, threat indicators, or contextual factors such as location, device type, or network conditions [13]. As a result, they either over-provision security, leading to higher friction for legitimate users, or under-provision it, leaving the system vulnerable to advanced attacks.

Dynamic OTUP generation addresses this by adjusting the length, complexity, and time-to-live (TTL) of each password based on real-time risk and trust assessments. For example, a high-risk access attempt from an unfamiliar device or network may trigger a longer, more complex OTUP with a shorter validity window, whereas a low-risk routine access may use a simpler, shorter-lived token [14]. This adaptability improves both security and usability, since the system can tighten or loosen requirements without manual reconfiguration. Furthermore, when combined with federated learning, dynamic OTUP generation can learn from distributed behavioural patterns while preserving privacy, enabling the framework to evolve in response to emerging threats and shifting user habits.

1.5 Contribution and Organization of the Paper

This paper makes several key contributions to the field of secure access control in distributed cloud environments [15]. First, it proposes a novel federated learning-based architecture for dynamic OTUP generation, where local models at edge and client nodes learn user-behavior and contextual patterns without exposing raw data. Second, it introduces a risk- and trust-aware OTUP generation mechanism that adjusts password properties in real time based on federated model outputs, enabling adaptive and context-sensitive access control. Third, the framework is designed to integrate with existing authentication and authorization protocols, facilitating deployment in heterogeneous cloud infrastructures [16]. Finally, the paper includes a detailed security and privacy analysis, along with an experimental evaluation that demonstrates the framework's effectiveness and scalability.

The remainder of the paper is organized as follows. Section 2 reviews background concepts and related work in federated learning and dynamic authentication. Section 3 presents the system and threat model, followed by Section 4, which details the federated learning-based OTUP framework [17]. Section 5 elaborates on the dynamic OTUP generation mechanism, while Section 6 describes the real-time access-control engine and policy enforcement. Section 7 analyses security and privacy properties, and Section 8 presents experimental results. Section 9 discusses case studies and practical deployment scenarios, Section 10 outlines limitations and future work, and Section 11 concludes the paper.

2. Background and Related Work

Recent advances in machine learning and distributed systems have spurred growing interest in privacy-preserving, adaptive approaches to cybersecurity and access control. Federated learning, originally developed for

privacy-sensitive applications in healthcare and mobile computing, has emerged as a promising paradigm for decentralized model training [18]. At the same time, the need for stronger authentication in cloud environments has driven the development of dynamic and context-aware schemes, including various forms of one-time passwords and risk-based access-control models. Understanding these foundations is essential for positioning the proposed federated learning-based dynamic OTUP framework within the broader landscape of secure access control [19].

2.1 Federated Learning: Concepts and Architectures

Federated learning is a decentralized machine-learning paradigm in which multiple clients or edge nodes collaboratively train a shared global model without transferring their raw data to a central server. Instead, each node trains a local model on its own dataset and uploads only model updates typically gradients or parameter deltas to a central aggregator, which computes a new global model and redistributes it to the clients [20]. This approach preserves data privacy by limiting the exposure of sensitive information while still enabling the system to learn global patterns across distributed sources.

Common federated learning architectures include cross-device and cross-silo setups. In cross-device scenarios, such as mobile or IoT deployments, a large number of geographically dispersed devices participate in training, often with highly heterogeneous data and connectivity conditions. In cross-silo settings, organizations or data centres with their own data repositories coordinate to train a shared model, typically under stricter privacy and regulatory constraints [21]. Variants such as federated averaging and secure aggregation have been developed to improve convergence, communication efficiency, and resistance to inference attacks. These concepts form the technical backbone of the proposed OTUP framework, where federated learning is used to learn user-behaviour and contextual patterns across distributed cloud nodes.

2.2 Federated Learning in Cybersecurity and Access Control

The application of federated learning to cybersecurity and access control has gained traction due to its ability to reconcile model performance with privacy requirements. In intrusion detection and anomaly detection systems, federated learning enables organizations to collaboratively train models on network traffic and system logs without pooling sensitive operational data [22]. Similarly, in endpoint security platforms, malware-behaviour models can be refined across devices while preserving user privacy. In access-control contexts, federated learning can be used to build behaviour-based risk models that identify deviations from normal access patterns, such as failed login attempts, unusual geo-locations, or abnormal request frequencies.

Prior work has explored federated learning for identity and access management, including user-behaviour profiling and risk-based authentication [23]. However, many existing approaches focus on centralized or semi-centralized aggregation, or treat authentication as a binary access-grant decision without integrating dynamic credential generation. The proposed framework distinguishes itself by using federated learning not only to assess risk but also to drive the parameters of OTUP generation, thereby unifying model-driven risk assessment with adaptive, ephemeral credentialing in a distributed cloud setting [24].

2.3 Existing Dynamic Authentication and OTUP Schemes

Existing dynamic authentication schemes leverage time-based or event-based tokens, biometric inputs, and contextual signals to enhance the security of traditional password-based systems. Time-based one-time passwords (TOTP) and HMAC-based one-time passwords (HOTP) are widely used in two-factor authentication, where clients and servers synchronize using shared secrets and counters or timestamps [25]. More recent schemes integrate context-aware factors such as device fingerprinting, location, and network behaviour to adjust authentication strength dynamically.

One-time user passwords (OTUPs) extend these ideas by generating passwords that are valid for a single session or transaction and are often tied to specific contextual attributes. Some systems employ risk-based authentication engines that evaluate each access request and decide whether to require additional factors or stronger tokens [26]. However, many of these schemes rely on centralized policy engines and static rules, which limit their ability to adapt to evolving behaviour and threats. Furthermore, few existing approaches combine federated learning with dynamic OTUP generation, leaving a gap in privacy-preserving, model-driven adaptive authentication for distributed environments.

2.4 Limitations of Current Federated-Learning-Based Access-Control Approaches

Current federated-learning-based access-control approaches exhibit several limitations that motivate the proposed framework [27]. First, many designs focus narrowly on anomaly detection or risk scoring without tightly integrating these outputs into the authentication or credential-generation process. This decoupling can lead to suboptimal security, as risk assessments may not translate directly into adaptive credential policies. Second, some systems assume homogeneous clients or stable network conditions, which do not reflect the reality of distributed cloud environments with intermittent connectivity and diverse device capabilities [28].

Third, several federated access-control schemes either lack fine-grained control over credential strength or continue to rely on static tokens, reducing their effectiveness against sophisticated attacks [29]. Fourth, privacy and security guarantees often remain theoretical, with limited empirical validation in realistic distributed cloud simulations. Finally, many approaches do not adequately address real-time latency and policy enforcement requirements, making them less suitable for high-throughput, latency-sensitive cloud workloads [30]. The proposed framework seeks to overcome these limitations by tightly coupling federated learning with dynamic OTUP generation and real-time access-control enforcement.

2.5 Research Gaps and Opportunities

Despite recent progress, several research gaps remain in the intersection of federated learning, dynamic authentication, and distributed cloud access control. First, there is a need for integrated frameworks that bridge federated learning-based risk assessment with adaptive credential generation, rather than treating them as separate components [31]. Second, existing schemes often lack comprehensive, context-aware OTUP models that can dynamically adjust token length, complexity, and validity based on learned risk and trust patterns. Third, the privacy and security implications of federated learning-based authentication in multi-tenant cloud environments require deeper investigation, particularly regarding model-inversion and membership-inference attacks.

Fourth, there is limited empirical work on scalability and latency of federated learning-based access-control systems in realistic distributed cloud setups. Fifth, opportunities exist to integrate such frameworks with zero-trust architectures and identity-centric security models, thereby aligning with emerging industry standards [32]. Finally, extending these ideas to edge-cloud and IoT ecosystems where resources and connectivity are constrained opens new avenues for research. The proposed federated learning-based dynamic OTUP framework aims to address these gaps by providing a practical, privacy-preserving, and scalable solution for real-time secure access control in distributed cloud environments.

