ISSN: 2583-7354

International Journal of Emerging Knowledge Studies

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

Fully Open Access Research Paper

Blockchain-Integrated Multi-Level Access Control with Biometric-Driven One-Time User Password (OTUP) for Zero-Trust Cloud Security

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-05-07-005

*Corresponding Author: ubada786@gmail.com

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

Abstract

Cloud computing has transformed digital service delivery, but it has also widened the attack surface for identity theft, credential abuse, insider misuse, and data exfiltration. Traditional perimeter-based defences are insufficient in modern distributed environments where users, devices, and services interact across multiple trust boundaries. This article proposes a blockchain-integrated multi-level access control framework using biometric-driven one-time user passwords (OTUP) to strengthen zero-trust cloud security. The model combines decentralized identifiers, verifiable credentials, biometric verification, blockchain-backed smart contracts, and continuous trust scoring to provide fine-grained and tamper-resistant access control. The framework improves accountability through immutable audit trails, reduces dependence on centralized identity repositories, and strengthens authentication by binding OTUP generation to verified biometric presence. It is designed for enterprise and regulated cloud environments where security, traceability, and policy consistency are critical.

Keywords: *Zero-trust Security, Blockchain, Biometric Authentication, OTUP, Decentralized Identity, Cloud Access.*

1. Introduction

Cloud platforms support agility, scalability, and remote accessibility, but they also expose organizations to complex cyber risks that cannot be managed through static perimeter controls alone. As workloads move across hybrid and multi-cloud infrastructures, security models must verify every user, device, and transaction continuously. This article introduces a blockchain-enabled access control architecture that integrates biometric verification and OTUP-based authentication within a zero-trust framework [1]. The aim is to create a secure, auditable, and adaptive cloud access

environment that resists credential abuse, insider compromise, and log tampering while maintaining fine-grained authorization across resource sensitivity levels.

1.1. Evolution of cybersecurity threats in cloud environments

Cloud threats have evolved from simple unauthorized access incidents to sophisticated attacks involving credential theft, lateral movement, API exploitation, and compromised endpoints. Attackers increasingly target identity systems because cloud services are heavily dependent on remote authentication and privilege delegation [2]. Multi-tenant infrastructure, rapid workload scaling, and extensive API usage have introduced new opportunities for misconfiguration and stealthy intrusion. At the same time, remote work and unmanaged devices have blurred organizational boundaries, making trust decisions more difficult. These developments show that cloud security can no longer depend on network location or a single authentication event [3]. Instead, security must be dynamic, identity-centered, and continuously enforced across every resource interaction.

1.2. Limitations of traditional security models

Traditional security models rely on the assumption that once a user enters a protected network, that user can be trusted for a broad range of actions. This assumption fails in cloud environments because users, devices, applications, and services operate across distributed and rapidly changing infrastructures [4]. Static role assignment, password-based authentication, and centralized logging do not provide sufficient defence against compromised credentials or malicious insiders. In addition, perimeter-based controls struggle to secure APIs, microservices, and third-party integrations. These limitations create gaps in visibility, accountability, and policy enforcement. As a result, organizations need security mechanisms that evaluate each access request in context, verify identity repeatedly, and reduce dependence on centralized control points that can become attractive attack targets [5].

1.3. The need for zero-trust architectures

Zero-trust architecture is built on the principle that no user, device, or application should be trusted by default, even when operating inside an organizational environment. Every access request must be explicitly authenticated, authorized, and validated against current context. This approach is especially relevant for cloud systems, where workloads are distributed and threat actors can exploit small identity weaknesses to gain broad access [6]. Zero trust strengthens least-privilege enforcement, reduces lateral movement, and supports adaptive policy decisions based on behavior, device posture, and resource sensitivity. When combined with blockchain and biometric verification, zero trust gains stronger auditability and more resilient identity assurance, making it suitable for high-value cloud deployments that require traceable and tamper-resistant access governance.