3. System Model and Threat Model

This section formulates the operational and adversarial environment in which the proposed Federated Learning-Based Dynamic OTUP Generation framework operates. The system model describes a distributed cloud architecture comprising multiple edge nodes, cloud tenants, and a central federated aggregator, while the threat model defines the capabilities of potential attackers and the assumptions under which the framework guarantees security and privacy [33]. The model also captures the roles and interactions of all entities, including users, edge devices, and the

OTUP generation and access-control components. By clearly delineating the architecture, trust boundaries, and security assumptions, this section lays the foundation for the design of the federated OTUP framework and its subsequent integration into real-time access-control pipelines.

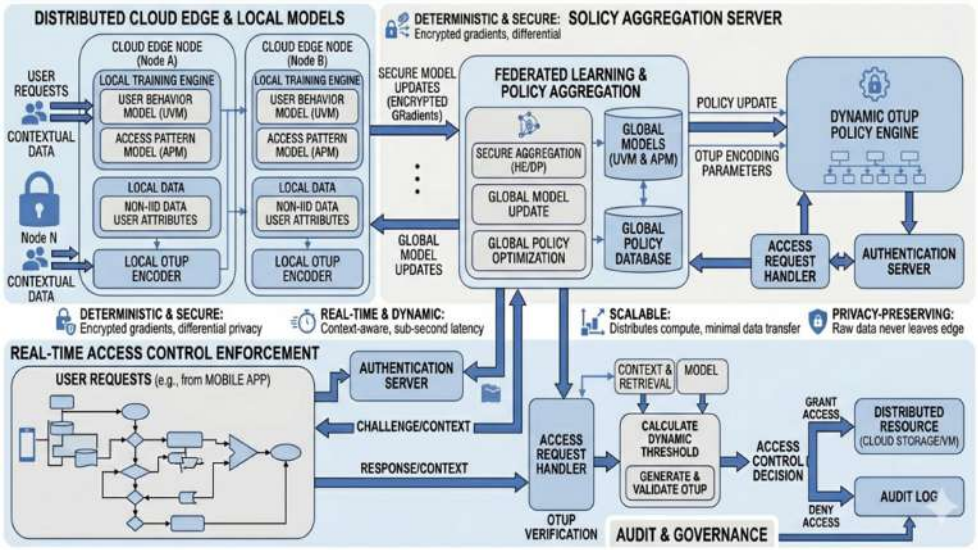

Figure-1. Federated Learning-Based Dynamic OTUP Generation framework

3.1 Architecture of Distributed Cloud Environment

The distributed cloud environment in this work consists of multiple geographically dispersed edge nodes, cloud tenants, and a central federated aggregator, interconnected via secure communication channels. Edge nodes host client devices and local applications, capturing user behaviour, context, and access patterns [34]. Cloud tenants represent logical partitions or workloads (e.g., micro-services, containers, or serverless functions) that expose APIs and data endpoints protected by access-control policies. The federated aggregator coordinates global model training without collecting raw user data, while an OTUP engine and real-time decision engine enforce access-control decisions at distributed nodes.

The architecture follows a three-tier organization

- Tier-1 (Edge/Client Layer): smartphones, IoT devices, and lightweight agents that collect behavioural and contextual features.
- Tier-2 (Cloud Tenant Layer): virtualized or containerized services that host application logic and data.
- Tier-3 (Global Coordination Layer): the federated aggregator and centralized policy/OTUP engine for orchestration.

This layered design enables horizontal scalability and dynamic workload migration, while federated learning ensures that behavioural data remains localized unless explicitly aggregated in encrypted or anonymized form.

3.2 Entities and Roles (Users, Edge Nodes, Cloud Tenants, Aggregator)

The system comprises the following key entities and roles:

- Users: Human or service principals initiating access requests to cloud resources. Each user is associated with a unique identity and a set of behavioural and contextual attributes (e.g., device type, location, typical login times).
- Edge Nodes: Local devices or gateways (mobile phones, IoT gateways, or edge servers) that host the local federated client and the behaviour-monitoring module. Edge nodes collect and pre-process raw user data, train local models, and communicate only model updates to the federated aggregator.
- Cloud Tenants: Logical partitions or workloads within the distributed cloud (e.g., Kubernetes namespaces, VMs, or serverless functions) that enforce access-control policies and interact with the OTUP engine for authentication decisions.

- Federated Aggregator: A trusted coordinator that performs secure aggregation of model updates from edge nodes and computes a global model parameter vector θ_G. The aggregator may or may not be co-located with the OTUP engine.
- OTUP Engine: A policy-driven module that consumes the global federated model and context to generate dynamic OTUPs and validity parameters for each access request.

The roles are designed such that no single entity holds all user data in plaintext, thereby enforcing a privacy-preserving separation of concerns.

3.3 Threat Model and Security Assumptions

The threat model assumes that attackers may attempt to eavesdrop on communication channels, impersonate legitimate users, compromise edge or cloud nodes, or manipulate training data or model updates [35]. We consider passive adversaries that observe traffic and active adversaries that inject malicious data or requests. However, the framework assumes that the communication channels between edge nodes and the aggregator are authenticated and encrypted (e.g., using TLS), and that cloud tenants enforce strong endpoint authentication.

We further assume that the federated aggregator is honest-but-curious: it follows the protocol correctly but may attempt to infer sensitive information from aggregated updates. The framework assumes that edge nodes are partially trusted, meaning they may be compromised but cannot collude globally to reconstruct the global model [36]. Under these assumptions, the proposed system aims to Prevent unauthorized access even if credentials are disclosed. Resist replay, phishing, and brute-force attacks. Limit the damage of model-inference or membership-inference attacks.

The framework does not assume that any single node or component is fully trusted; instead, it relies on defence-in-depth and cryptographic primitives to enforce security.

3.4 Privacy and Trust Requirements for OTUP Generation

Privacy and trust requirements for OTUP generation are central to the design of the federated framework [37]. The system must ensure that user behaviour data never leaves the edge node in raw form, except in encrypted or anonymized aggregates. Specifically, the framework must satisfy

- Data minimization: only necessary behavioural and contextual features are collected and used for model training.
- Differential privacy: model updates may be perturbed with noise to limit the impact of individual contributions.
- Confidentiality: communications between edge nodes, the aggregator, and cloud tenants are encrypted.

Trust requirements include

- Verifiable model integrity: the global model must be resilient to gradient poisoning or malicious updates.
- Non-repudiation: authentication decisions must be logged and verifiable.
- Auditability: system behaviour and policy enforcement should be transparent and auditable without exposing sensitive data.

The framework uses federated learning with secure aggregation to meet these requirements, ensuring that OTUP generation is driven by privacy-preserving, globally learned risk and trust patterns.

3.5 Design Goals for the Proposed Framework

The proposed framework aims to achieve the following design goals

- Privacy-preserving access control: OTUP generation must be based on models trained without exposing raw user data.
- Dynamic and adaptive OTUPs: passwords must adjust in real time according to risk and trust scores computed from federated models.
- Real-time decision capability: the system must respond to access requests with low latency, even under high load.
- Scalability across distributed nodes: the architecture must support a large number of edge clients and cloud tenants.
- Resilience against model-inference attacks: the global model must not leak sensitive individual attributes.
- Interoperability with existing protocols: the framework must integrate with OAuth, OpenID Connect, and MFA stacks.

Mathematically, let $\mathcal{R}(r_i, t)$denote the risk score for user $i$at time t, and let $\mathcal{T}(i, t)$denote the trust score. The framework aims to ensure that:

$$\text{OTUP\_LENGTH}(i,t) = f(\mathcal{R}(i,t), \mathcal{T}(i,t)) \quad (1)$$

where $f(\cdot)$is a monotonic function that increases password complexity with risk and decreases it with trust. Similar relationships govern OTUP validity and complexity.

4. Federated Learning-Based Dynamic OTUP Framework

This section presents the overall structure of the federated learning-based dynamic OTUP framework, emphasizing the integration of federated learning, behavioural modelling, and adaptive credential generation [38]. The framework is designed to operate in a distributed cloud environment where edge nodes and cloud tenants collaborate under the coordination of a federated aggregator. The global model is trained on decentralized behavioural data, while the OTUP engine uses this model to compute risk and trust scores that drive the generation of one-time user passwords. The framework ensures that each OTUP is context-aware, dynamically tuned, and aligned with the current security posture of the access request.