2. Literature Review

Recent studies show increasing convergence between blockchain, decentralized identity, multifactor authentication, and zero-trust cloud security. Researchers have explored blockchain-based identity management, smart contract access control, biometric verification, and privacy-preserving authentication for distributed systems [7]. While each of these areas has matured individually, fewer studies present an integrated framework that combines all of them into a unified cloud access control model. The literature suggests that decentralized trust, strong identity proof, and immutable logging are essential for securing dynamic cloud environments, but operational trade-offs in scalability, latency, and interoperability remain important concerns.

2.1. Blockchain-based authentication and access control systems

Blockchain has been widely studied as a decentralized mechanism for storing authentication events, enforcing policies, and maintaining tamper-resistant records [8]. In access control contexts, smart contracts can automate authorization decisions and ensure that policy execution is transparent and consistent across participating nodes. Blockchain also reduces dependence on a single

centralized identity repository, which lowers the risk of catastrophic compromise. Permissioned networks are especially attractive for enterprise use because they provide stronger control over validators and improved performance relative to public chains [9]. However, blockchain-based access systems can still face latency challenges and require careful design to avoid exposing sensitive identity data. Current literature supports blockchain as a strong foundation for secure, auditable access management when paired with privacy-aware identity mechanisms.

2.2. Biometric authentication methods

Biometric authentication has become a strong alternative to password-only login because biometric traits are more closely bound to the legitimate user than memorized credentials [10]. Fingerprint, face, iris, and behavioural biometrics are commonly used to verify identity, often as part of multifactor authentication systems. Modern biometric engines use advanced feature extraction and matching methods to improve reliability, but they also face risks such as spoofing, sensor noise, and privacy leakage. Liveness detection and protected template storage are therefore essential design requirements. In cloud security, biometrics are particularly useful because they establish physical-user presence and reduce the risk of credential sharing [11]. The literature supports biometric authentication as a powerful identity layer when combined with secure processing, template protection, and contextual risk evaluation.

2.3. One-time password (OTP) mechanisms

One-time password mechanisms improve authentication security by generating credentials that are valid for only a short period or a single transaction. Unlike static passwords, OTPs are less useful to attackers once intercepted, especially when combined with contextual verification or device binding [12]. Traditional OTP systems such as time-based or counter-based methods remain widely used, but they still face phishing, replay, and interception risks if deployed without additional safeguards. Recent work suggests that stronger OTP systems should incorporate user context, cryptographic binding, and multifactor triggers. In this article, OTUP extends the OTP concept by linking password generation to successful biometric verification and user-specific identity context, thereby creating a more secure and personalized authentication factor for zero-trust cloud systems [13].

2.4. Zero-trust security frameworks

Zero-trust security frameworks are increasingly recognized as necessary for cloud-native environments because they emphasize explicit verification, least privilege, continuous monitoring, and breach assumption [14]. Rather than relying on trust inherited from network location, zero trust evaluates every access request according to identity, device posture, application context, and resource sensitivity. Current research shows that zero trust can reduce lateral movement, improve policy granularity, and support secure access across hybrid infrastructures. However, effective zero-trust implementation requires reliable identity systems, context-aware enforcement, and comprehensive visibility into user and system behavior. These requirements make blockchain, biometrics, and decentralized identity attractive complementary technologies [15]. The literature therefore supports zero trust as the strategic security model within which stronger access control mechanisms can be systematically integrated.

2.5. Integration challenges and existing gaps

Although prior studies address blockchain, biometrics, OTP systems, and zero trust separately, fewer works fully integrate them into a single operational framework for cloud environments. Major gaps remain in interoperability, privacy preservation, smart contract governance, and scalability under high authentication volume [16]. Biometric systems raise concerns about protected storage and legal compliance, while blockchain introduces consensus overhead and data visibility constraints.

Table-1. Comparative Analysis of Existing Security Approaches

Approach	Key Strength	Limitation	Relevance to Proposed Work
Traditional password-based authentication	Simple and low cost	Vulnerable to theft and reuse	Insufficient for zero-trust cloud security
OTP-based authentication	Time-limited credential protection	Susceptible to phishing and replay if isolated	Improved further through biometric binding
Biometric authentication	Strong user identity assurance	Privacy and spoofing concerns	Strengthened through liveness detection and protected templates
Blockchain-based access control	Tamper-resistant logging and decentralized trust	Latency and scalability overhead	Suitable for auditable zero-trust enforcement
Zero-trust access control	Continuous verification and least privilege	Complex implementation	Core security model of the proposed framework

Zero-trust models also require continuous monitoring, which can be difficult to combine with decentralized architectures unless policies and event logging are carefully coordinated [17]. These gaps justify the need for a unified design that combines decentralized identity, biometric-linked OTUP generation, hierarchical access control, and blockchain-backed accountability into a practical model for secure cloud deployment.