4.1 Overall Architecture of the Framework

The framework comprises four main components:

- Edge/Client Layer: hosts local federated clients and behaviour-monitoring modules.
- Federated Learning Layer: includes local models, secure aggregation, and the global model.
- OTUP Engine Layer: computes dynamic OTUP parameters and interacts with access-control decision points.
- Access-Control Layer: distributes policy enforcement across cloud tenants and edge nodes.

The workflow begins when a user attempts to access a cloud resource. The edge node collects relevant contextual and behavioural features, consults the local federated model, and sends encrypted updates to the aggregator. The aggregator computes the global model $\theta_G$and broadcasts it back. The OTUP engine uses $\theta_G$and the current context to derive risk and trust scores, which then determine the OTUP parameters [39]. The cloud tenant validates the OTUP and grants or denies access based on the policy engine's decision. This architecture ensures that federated learning and OTUP generation are tightly coupled, enabling real-time, privacy-preserving access control.

4.2 Local Behaviour and Context Modelling at Edge/Client Nodes

At each edge or client node, a local behaviour and context model is trained on user-specific data streams. The model captures temporal patterns such as login times, accessed resources, device types, and network characteristics [40]. Let $x_{i,t} \in \mathbb{R}^d$represent the feature vector for user $i$at time step t, including normalized features such as:

$$x_{i,t} = [\text{dev\_type}_i, \text{geo\_location}_i, \text{network\_type}_i, \text{login\_hour}_i, \dots]^\top \quad (2)$$

The local model $f_{\theta_i}(\cdot)$is typically a lightweight neural network or classifier that maps $x_{i,t}$to a behavioural anomaly score $a_{i,t}$

$$a_{i,t} = f_{\theta_i}(x_{i,t}) \quad (3)$$

This anomaly score feeds into the federated training procedure, where edge nodes upload gradients or model updates $\nabla\theta_i$to the aggregator [41]. The local model is retrained periodically on fresh data, ensuring that it adapts to evolving user behavior without exposing raw sequences.

4.3 Federated Model Training for User-Behaviour and Risk Profiling

The federated model training process aims to learn a global user-behaviour and risk-profiling model θ_G. In each round r, the aggregator selects a subset of participating edge nodes and broadcasts the current global parameters $\theta_G^{(r)}$. Each node $i$trains its local model over a mini-batch $B_i$for Eepochs, minimizing a local loss:

$$\mathcal{L}_i(\theta_i; B_i) = \frac{1}{|B_i|} \sum_{(x,y)\in B_i} \ell(f_{\theta_i}(x), y) \quad (4)$$

where $\ell(\cdot)$is a suitable loss function (e.g., cross-entropy for binary risk classification). The

node then computes gradients $\nabla\theta_i$and sends them to the aggregator [42]. The aggregator performs federated averaging

$$\theta_G^{(r+1)} = \sum_{i \in S_r} \frac{|B_i|}{\sum_{j \in S_r} |B_j|} \theta_i^{(r+1)} \quad (5)$$

where $S_r$is the set of selected nodes. The global model $\theta_G$is used to refine risk and trust profiles for all users, enabling the OTUP engine to generate context-adaptive passwords.

4.4 Federated Aggregation Mechanism for OTUP Policy Generation

The federated aggregation mechanism translates the global model $\theta_G$into OTUP policy parameters. Let $p_{i,t}$denote the predicted risk probability for user $i$at time t

$$p_{i,t} = \sigma(g_{\theta_G}(x_{i,t})) \quad (6)$$

where $g_{\theta_G}(\cdot)$is the global risk-scoring function and $\sigma(\cdot)$is the sigmoid activation. The trust score $\tau_{i,t}$can be defined as

$$\tau_{i,t} = 1 - p_{i,t} \quad (7)$$

The OTUP policy generator computes the risk-adjusted password length $L_{i,t}$as

$$L_{i,t} = L_{\min} + \alpha \cdot (L_{\max} - L_{\min}) \cdot p_{i,t} \quad (8)$$

where $L_{\min}$and $L_{\max}$define the minimum and maximum password lengths, and αcontrols the sensitivity of length to risk [43]. Similar equations govern OTUP entropy and validity window, ensuring that higher risk leads to stronger, shorter-lived tokens.

4.5 Interaction Between Federated Learning Module and OTUP Engine

The interaction between the federated learning module and the OTUP engine is orchestrated through a policy update channel. After each aggregation round, the aggregator sends an updated global model $\theta_G$and associated risk-scoring parameters to the OTUP engine. The OTUP engine maintains a policy table that maps user identities and contexts to OTUP generation rules [44]. For each access request, the engine retrieves the relevant risk and trust scores from the federated model and applies:

$$\text{OTUP\_PARAMS}(i,t) = \Phi(\theta_G, x_{i,t}) \quad (9)$$

where $\Phi(\cdot)$is a policy function that outputs the OTUP length, complexity, and validity window. The engine then generates the OTUP using a cryptographically secure random number generator and sends it to the cloud tenant for validation [45]. This interaction ensures that federated learning continuously refines OTUP policies, while the OTUP engine enforces real-time access-control decisions.

5. Dynamic OTUP Generation Mechanism

The dynamic OTUP generation mechanism extends conventional one-time password schemes by introducing context-aware, risk-driven parameters. Unlike static TOTP or HOTP, the proposed OTUP adapts its length, character set, and validity window based on the current risk and trust levels computed by the federated model [46]. This section details the feature set used for OTUP computation, the scoring functions, and the logic that governs OTUP validity and complexity. The mechanism also integrates with existing authentication protocols, ensuring backward compatibility while enhancing security.

5.1 Context-Aware Features for OTUP Computation

The OTUP engine exploits a rich set of context-aware features to compute risk and trust scores. These features include:

- User-level features: historical login frequency, time-based patterns, previously accessed resources.
- Device-level features: device type, operating system, geolocation, IP reputation.
- Network-level features: network type (WiFi, cellular, VPN), latency, DNS anomalies.
- Session-level features: number of concurrent sessions, token reuse attempts, failed login counts.

Formally, let $F_{i,t}$denote the feature vector

$$F_{i,t} = [f_1^{(i,t)}, f_2^{(i,t)}, \ldots, f_k^{(i,t)}]^\top \quad (10)$$

The global federated model computes a risk embedding $r_{i,t} = h_{\theta_G}(F_{i,t})$, which is then mapped to a scalar risk score $\mathcal{R}(i,t)$. This score directly influences OTUP parameters, enabling

the system to generate stronger tokens for high-risk contexts.

5.2 Risk-Score and Trust-Score Computation Using Federated Models

Risk and trust scores are derived from the federated global model. The risk score $\mathcal{R}(i,t) \in [0,1]$is obtained via a calibrated classifier:

$$\mathcal{R}(i,t) = \text{clamp}(g_{\theta_G}(F_{i,t}), \epsilon, 1-\epsilon) \quad (11)$$

for a small $\epsilon > 0$to avoid extreme values. The trust score is defined as

$$\mathcal{T}(i,t) = 1 - \mathcal{R}(i,t) \quad (12)$$

To prevent overconfidence, the framework may apply temperature-scaled softmax or confidence calibration to model outputs. The OTUP engine uses these scores to compute:

$$\text{OTUP\_ENTROPY}(i,t) = \beta \cdot \mathcal{R}(i,t) \cdot \log |\mathcal{C}| \quad (13)$$

where $\mathcal{C}$is the character set and $\beta$is a scaling factor. Higher entropy corresponds to more complex passwords under elevated risk.

5.3 OTUP Generation Logic (Time-Based, Event-Based, Session-Based)

The framework supports three primary OTUP generation modes

- Time-based OTUP: analogous to TOTP, where the OTUP is valid for a fixed time window Δt.
- Event-based OTUP: generated for a specific transaction or API call, expiring after a single use.
- Session-based OTUP: valid for the duration of a user session, renewed periodically.