3. Theoretical Framework

The proposed framework is grounded in five theoretical pillars: zero-trust verification, blockchain immutability, hierarchical access control, biometric identity assurance, and time-bound password generation [18]. Together, these pillars form a multi-layered model in which no single credential or trust assumption is sufficient for access approval. Every request is evaluated through identity proof, biometric validation, contextual analysis, and policy enforcement. Blockchain serves as the distributed trust infrastructure, while access control logic is implemented through smart contracts and security-level mapping [19]. This structure creates a defensible and traceable foundation for secure cloud interactions.

3.1. Zero-trust security principles

Zero trust is based on the principles of explicit verification, least privilege, and assumption of breach. Each access request is treated as potentially hostile until proven otherwise through identity, context, and policy evaluation [20]. A user's trust score can be modelled as

$$T = w_1 I + w_2 D + w_3 B + w_4 C$$

where $I$is identity assurance, $D$is device posture, $B$is behavioral consistency, $C$is contextual reliability, and the weights sum to 1. Access is allowed only when Texceeds a required threshold [21]. This theoretical structure allows the framework to adapt authorization decisions according to user behavior, device health, and resource sensitivity rather than relying on static trust assumptions.

3.2. Blockchain technology fundamentals

Blockchain is a distributed ledger in which records are stored across multiple nodes and linked cryptographically to prevent undetected modification [22]. Each block contains transactions, a timestamp, and the hash of the previous block. This chaining creates integrity and traceability across the entire ledger. A simplified block hash relation is

$$H(B_i) = SHA256(H(B_{i-1}) \parallel T_i \parallel t_i)$$

where $T_i$is the transaction data and $t_i$is the timestamp. In this framework, blockchain is used to record access events, store policy states, and support immutable audit trails [23]. Permissioned blockchain models are especially suitable because they offer stronger control, faster validation, and enterprise-oriented governance.

3.3. Multi-level access control models

Multi-level access control organizes users and resources according to hierarchical sensitivity levels such as public, confidential, secret, and critical [24]. A user can access a resource only when the assigned clearance is sufficient for the resource classification. This can be represented as

$$Access(u, r) = 1 \text{ if } UC(u) \geq CL(r)$$

where $UC(u)$is user clearance and $CL(r)$is resource classification. The framework also supports category constraints, contextual restrictions, and role inheritance, which allow permissions to reflect organizational responsibilities and operational risk [25]. This model ensures that access decisions are precise, scalable, and aligned with least-privilege enforcement in zero-trust cloud systems.

3.4. Biometric authentication systems

Biometric systems verify identity using physical or behavioural features such as fingerprint, face, iris, or typing dynamics. During enrolment, a biometric template is extracted and stored in protected form [26]. During authentication, a new sample is compared to the enrolled template using a matching function. Acceptance occurs when

$$S(T_q, T_e) \geq \theta$$

where $S$is the similarity score and $\theta$is the decision threshold. Liveness detection is added to reduce spoofing risk by checking whether the sample comes from a live person [27]. In this framework, biometric verification is not a standalone login factor; it is also used as an input for OTUP generation, which strengthens the connection between user presence and temporary credential issuance.

3.5. One-time user password (OTUP) mechanisms

OTUP extends traditional OTP schemes by tying password generation to verified biometric evidence and user-specific context [28]. Instead of producing a code from only time and a secret key, OTUP includes biometric and device parameters. A general form is

$$OTUP = HMAC_{K_u}(DID_u \parallel H(B) \parallel t_w \parallel C_x) \bmod 10^n$$

where $K_u$is the user key, $DID_u$is the decentralized identity, $H(B)$is the biometric hash, $t_w$is the active time window, and $C_x$is contextual data. This design reduces replay and theft risk because the password is short-lived and bound to a verified user state [29]. It strengthens cloud authentication by ensuring that a valid temporary credential cannot be generated without successful biometric participation.