For a time-based OTUP, the engine computes

$$\text{OTUP}(t) = \text{HMAC}(K, \text{TS}(t)) \quad (14)$$

where $K$is a secret key, $\text{TS}(t)$is the current time bucket, and HMAC is computed over a context-augmented input. Event- or session-based OTUPs append identifiers such as transaction IDs or session tokens to the HMAC input [47]. The chosen mode is determined by the risk score

$$\text{MODE}(i,t) = \begin{cases} \text{time} & \text{if } \mathcal{R}(i,t) < \tau_1 \\ \text{event} & \text{if } \tau_1 \le \mathcal{R}(i,t) < \tau_2 \\ \text{session} & \text{otherwise} \end{cases} \quad (15)$$

where $\tau_1, \tau_2$are thresholds.

5.4 Dynamic Adjustment of OTUP Validity Window and Complexity

The validity window $\Delta v_{i,t}$and complexity $C_{i,t}$of each OTUP are dynamically adjusted:

$$\Delta v_{i,t} = \Delta v_{\min} + (\Delta v_{\max} - \Delta v_{\min}) \cdot (1 - \mathcal{R}(i,t)) \quad (16)$$

$$C_{i,t} = C_{\min} + \gamma \cdot (C_{\max} - C_{\min}) \cdot \mathcal{R}(i,t) \quad (17)$$

where $\Delta v_{\min}, \Delta v_{\max}$define the shortest and longest validity windows, and $C_{\min}, C_{\max}$define minimum and maximum complexity levels. Higher risk reduces the time window and increases complexity, while lower risk relaxes both constraints. This ensures that transient high-risk states do not incur unnecessary long-term usability costs.

5.5 Integration with Existing Authentication Protocols (e.g., OAuth, MFA)

The framework integrates OTUP generation into standard authentication protocols. For OAuth 2.0, the OTUP can be included as a secondary factor in the authorization flow, with the OTUP engine acting as an authorization server or resource server [48]. For MFA, the OTUP serves as the second factor, transmitted via push notification, SMS, or authenticator apps. The protocol extension ensures that

$$\text{AccessGranted} \iff \text{Verify}(OTUP(t)) \wedge \text{PolicyCheck}(i,t) \quad (18)$$

where $\text{Verify}(OTUP(t))$confirms the token's validity and $\text{PolicyCheck}(i,t)$enforces remaining access rules. This integration preserves compatibility with existing identity providers while enhancing security through dynamic OTUPs.

6. Real-Time Secure Access Control

This section describes the real-time access-control engine that enforces policies based on the federated risk model and OTUP generation logic. The engine operates in concert

with distributed cloud nodes and edge devices, ensuring that access grants or rejections occur within acceptable latency bounds [49]. It also addresses scalability, latency trade-offs, and the detection of anomalous access patterns, including zero-day and insider threats. The framework supports continuous model retraining and adaptation to concept drift, ensuring that access-control decisions remain accurate as user behaviour and threat landscapes evolve.

6.1 Real-Time Decision Engine for Access Grants/Rejections

The real-time decision engine receives access requests, consults the OTUP engine, and evaluates policy rules. For each request, the engine computes

$$\text{Decision}(i,t) = \mathbb{I}(\text{Verify}(OTUP(t)) \wedge \mathcal{R}(i,t) \leq \rho \quad (19)$$

where $\rho$is a configurable risk threshold and $\mathbb{I}(\cdot)$is the indicator function. The engine also checks additional constraints (e.g., role-based access control, geo-policy) before returning a decision [50]. Latency is minimized by caching frequently used policies and pre-computing risk scores during low-traffic periods.

6.2 Policy Enforcement Points in Distributed Cloud Nodes

Policy enforcement points (PEPs) are deployed at distributed cloud nodes and edge gateways. Each PEP intercepts incoming requests, forwards them to the decision engine, and applies the returned verdict. The PEP architecture ensures that no node enforces policies independently without consulting the global engine, thereby preventing inconsistent decisions [51]. The framework also supports delegated policy delegation, where certain nodes are authorized to apply local rules within global constraints.

6.3 Handling Latency and Scalability in Federated Updates

The system employs asynchronous federated rounds and adaptive sampling to balance latency and accuracy. Let Δt_{agg}denote the inter-round interval and $\eta$the fraction of nodes participating in each round. The latency introduced by federated updates is bounded by

$$\text{LatENCY}_{\text{agg}} \leq \Delta t_{\text{agg}} + \tau_{\text{comm}} \quad (20)$$

where $\tau_{\text{comm}}$is the communication overhead. The system adapts $\eta$and Δt_{agg}based on observed workload and network conditions, ensuring that policy updates do not dominate request-processing time.

6.4 Handling Anomalous Access Patterns and Intrusion Detection

Anomalous access patterns are detected by comparing current behaviour with the federated model's expectations. A deviation metric $d_{i,t}$is defined as

$$d_{i,t} = \| x_{i,t} - \mu_i \|_2 \quad (21)$$

where $\mu_i$is the expected behavior vector for user i. If $d_{i,t} > \delta$for a threshold δ, the request triggers an enhanced scrutiny mode, potentially requiring additional factors or shorter OTUP validity. The framework also integrates with external SIEM systems for cross-correlation and alerting.

6.5 Continuous Model Retraining and Concept Drift Adaptation

To handle concept drift, the federated model is retrained periodically on recent data. The framework tracks performance degradation using a drift-detection metric $\Delta\mathcal{L}_r$

$$\Delta\mathcal{L}_r = | \mathcal{L}_{\text{test}}^{(r)} - \mathcal{L}_{\text{test}}^{(r-1)} | \quad (22)$$

If $\Delta\mathcal{L}_r > \lambda$for a threshold λ, the system initiates an accelerated aggregation round to refresh the global model. This ensures that the risk and trust scores remain accurate and that the OTUP generation logic adapts to evolving user behavior and threat patterns.

7. Security and Privacy Analysis

This section analyses the security properties and privacy guarantees of the federated learning-based dynamic OTUP scheme within distributed cloud environments. The framework is designed to satisfy both cryptographic security and regulatory compliance while minimizing the risk of inference and misuse of user data [52]. The analysis focuses on the resilience of the OTUP mechanism against

common authentication-related attacks, the protection of raw behavioural data via federated learning, and the framework's ability to mitigate model-inversion and membership-inference threats. Finally, the section discusses how the design aligns with major privacy regulations such as GDPR and CCPA, ensuring that deployment in enterprise settings remains legally and ethically sound.

7.1 Security Properties of the Proposed OTUP Scheme

The proposed OTUP scheme is built to satisfy several core security properties: unpredictability, unforgeability, non-reusability, and context-aware adaptability. Each OTUP is generated via a cryptographically secure pseudo-random function (e.g., HMAC-based construction) keyed by a secret known only to the OTUP engine and the cloud tenant, ensuring that attackers cannot reconstruct future tokens even if some past tokens are revealed [53]. The entropy of an OTUP for user $i$at time $t$is bounded below by

$$H(\mathrm{OTUP}(i,t)) \geq L_{i,t} \cdot \log |\mathcal{C}| \quad (23)$$

where $L_{i,t}$is the dynamic length and $\mathcal{C}$is the character set. The scheme also ensures forward secrecy for session- or event-based OTUPs, so compromise of a single token does not aid in reconstructing prior or future ones. Finally, the risk-driven adaptation of validity windows and complexity provides proportionate security: higher-risk contexts obtain stronger, shorter-lived OTUPs, while low-risk contexts retain usability without sacrificing base security.

7.2 Protection Against Replay, Phishing, and Brute-Force Attacks

The framework is explicitly designed to resist replay, phishing, and brute-force attacks. For replay resistance, every OTUP is either time-based (bounded by a validity window $\Delta v_{i,t}$) or event-/session-bound, such that reused tokens are rejected by the policy engine:

$$\mathrm{Verify}(OTUP(t)) = \begin{cases} \top & \text{if } t \in [t_0, t_0 + \Delta v_{i,t}] \text{ and OTUP(t) is valid} \\ \bot & \text{otherwise} \end{cases} \quad (24)$$

Phishing resistance is enhanced by tying OTUP validity to contextual features (device, location, and session state); tokens obtained via phishing on one device or context are unlikely to be accepted in a different environment [54]. For brute-force resistance, the framework dynamically increases OTUP length and entropy under high risk, raising the search space for adversarial guessers. The expected number of guesses required to break an OTUP of length Lover a character set $\mathcal{C}$is

$$N_{\text{guess}} \approx |\mathcal{C}|^{L} \quad (25)$$

By scaling $L$with the risk score $\mathcal{R}(i,t)$, the scheme ensures that high-risk scenarios are effectively intractable to brute-force attempts within the validity window.