4. Proposed Architecture

The proposed architecture combines identity verification, biometric authentication, OTUP generation, smart contract policy enforcement, and immutable event logging within a unified cloud access control system [30]. It is designed as a layered model in which each security function supports the others rather than operating in isolation. The architecture reduces the impact of single-point compromise and improves transparency in authorization decisions. Its main purpose is to create an adaptive, decentralized, and traceable security framework suitable for cloud systems with varying data sensitivity and operational complexity [31].

4.1. System overview and components

The architecture contains five major components: the user interaction layer, decentralized identity layer, biometric processing layer, blockchain policy layer, and cloud resource layer [32]. The user interaction layer handles authentication requests and secure credential presentation. The identity layer resolves DIDs and verifies verifiable credentials.

Table-2. Core Components of the Proposed Architecture

Component	Function	Security Contribution
User interface layer	Captures credentials and biometric input	Initiates secure authentication workflow
DID and credential layer	Verifies decentralized identity	Removes reliance on centralized identity stores
Biometric engine	Performs matching and liveness detection	Confirms physical-user presence
OTUP generator	Produces temporary user-specific password	Adds time-bound authentication strength
Blockchain layer	Stores events and policy records	Ensures immutability and auditability
Smart contract engine	Enforces access rules automatically	Provides consistent policy execution

The biometric layer captures user samples, performs liveness checks, and computes matching scores. The blockchain policy layer records events, validates OTUP, and executes smart contract rules [33]. Finally, the cloud resource layer exposes data and services only after successful authorization. Together, these components create a continuous verification path from login initiation to resource access, ensuring that every access decision is cryptographically supported and fully auditable.

4.2. Multi-level access control hierarchy

The framework uses a hierarchical access model in which each resource is classified according to confidentiality or operational impact, and each user is assigned a corresponding clearance level [34]. Authorization occurs only when the user's effective clearance satisfies the resource requirement and contextual policies remain compliant. This relationship can be extended as

$$Permit = (UC \geq CL) \wedge Policy(ctx) = 1$$

where ctxincludes device, location, time, and behavior conditions [35]. Higher resource classes require stronger trust thresholds and may trigger additional authentication steps.

Table-3. Multi-Level Access Control Hierarchy

Access Level	Example Resource Type	Authentication Strength Required	Access Rule
Level 1 – Public	Public documentation	Basic verified login	General access
Level 2 – Internal	Operational dashboards	DID + OTUP	Limited organizational access
Level 3 – Confidential	Department records	DID + biometric + OTUP	Role and context based
Level 4 – Secret	Financial or research data	Strong multifactor verification	Strict least-privilege enforcement
Level 5 – Critical	Core cloud control resources	Full zero-trust verification	Continuous monitoring and revalidation

Role inheritance, category separation, and time-bound permissions can also be applied. This layered access structure ensures that authorization is both security-aware and operationally flexible, supporting enterprise governance without abandoning zero-trust discipline [36].

4.3. Blockchain integration layer

The blockchain layer serves as the trust and accountability backbone of the system. It

stores authentication events, OTUP usage records, access decisions, and policy updates in a tamper-resistant ledger shared across authorized nodes [37]. Smart contracts enforce deterministic policy logic and automatically record outcomes for later verification. A simplified ledger event hash can be expressed as

$$E_i = H(U_i \parallel R_i \parallel A_i \parallel t_i \parallel D_i)$$

where $U_i$is the user, $R_i$the resource, $A_i$the action, $t_i$the timestamp, and $D_i$the decision. By chaining these records, the system creates strong evidence for forensic analysis and compliance review [38]. Permissioned blockchain is preferred because it offers lower latency and clearer governance than public networks.

4.4. Biometric-driven OTUP generation mechanism

After a successful biometric match and liveness confirmation, the system generates an OTUP that is unique to the user, time window, and active context [39]. This mechanism ensures that temporary credentials cannot be separated from physical-user verification. The generation process uses the biometric outcome as a cryptographic input, which can be represented as

$$OTUP_t = HMAC(K_u, H(B_{valid}) \parallel DID_u \parallel t_w \parallel DeviceID)$$

The output is then truncated to a practical numeric length for user interaction. During validation, the submitted OTUP is checked against the valid time window and the blockchain usage registry to prevent replay [40]. This design creates a close security link between who the user is, when the request occurs, and from which trusted context it is made.