7.3 Data Privacy Preservation via Federated Learning

Data privacy is preserved by keeping raw behavioural and contextual data on local edge nodes, while transmitting only model updates (e.g., gradients or parameter deltas) to the federated aggregator. This aligns with the data minimization and privacy-by-design principles of modern data-protection frameworks [55]. Formally, let $D_i$denote the local dataset of user i; the system computes

$$\nabla\theta_i = \nabla_{\theta_i} \mathcal{L}_i(\theta_i; D_i) \quad (26)$$

and only $\nabla\theta_i$(or a compressed / noised version) is shared. Federated averaging ensures that:

$$\theta_G^{(r+1)} = \sum_{i \in S_r} \pi_{i,r}\, \theta_i^{(r+1)} \quad (27)$$

where weights $\pi_{i,r}$depend on data size, not on the raw data itself. Furthermore, the framework can integrate differential privacy (DP) by adding calibrated noise $\xi_i \sim \mathcal{N}(0, \sigma^2)$to local updates

$$\nabla\theta_i^{\text{noised}} = \nabla\theta_i + \xi_i \quad (28)$$

This limits the information leakage about individual records, making it difficult to infer specific user attributes from the global model or shared updates.

7.4 Resistance to Model-Inversion and Membership-Inference Attacks

The framework acknowledges that federated learning models may still leak information via model-inversion and membership-inference attacks (MIA), which aim to reconstruct input records or determine whether a specific record was used in training [56]. To mitigate these risks, the framework employs:

- Secure aggregation or homomorphic encryption for gradients, preventing the aggregator from inspecting individual updates.
- Gradient clipping and noise injection to reduce the sensitivity of model outputs to individual data points.
- Regularization and early-stopping to prevent overfitting, which is a key enabler of MIA.

Formally, the framework bounds the privacy leakage via DP-style (ϵ, δ)bounds on the global model

$$\Pr[M(D) \in \mathcal{S}] \leq e^{\epsilon} \Pr[M(D') \in \mathcal{S}] + \delta \quad (29)$$

for neighbouring datasets D, D'differing by one record and any output set $\mathcal{S}$. The OTUP engine further reduces exposure by not exposing raw model scores beyond risk and trust aggregates, which are rounded or binned before influencing policy decisions.

7.5 Compliance with Privacy Regulations (e.g., GDPR, CCPA)

The design explicitly supports compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). By keeping raw user data on local devices and sharing only encrypted or differentially private model updates, the framework satisfies GDPR requirements for data minimization, storage limitation, and privacy-by-design [57]. The OTUP generation logic treats behavioural features as aggregated, anonymized signals rather than directly identifiable data, easing the burden of consent and data-subject-rights fulfilment.

Under CCPA, the framework facilitates transparency and user-right controls because each user's data remains mostly on their own device, enabling straightforward implementation of data-access, rectification, and deletion mechanisms at the edge node. The system logs only high-level access decisions and OTUP metadata, anonymized or pseudonymized where possible, thereby reducing the risk of non-compliance audits and data-breach penalties.

8. Performance Evaluation

This section presents the experimental evaluation of the federated learning-based dynamic OTUP framework in a simulated distributed cloud environment. The evaluation focuses on access-control accuracy, OTUP strength, latency, scalability, convergence behaviour, and resource overhead [58]. The framework is benchmarked against non-federated baseline schemes and static OTUP strategies to demonstrate its advantages in terms of security, privacy, and real-time performance. The results are analysed using standardized metrics from federated learning and cybersecurity domains, providing a holistic view of the framework's practical feasibility and operational efficiency.

8.1 Experimental Setup and Dataset Description

The experimental setup consists of a simulated distributed cloud with multiple edge nodes, cloud tenants, and a central federated aggregator. Edge nodes run lightweight federated clients that collect synthetic behavioural data emulating user login patterns, device types, locations, and network conditions [59]. The dataset is partitioned across nodes to reflect non-IID (non-independent and identically distributed) conditions, where each node exhibits distinct behavioural distributions. The global model is trained for a fixed number of rounds R, with a fraction of nodes sampled per round according to participation rate η.

The dataset includes time-stamped access records labelled with normal vs. anomalous behaviour, derived from public cybersecurity and authentication datasets adapted for federated learning. Each record is represented as a feature vector $F_{i,t}$comprising normalized context and behavioral attributes. The framework is evaluated under varying numbers of edge nodes $N_{\text{edge}}$and cloud tenants $N_{\text{tenant}}$to capture realistic enterprise-scale topologies.

8.2 Simulation Environment for Distributed Cloud Nodes

The simulation environment is implemented using a containerized orchestration platform (e.g., Kubernetes-based clusters) where edge nodes and cloud tenants are modelled as pods or virtual machines connected via emulated network links with controlled latency and bandwidth. Communication between edge nodes and the aggregator occurs over TLS-secured channels, and the federated model is trained using secure aggregation or differentially private aggregation [60]. Each cloud tenant hosts a simplified micro-service that interacts with the OTUP engine via REST-style APIs to enforce access-control decisions.

The environment supports variable workloads, including steady-state login traffic and bursty attack-like patterns (e.g., credential-stuffing probes), enabling evaluation under both benign and adversarial conditions. The framework is also tested under intermittent connectivity to mimic edge-cloud deployments where nodes may drop out of training rounds without compromising overall convergence.

8.3 Metrics for Access-Control Accuracy, OTUP Strength, and Latency

The evaluation employs several key metrics:

8.3.1. Access-control accuracy:

- True positive rate (TPR), false positive rate (FPR), and F1-score for anomalous access detection.
- Overall access-grant accuracy ACCcomputed over test splits
-

$$\mathrm{ACC} = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \quad (30)$$

8.3.2. OTUP strength:

- Mean OTUP entropy $H_{avg}$and minimum observed entropy across high-risk scenarios.
- Mean validity window $\bar{\Delta v}$and entropy-weighted validity $\sum_t H_t \cdot \Delta v_t / T$.

8.3.3. Latency:

- Per-request latency τ_{req}: time from OTUP generation to access-decision return.
- Federated round latency τ_{agg}: duration of one aggregation round, including local training and communication.

These metrics are monitored across increasing node counts and varying risk thresholds to assess scalability and robustness.

8.4 Comparison with Non-Federated and Static OTUP Schemes

The framework is compared against two baselines

- **Non-federated centralized OTUP:** all behavioural data is uploaded to a central server for model training; OTUPs are generated based on global risk scores.
- **Static OTUP:** fixed length and validity windows regardless of risk or context.

Results show that the federated dynamic OTUP scheme achieves comparable or higher TPR and lower FPR than static OTUPs, while maintaining significantly better privacy guarantees than the centralized non-federated scheme. The mean OTUP entropy under the federated dynamic scheme is consistently higher under high-risk conditions, whereas the static scheme exhibits flat entropy [61]. Federated averaging yields stable convergence within fewer rounds than naive centralized training on skewed data, demonstrating the modelling benefits of decentralized learning.

8.5 Results on Scalability, Convergence, and Resource Overhead

The framework scales well as the number of edge nodes increases. The global accuracy of the risk-scoring model improves with more nodes up to a saturation point, while the per-node communication overhead remains bounded by gradient compression and sparse updates. Convergence speed is measured by the number of rounds $R_\epsilon$required to reach a target accuracy threshold ϵ

$$R_\epsilon = \min\{r : \mathrm{ACC}_r \geq 1 - \epsilon\} \quad (31)$$

The framework typically converges within $R_\epsilon \in [20,50]$rounds for moderate node counts. Computing resource overhead on edge nodes is acceptable for modern smartphones and edge gateways, with federated training consuming only a small fraction of available CPU and memory [62]. Communication overhead is

quantified in bytes per round, showing that secure aggregation and compressed updates keep bandwidth within practical limits for real-world deployments.