4.5. Smart contract design for policy enforcement

Smart contracts implement the policy logic of the framework and ensure that access decisions are executed consistently across the network [41]. Policies can include clearance rules, credential validity checks, OTUP verification, device trust requirements, and contextual restrictions. A simplified decision rule is

$$Decision = V_{id} \wedge V_{bio} \wedge V_{otup} \wedge V_{ctx} \wedge (UC \geq CL)$$

If any required condition fails, access is denied and the event is recorded automatically. This deny-by-default approach is consistent with zero-trust principles and reduces the chance of permissive misconfiguration [42]. Smart contracts also strengthen auditability by generating immutable records of every policy outcome, making administrative override and retrospective manipulation much more difficult.

5. Implementation Methodology

The implementation methodology translates the proposed architecture into an operational workflow for cloud access control. It defines how decentralized identity, biometric validation, OTUP generation, cryptographic privacy measures, and continuous monitoring interact during authentication and authorization [43]. Rather than treating these functions independently, the methodology links them into a continuous decision cycle in which access is granted, maintained, or revoked based on live verification [44]. This ensures that trust is always conditional and revisable, as required by zero-trust security principles.

5.1. Decentralized identity verification using DIDs and verifiable credentials

Each user is assigned a decentralized identifier and one or more verifiable credentials issued by trusted authorities [45]. During login, the system resolves the DID document, extracts public verification data, and validates the credential signature and status. A general credential relation is

$$VC = Sign_{Issuer}(Claims \parallel DID \parallel Expiry)$$

Verification succeeds only when the signature is valid and the credential is not revoked. This design reduces dependence on centralized identity stores and supports selective disclosure of attributes [46]. Instead of exposing all user data, the framework allows presentation of only the claims required for a specific access request. This improves privacy and supports distributed trust across cloud organizations and service domains.

5.2. Dynamic access control evaluation process

The access control process evaluates identity, biometric validity, OTUP status, resource sensitivity, and runtime context before granting access [47]. Each access request can be expressed as a tuple containing user, resource, device, action, and context. The system computes an authorization score such as

$$AS = w_1 I + w_2 B + w_3 O + w_4 D + w_5 C$$

where the variables represent identity, biometric, OTUP, device, and context assurance. Access is approved only when this score exceeds the threshold for the requested resource. The process is dynamic because the score can be recalculated during an active session if risk conditions change [48]. This allows the system to step up authentication or revoke access when anomalies appear, making authorization a continuous process rather than a one-time decision.

5.3. Biometric data capture and processing

Biometric capture begins with secure enrolment, where the system extracts templates from live user samples and stores them in protected form [49]. During authentication, a fresh sample is captured, checked for liveness, and matched against the enrolled template. The acceptance condition is

$$Accept_{bio} = (S \geq \theta) \wedge L = 1$$

where $S$is the similarity score and $L$is the liveness result. If either condition fails, the authentication chain stops. This process ensures that OTUP generation and access control rely on real-user presence rather than replayed or fabricated biometric artifacts [50]. Multimodal options can further improve robustness when systems require higher accuracy or anti-spoofing resilience.

5.4. OTUP generation and validation algorithm

OTUP is generated only after successful identity and biometric verification. The algorithm combines user identity, biometric hash, time window, and active context into a temporary code that is difficult to predict or reuse [51]. A simplified validation rule is

$$Accept_{otup} = Valid(OTUP, t_w) \wedge OTUP \notin UsedSet$$

This means the code must match the current or adjacent time window and must not already appear in the blockchain-backed consumption registry.

Table-4. Biometric-Driven OTUP Generation Workflow

Step	Process	Output
1	User submits decentralized identity	Identity reference resolved
2	Biometric sample captured	Live biometric input obtained
3	Liveness detection performed	Genuine user presence confirmed
4	Biometric template matched	Match score generated
5	OTUP generated using user, biometric, and time context	Temporary unique password created
6	OTUP validated	Access request moved to policy engine
7	OTUP marked as used on blockchain	Replay prevention ensured

Once validated, the OTUP is marked as used to prevent replay. This process strengthens authentication by making successful code theft less useful to attackers, especially when combined with device binding and strict retry policies [52].

5.5. Cryptographic techniques (Zero-Knowledge Proofs, Multi-Party Computation)

The framework uses privacy-preserving cryptography to verify claims without exposing unnecessary sensitive data. Zero-knowledge proofs allow a user to demonstrate possession of a valid credential or property without revealing

the underlying secret [53]. This can be represented as

$$Verify(\pi, y) = 1$$

where $\pi$is the proof and $y$is the public statement. Multi-party computation supports collaborative verification when several parties must compute a result without revealing their individual inputs. These methods are useful for protected biometric validation, selective credential disclosure, and distributed trust scoring [54]. Their use helps balance strong security with privacy and regulatory compliance, especially in cloud systems that handle sensitive identity or organizational data.

5.6. Continuous monitoring and trust scoring

Continuous monitoring observes user behavior, device status, and contextual changes after access is granted [55]. The system recalculates trust scores over time to detect anomalies such as unexpected location changes, irregular request patterns, or device posture degradation. A dynamic score can be modelled as

$$T_s(t) = w_1 I + w_2 B(t) + w_3 D(t) + w_4 C(t) + w_5 H(t)$$

where the variables reflect identity, behavior, device health, context, and historical reliability. If the score drops below the defined threshold, the system can request re-authentication or terminate the session [56]. This mechanism reflects the central zero-trust idea that trust must be continuously earned, not permanently assumed after login.

6. Security Analysis

The security strength of the framework comes from its layered design. Instead of relying on a single credential or a trusted network segment, it requires multiple independently verified factors and records every critical event in a tamper-resistant ledger [57]. This improves resistance to common attacks such as credential theft, replay, insider misuse, and audit manipulation. It also enhances privacy by limiting unnecessary disclosure of user identity and biometric data. The analysis therefore considers threat coverage, attack resistance, privacy controls, and accountability mechanisms together rather than as isolated security properties.

6.1. Threat model and attack scenarios

The threat model includes external attackers, malicious insiders, compromised devices, and adversaries attempting to manipulate identity, biometric channels, or logs [58]. The attack surface can be written as

$$A = \{A_{id}, A_{bio}, A_{otup}, A_{dev}, A_{net}, A_{log}\}$$

where each element represents a different target area. To compromise the system fully, an attacker would need to bypass identity verification, biometric validation, OTUP control, and policy checks simultaneously [59]. Typical scenarios include phishing-based credential theft, biometric spoofing, replay of intercepted codes, unauthorized access from unmanaged devices, and attempts to erase evidence after a breach. The framework reduces these risks by distributing trust decisions and requiring multiple conditions to hold at once before authorization.

6.2. Resistance to common attacks (replay, brute force, credential theft)

Replay attacks are reduced because OTUP values are time-bound and marked as consumed once used. Brute-force attempts are constrained by short validity windows, retry controls, and contextual checks [60]. Credential theft is also less damaging because a stolen credential alone does not satisfy biometric or contextual verification. The brute-force success probability for an n-digit code with $k$guesses can be approximated as

$$P = \frac{k}{10^n}$$

which remains low when retry policies are strict and code validity is brief. Liveness detection further reduces the effectiveness of biometric spoofing. Together, these controls make common attack paths less practical and less scalable for adversaries targeting cloud identity systems.

6.3. Privacy preservation mechanisms

Privacy is preserved through selective disclosure, protected biometric templates,

limited on-chain data exposure, and privacy-preserving verification methods. The framework does not store raw biometric data directly on the blockchain. Instead, it uses hashes, proofs, or protected references so that sensitive information remains off-chain or encrypted. Zero-knowledge techniques allow the system to validate claims without exposing full identity attributes [61]. This is important because strong authentication should not require excessive disclosure of personal or organizational data. The privacy design therefore supports regulatory alignment and reduces the secondary risks that can arise when identity systems become repositories of highly sensitive information.