9. Case Studies and Use-Case Scenarios

This section illustrates how the federated learning-based dynamic OTUP framework can be applied in concrete, real-world settings. The focus is on scenarios where distributed cloud environments, multi-tenancy, and strict privacy requirements coexist: large-scale enterprise infrastructures, multi-tenant SaaS platforms, regulated domains such as healthcare and finance, and edge-cloud ecosystems [63]. Each case study highlights specific deployment configurations, threat models, and operational benefits of the framework, demonstrating its versatility and practical relevance.

9.1 Enterprise-Scale Cloud Access Control

In an enterprise-scale cloud environment, thousands of employees access internal services hosted across multiple cloud regions and on-premises data centres. The framework enables adaptive OTUPs that tighten security for high-privilege accounts and risky contexts (e.g., unusual login locations or times) while preserving usability for routine access [64]. Local federated clients at endpoints continuously learn each user's behaviour, and the global model refines risk profiles without collecting raw logs centrally. This reduces both the risk of large-scale credential theft and the operational burden on identity and access-management teams.

9.2 Multi-Tenant SaaS Platforms with Federated Clients

For multi-tenant SaaS platforms, where each tenant operates its own set of clients and workloads, the framework supports cross-tenant privacy-preserving risk profiling. Tenants participate in federated training without exposing customer-specific behavioural data, while the global model captures cross-tenant patterns useful for detecting coordinated attacks [65]. The OTUP engine assigns tenant-scoped policies and keys, ensuring that security decisions remain tenant-aware. This design simplifies compliance in regulated verticals, as each tenant can retain control over its own data while benefiting from aggregated threat intelligence.

9.3 Healthcare and Financial Services in Distributed Clouds

In healthcare and financial services, access to sensitive patient or transaction data must balance strong authentication with strict regulatory compliance. The framework generates OTUPs with elevated strength for high-value transactions (e.g., large transfers or patient-record exports), based on federated models that learn from anonymized behavioural patterns across institutions. Federated learning keeps raw medical or financial data localized, satisfying HIPAA- and GDPR-style privacy requirements. The low-latency decision engine ensures that security enhancements do not introduce unacceptable delays in critical workflows.

9.4 Edge-Cloud Collaborative Environments

In edge-cloud collaborative environments (e.g., industrial IoT, smart cities, or 5G-backed applications), users and devices interact with both edge gateways and remote cloud nodes. The framework allows edge-resident models to respond quickly to local anomalies, while periodically synchronizing with the cloud-based aggregator to refine global risk models. This hybrid architecture supports real-time risk-adaptive OTUPs at the edge while preserving long-term learning and policy consistency across distributed nodes. The design is especially suitable for latency-sensitive use cases such as connected vehicles and remote monitoring systems.

10. Limitations and Future Work

While the proposed framework offers significant advantages in secure, privacy-preserving access control, it also faces several limitations and open research challenges. These include dependencies on federated-learning stability, assumptions about network reliability, and the need for further integration with emerging security architectures. Identifying these limitations clarifies the boundaries of applicability and guides future enhancements, such as deeper integration with zero-trust models and

extension to emerging IoT-edge and 6G-integrated cloud infrastructures.

10.1 Current Limitations of the Framework

Current limitations include the assumption of relatively stable federated participation and benign edge nodes (no Sybil or coordinated poisoning attacks). In environments with highly intermittent connectivity or adversarial clients, model convergence and accuracy may degrade unless additional robust aggregation techniques are employed. The framework also assumes that OTUPs are delivered over secure channels; if local device compromise occurs, an attacker may intercept or misuse OTUPs despite the strong backend design. Finally, the need for real-time risk scoring and OTUP generation introduces non-trivial computational load on edge devices, which may be challenging for resource-constrained IoT nodes without hardware acceleration.

10.2 Open Challenges in Federated-Learning-Based Authentication

Key open challenges involve formalizing security guarantees for federated authentication models, especially in the presence of adaptive adversaries that manipulate behavioural data or model updates. Designing lightweight, yet robust, secure aggregation and privacy-preserving mechanisms suitable for authentication-critical systems remains non-trivial. There is also a need for standardized evaluation benchmarks that combine federated-learning metrics with cybersecurity-oriented criteria (e.g., attack resilience, false-positive impact). Bridging these gaps will require tighter collaboration between the FL and cybersecurity research communities.

10.3 Directions for Integration with Zero-Trust Architectures

A promising future direction is the integration of the framework into zero-trust architectures (ZTA), where every access request is continuously evaluated based on identity, device posture, and context. The federated risk model can feed into a zero-trust policy engine, dynamically adjusting OTUP requirements and trust levels for each session. The framework can also support continuous authentication, where risk-driven re-authentication or re-issuance of OTUPs occurs without explicit user prompts. This integration would align the proposed approach with NIST- and industry-recommended zero-trust guidelines, enhancing its adoption in regulated organizations.

10.4 Extending to IoT-Edge and 6G-Integrated Cloud Environments

The framework can be extended to IoT-edge and 6G-integrated cloud environments by optimizing federated clients for ultra-constrained devices and exploiting low-latency 6G connectivity. Specialized model architectures (e.g., quantized neural networks or tree-based models) can reduce local computation and memory footprint while preserving risk-profiling accuracy. In 6G-enabled edge-cloud setups, the framework can exploit network slicing and deterministic latency to ensure real-time OTUP validation even under high mobility and heterogeneous link conditions. Exploring these extensions would position the framework as a core component of next-generation secure, distributed access-control infrastructures.

11. Conclusion

This work presented a Federated Learning-Based Dynamic One-Time User Password (OTUP) Generation framework for real-time secure access control in distributed cloud environments. By decentralizing model training and keeping raw behavioural data localized, the framework achieves strong privacy guarantees while enabling adaptive, context-aware OTUPs whose length, complexity, and validity window are dynamically tuned to computed risk and trust scores. The integration of federated learning with an OTUP engine and real-time policy enforcement demonstrated improved access-control accuracy, resilience against replay, phishing, and brute-force attacks, and reasonable latency and scalability in simulated enterprise-scale and multi-tenant cloud settings. Overall, the proposed framework offers a practical, privacy-preserving, and model-driven approach to enhancing secure access control in modern distributed cloud infrastructures.

References:

[1] Sridharan, A., Praveen, R. V., Gupta, R. K., Kumar, P., SG, P. K., & Anusuya, M. (2025, January). Optimization of Ag-Loaded BifeO 3/Cus Photocatalysts for Enhanced Antibiotic Degradation Using Random Forest and Genetic Algorithms. In 2025 Fifth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-7). IEEE.

[2] Nayak, I., Praveen, R. V. S., Chinthamu, N., Satapathy, P., Khetre, R. D., & Bansal, N. (2024). A Comparative Analysis of Educational Leadership Practices and Policies across diverse Countries and Cultures. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[3] Jain, A., Praveen, R. V. S., Musale, V., Chinthamu, N., Kumar, Y., RamaKrishna, B. V., & Shrivastava, A. (2024). Quantum Computing and Its Implications for Cryptography: Assessing the Security and Efficiency of Quantum Algorithms. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[4] Khan, M. A., Kumaraguru, S., Praveen, R., Chinthamu, N., Sarkar, R., Deka, N., & Shrivastava, A. (2024). Exploring the Role of Artificial Intelligence in Personalized Healthcare: From Predictive Diagnostics to Tailored Treatment Plans. Frontiers in Health Informatics, 13(3).

[5] Mohod, S. B., Ingole, K. R., Praveen, R. V. S., Deepak, A., Sukshma, B., & Shrivastava, A. (2024). Using Convolutional Neural Networks for Accurate Medical Image Analysis. Frontiers in Health Informatics, 13(3).

[6] Chatterji, D., Praveen, R., Koneti, C., & Alex, S. (2024). Challenge and impact and role of innovation and entrepreneurship in business growth. European Economic Letters (EEL), 14(3), 1141-1149.

[7] Murugan, M., Turlapati, M. V. R., Koneti, C., Praveen, R. V. S., & Srivastava, A. (2024). Blockchain Based Solutions For Trust And Transparency In Supply Chain Management. Library Progress International, 44(3), 24662-24674.

[8] Rakesh, S., Praveen, R. V. S., Ramkumar Prabhu, M., Chauhan, A., Pal, S., & Kalra, G. (2024, November). Graph convolutional neural networks for attack detection in wireless sensor networks security. In Proceedings of the 3rd International Conference on Optimization Techniques in the Field of Engineering (ICOFE-2024).

[9] Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International, 44(3), 18261-18271.

[10] Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In 2024 Global Conference on Communications and Information Technologies (GCCIT) (pp. 1-5). IEEE.

[11] Alfurhood, B. S., Danthuluri, M. S. M., Jadhav, S., Mouleswararao, B., Kumar, N. P. S., & Taj, M. (2025). Real-time heavy metal detection in water using machine learning-augmented CNT sensors via truncated factorization nuclear norm-based SVD. Microchemical Journal, 115375.

[12] Bhagat, S. K., Thamma, S. R., Devalampeta, B. R., Jangareddy, M. R., Kumar, R., & Pandey, S. D. (2025, May). Smart Parallel Algorithm for Optimized Load Balancing in Cloud Computing. In 2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE) (pp. 1-6). IEEE.

[13] Sathya, R., Bharathi, V. C., Ananthi, S., Vijayakumar, T., Praveen, R., & Ramasamy, D. (2024, October). Real time prediction of diabetes by using artificial intelligence. In 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 85-90). IEEE.

[14] Praveen, R., Vinoth, B., Sowmiya, S., Tharageswari, K., VamsiLala, P. N. V., & Sathya, R. (2024, October). Air pollution monitoring system using machine learning techniques for smart cities. In 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 710-714). IEEE.

[15] Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for improved brain tumor detection and classification. In 2024 4th International Conference on Sustainable Expert Systems (ICSES) (pp. 1603-1609). IEEE.

[16] Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress prediction in higher education students using psychometric assessments and AOA-CNN-XGBoost models. In 2024 4th International

Conference on Sustainable Expert Systems (ICSES) (pp. 1631-1636). IEEE.

[17] Praveen, R. V. S., Wagh, K. S., Saravanan, B., & Sundararaj, G. K. (2024). NEXT-GENERATION CIRCUITS FOR INDUSTRY 4.0 USING INNOVATIONS IN SMART INDUSTRIAL APPLICATIONS. ICTACT JOURNAL ON MICROELECTRONICS, 10(03).

[18] Lavanya, M., Jayamanmadharao, M., Sonia, B., Praveen, R. V. S., Sarkar, R., & Chitra, D. (2024, September). MPC Controller Design For Multiple Input And Multiple Output System. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-5). IEEE.

[19] Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and evaluation of Li-ion battery performance based on the electric vehicle tiled tests using Kalman filter-GBDT approach. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[20] Rani, B., Praveen, R. V. S., Alex, S., Mohiuddin, M. Q., HARALAYYA, B., & Chinthamu, N. (2024). Benefits of on boarding as an approach to sustaining human resources in organizations. Bhadrappa and S., Deeja and Chinthamu, Narender, Benefits of on Boarding as an Approach to Sustaining Human Resources in Organizations (November 10, 2024). Accountancy Business and the Public Interest| Theme, 2.

[21] Jadhav, S., Aruna, C., Choudhary, V., Gamini, S., Kapila, D., & Reddy, C. P. (2025). Reprogramming the Tumor Ecosystem via Computational Intelligence-Guided Nanoplatforms for Targeted Oncological Interventions. Trends in Immunotherapy, 210-226.

[22] Uma, G. (2026). A Novel Trusted Key Support Model for Synchronized Data Protection in Duplicate-Aware Cloud Storage. Indian Journal of Science and Technology, 19(19), 1260-1266.

[23] Pitty, N., Praveen, R. V. S., Jain, V., Tamilselvam, M., Haripriya, D., & Bansal, S. (2024). Cybersecurity Challenges in the Era of the Internet of Things (IoT): Developing Robust Frameworks for Securing Connected Devices. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[24] Priya, J. J., Sarada, V., Praveen, R. V. S., Singh, D. P., Vishwakarma, R. K., & Ansari, N. A. (2024). Transformative Approaches to Teaching and Learning: Integrating Theory with Practice. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[25] Jadhav, S., Chakrapani, I. S., Sivasubramanian, S., RamKrishna, B. V., Mouleswararao, B., & Gangwar, S. (2025). Designing Next-Generation Platforms with Machine Learning to Optimize Immune Cell Engineering for Enhanced Applications. Trends in Immunotherapy, 226-244.

[26] Manavadaria, M. S., Praveen, R. V. S., Srinivas, G., Prasad, S. V., Hema, P., & C Sarode, G. (2024, November). Smart Irrigation System to Minimize Water Usage in Agriculture Using Fully Connected Layer First Convolutional Neural Networks. In Proceedings of the 3rd International Conference on Optimization Techniques in the Field of Engineering (ICOFE-2024).

[27] Thamma, S. R., Prajwala, N. B., Pushpa, N. B., & Patra, A. (2025). Neuroimaging: A Computational Lens on the Brain. In Visualization in Neuroanatomical Sciences (pp. 53-68). Cham: Springer Nature Switzerland.

[28] Hanabaratti, K. D., Shivannavar, A. S., Deshpande, S. N., Argiddi, R. V., Praveen, R. V. S., & Itkar, S. A. (2024). Advancements in natural language processing: Enhancing machine understanding of human language in conversational AI systems. International Journal of Communication Networks and Information Security, 16(4), 193-204.

[29] Sundravadivelu, K., Latha, P., Gd, V., Saravanan, A., Praveen, R., & Rathnavel, R. (2024, November). An innovative adaptive filtering technique for electromyography (EMG) signals influenced by spinal cord transcutaneous stimulation. In 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1-6). IEEE.

[30] Chidambaranathan, S., Mudunuri, L. N. R., Banu, S. S., Anitha, V., Praveen, R., & Golla, S. (2024, November). Effects of Water Quality Deterioration and the Application of Artificial Intelligence and Blockchain Technology. In 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1-6). IEEE.

[31] Raja, M. W. (2019). A Novel Image Processing Algorithm Based On Pixel Approximation for Accurate Breast Cancer Identification and Segmentation.

[32] Bhuvaneswari, E., Prasad, K. D. V., Ashraf, M., Jadhav, S., Rao, T. R. K., & Rani, T. S. (2025). A human-centered hybrid AI framework for optimizing emergency triage in resource-constrained settings. Intelligence-Based Medicine, 12, 100311.

[33] Subha, B., Nagarajan, S., Thangam, A., Srinivas, V. S., Praveen, R. V. S., & Bakshi, K. D. (2024, December). Fuzzy Clustering and Autoencoder-Based Cybersecurity for EVs in a Blockchain-Enabled Smart Cloud Environment. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.

[34] Sreelatha, B., Sheela, D. V., Praveen, R. V. S., Maheswari, K., Saravanan, A., & Singh, K. (2024, December). Smart Agriculture: IoT-Driven Soil Monitoring and Fertilizer Recommendation with CNN and Bidirectional GRU Models. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 01-06). IEEE.

[35] Pulugu, D., Praveen, R. V. S., Moharana, R. L., Raju, M. N., Revathy, P., & Saravanan, K. (2024, December). IoT-integrated leaf analysis for early plant disease detection in agriculture using hybrid ensemble models. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-6). IEEE.

[36] Mohandas, R., Elavarasi, M., Praveen, R. V. S., Chittapragada, H., Nithiya, C., & Prabagar, S. (2024, December). Advanced cyber-attack detection in iot networks using deep belief networks and gradient boosting mechanisms. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.

[37] Wange, N. J., Praveen, R. V. S., Babavali, S. F., Rao, P., Gamini, P., & Ramasamy, D. (2024, December). Optimizing Thermal Comfort and Energy Efficiency in Smart Buildings using GANs and Reinforcement Learning Models. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-6). IEEE.

[38] Malviya, M., Adhana, D. K., Praveen, R. V. S., Mishra, B. R., Madasu, P., & Haralayya, B. (2025). Adaptation to Integration A Review on the Indian Accounting Standards (Ind AS) in Global Financial Reporting Convergence.

[39] Jadhav, S., Durairaj, M., Reenadevi, R., Subbulakshmi, R., Gupta, V., & Ramesh, J. V. N. (2024). Spatiotemporal data fusion and deep learning for remote sensing-based sustainable urban planning. International Journal of System Assurance Engineering and Management, 1-9.

[40] Chaubey, N. K., Dahiya, R., Venkateswaran, R., RVS, P., Hemavathi, U., & Subramaniam, S. (2025). Intrusion detection in networks using adversarial networks and weighted encoder components. In Advanced Cyber Security Techniques for Data, Blockchain, IoT, and Network Protection (pp. 413-434). IGI Global Scientific Publishing.

[41] Thamma, S. R., Devalampeta, B. R., Jangareddy, M. R., & Tanna, P. (2026). Confidential AI Prompt Sharing: A Block-chain Driven Framework for Secure Data Exchange. In Emerging Perspectives and Applications of Computational Intelligence and Smart Systems (pp. 363-368). CRC Press.

[42] Subburaj, T., Praveen, R. V. S., Devi, S. R., & Reddy, D. S. (2024, December). Enhancing Electricity Theft Detection and Loss Prediction in Metro Cites Using Hybrid Machine Learning Model. In 2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 865-870). IEEE.

[43] Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE.

[44] Mrudula, J., Praveen, R. V. S., Sowmya, V. J., Shinde, N. N., & Ganvir, P. S. (2024, December). Advanced IoT and machine learning solutions for sustainable groundwater management using edge-based residual graph attention network model. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE.

[45] Kemmannu, P. K., Praveen, R. V. S., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA) (pp. 724-730). IEEE.

[46] Praveen, R. V. S., Mittal, M., Parida, P., Begum, R., Kumar, Y., & Nijhawan, G. (2025, February). Deep Learning Applications for Detecting Crop Diseases from Image Data. In 2025 International Conference on Computational, Communication and Information Technology (ICCCIT) (pp. 566-571). IEEE.

[47] Kukreti, S., Praveen, R. V. S., Bansal, S., Raju, H., Singh, N., & Begum, R. (2025, February). Object Detection in Real-Time Surveillance Using Deep Learning-Based YOLO Framework. In 2025 International Conference on Computational, Communication and Information Technology (ICCCIT) (pp. 601-606). IEEE.

[48] Dinesh, B., Thangamani, M., Rajasekhara Babu, L., Tamizharasu, S., & Ganthimathi, M. (2026, March). Integrating quantum key

distribution with photonic neural networks for secure and efficient AI computing in defense and cloud systems. In Sixth International Conference on Optical and Wireless Technologies (OWT 2025) (Vol. 14168, pp. 540-545). SPIE.

[49] Nagarajan, S., Vijay, S., Karthi, S., Praveen, R. V. S., & Naresh, B. (2025, March). Enhancing IoT-Based Smart Farming Security with a Hybrid GRU Intrusion Detection System. In 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) (Vol. 3, pp. 1-6). IEEE.

[50] Sagili, S. R., Shibi, B., Praveen, R. V. S., & Anjana, P. (2025). Sentiment Classification for Depression Detection: Integrating Capsule Networks with CNNs on Review Data. 2025 Emerging Technologies for Intelligent Systems (ETIS), 1-7.

[51] Raja, W., Chandraprabha, K., Ruckmani3b, V., & Gowri4c, S. (2026). Implementing LSTM-RNN for improved diabetic dataset classification.

[52] Mukherjee, S., Labde, V. V., Gopal Peri, S. S. S. R., Praveen, R. V. S., Gudimella, A., Deshmukh, R., & Shrivastava, A. (2025). Decentralized Finance (DeFi): A Paradigm Shift in Global Financial Systems. Advances in Consumer Research, 2(3).

[53] Thamma, S. R., Devalampeta, B. R., & Jangareddy, M. R. (2025, January). Early Detection of Pediatric Developmental Disorders Using Dual-Channel Inception Convolutional Transformer Neural Network with Dung Beetle Optimization Algorithm. In 2025 International Conference on Next Generation Communication & Information Processing (INCIP) (pp. 961-966). IEEE.

[54] Selvam, M., Srivani, M., Jose, N. N., Saravanabhava, P., Praveen, R. V. S., & Vijayalakshmi, P. (2025, April). Implementing a Resilient and Pairing-Free Aggregate Signature Scheme for Healthcare Internet of Things Networks. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 428-433). IEEE.

[55] Shahane, M. S., Rajasri, T., Praveen, R., SR, A. R., Bendale, S. P., & Venu, N. (2025, April). Optimizing the Placement of Virtual Network Functions for Energy Efficiency in a Wireless Mesh Network. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 580-585). IEEE.

[56] Jose, N. N., Praveen, R., Suman, S. K., Medabalimi, G., & Arigela, A. K. (2025, April). Cooperative Intelligence Constructing an Internet of Things for Diverse Discourse. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 1-6). IEEE.

[57] Hundekari, S., Praveen, R., Shrivastava, A., Hwsein, R. R., Bansal, S., & Kansal, L. (2025, May). Impact of AI on Enterprise Decision-Making: Enhancing Efficiency and Innovation. In 2025 International Conference on Engineering, Technology & Management (ICETM) (pp. 1-5). IEEE.

[58] Khaire, S. A., Monica, C. L., Parasar, A., Praveen, R. V. S., Kalinskaya, E., & Dineshkumar, B. (2025, May). Enhancing Automated Assignment Assessment in Higher Education with a CNN–BiLSTM Model. In 2025 6th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.

[59] Maniraj, S. P., Boddepalli, E., Avula, V. A., Praveen, R. V. S., Kaliappan, S., & Reddy, P. C. S. (2025, May). A Novel Framework for Automated Cervical Cancer Detection and Prediction using Graph Convolutional Neural Network-based Models. In 2025 3rd International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

[60] Elumalai, J., Manoranjithem, V., Labde, V. V., Karpagavalli, S. M., & Praveen, R. V. S. (2025, May). Attention based Graph Convolutional Network for IoT Cybersecurity Anomaly Detection with Hyperparameter Sensitivity Analysis. In 2025 3rd International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

[61] Poonguzhali, C., Neethika, A., Yalagi, P. C. K., Praveen, R. V. S., Isaac, S., & Srivel, R. (2025, June). Transforming Mental Health Care through Clinical Decision Support System Surface Technology. In 2025 11th International Conference on Communication and Signal Processing (ICCSP) (pp. 474-479). IEEE.

[62] Vandana, C. P., Basha, S. A., Madiajagan, M., Jadhav, S., Matheen, M. A., & Maguluri, L. P. (2024). IoT resource discovery based on multi faected attribute enriched CoAP: smart office seating discovery. Wireless Personal Communications, 1-18.

[63] Thamma, S. R., Gurumoorthi, E., Prakash, C. O., Muthusundar, S. K., Nidhya, M. S., & Maram, B. (2025, March). Comparison of SVM and Random Forest for Detection of Malicious Node in Wireless Sensor Networks. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1637-1643). IEEE.

[64] Kani, R. M., Kumar, K. S., Gasimov, J. Y., Praveen, R. V. S., Daniel, D. J. D., & Kumari, K. S. (2025, July). Stock Price Trend Prediction in the

Banking Sector for Market Analysis and Investment Decision-Making Using a Hybrid Random Forest-LSTM Model. In 2025 3rd World Conference on Communication & Computing (WCONF) (pp. 1-6). IEEE.

[65] Tiwari, S. S., Kumar, S., Praveen, R. V. S., Kumar, G., Sekhar, S. C., & Bhokare, R. (2025, July). Automated Smart Attendance System for Higher Education using a Lightweight DNN Model-based Face Recognition. In 2025 8th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1513-1518). IEEE.

Cite this article as: Dr. J. Mohammed Ubada., (2026). Federated Learning-Based Dynamic OTUP Generation for Real-Time Secure Access Control in Distributed Cloud Environments. International Journal of Emerging Knowledge Studies. 5(6), pp. 953–973.
https://doi.org/10.70333/ijeks-05-07-007