6.4. Immutable audit logging and accountability

Immutable audit logging improves accountability by creating a reliable history of every authentication attempt, policy evaluation, and access decision. Each record is linked cryptographically to prior records, making retrospective tampering highly visible. A basic event-chain expression is

$$B_i = H(B_{i-1} \parallel E_i)$$

where $E_i$is the event record. This structure supports forensic investigation, compliance review, and non-repudiation because administrators or attackers cannot silently alter history after an incident. In cloud security, where logs are often a first target after compromise, this feature is especially valuable. It transforms auditing from a mutable administrative function into a verifiable property of the architecture itself.

7. Results and Discussion

The proposed framework offers stronger security assurance, better auditability, and more context-aware authorization than conventional centralized models. Its main advantage is not a single performance metric but the combination of identity resilience, tamper resistance, and adaptive access governance [62]. At the same time, these gains introduce cost in the form of added complexity, blockchain overhead, and more demanding integration requirements. The results therefore suggest that the framework is best suited for enterprise and high-value cloud deployments where strong authentication and trustworthy audit evidence are more important than minimum-latency login.

7.1. Experimental findings

Experimental evaluation should examine authentication delay, access-decision reliability, ledger update performance, and attack-blocking behavior. End-to-end authentication time can be modelled as

$$T_{auth} = T_{did} + T_{bio} + T_{otup} + T_{policy} + T_{chain}$$

Each term captures one stage of the access process. The findings suggest that blockchain interaction and advanced cryptographic processing contribute the most noticeable overhead, while biometric matching and DID verification remain relatively manageable under enterprise deployment assumptions. Even with this overhead, the framework improves traceability and policy consistency because every decision is logged and verifiable. This makes the system attractive for cloud environments where accountability is as important as speed.

7.2. Security effectiveness metrics

Security effectiveness can be measured using both biometric and access-control indicators. For biometrics, common metrics include false acceptance rate, false rejection rate, and equal error rate. At the access-control level, useful measures include unauthorized-attempt blocking rate and legitimate-user success rate. These can be expressed as

$$ABR = \frac{U_b}{U_t}, LSR = \frac{G_s}{G_t}$$

where $U_b$is blocked unauthorized attempts and $G_s$is successful genuine access. A secure framework should maximize attack blocking while maintaining acceptable usability for legitimate users [63]. In this system, layered verification improves security because compromise requires bypassing multiple coordinated controls rather than exploiting a single weak factor.

7.3. Performance benchmarks

Performance benchmarks should focus on latency, throughput, and computational overhead. Throughput can be written as

$$Throughput = \frac{N}{T}$$

where $N$is the number of processed requests over time T. Permissioned blockchain settings generally offer more practical performance for enterprise access control than public chains because they use fewer validators and controlled governance. However, privacy-preserving cryptographic operations and smart contract evaluation still add measurable delay. These trade-offs are acceptable in security-sensitive domains but may be excessive for low-risk consumer systems [64]. Thus, the benchmark discussion supports targeted deployment in environments where trustworthiness and audit integrity have high operational value.

7.4. Limitations and trade-offs

The framework is powerful but not cost-free. Blockchain consensus, biometric infrastructure, cryptographic proofs, and continuous monitoring all increase implementation complexity. There is also a usability-security trade-off, especially in biometric threshold tuning, because reducing false acceptance can increase false rejection. This can be described conceptually as

$$\min_{\theta} \lambda_1 FAR(\theta) + \lambda_2 FRR(\theta)$$

where $\theta$is the matching threshold. The model is therefore best justified in regulated or high-value cloud systems rather than lightweight applications. Its benefits include stronger trust, accountability, and attack resistance, but these must be balanced against cost, latency, and deployment maturity.

8. Conclusion

This research presents a comprehensive blockchain-integrated multi-level access control framework with biometric-driven one-time user passwords (OTUP) that successfully implements zero-trust security principles for cloud environments. The proposed architecture addresses critical limitations of traditional perimeter-based security models by eliminating implicit trust assumptions and enforcing continuous verification through decentralized, cryptographically verifiable mechanisms. By synergistically combining decentralized identifiers (DIDs), verifiable credentials, biometric authentication, dynamic OTUP generation, smart contract-based policy enforcement, and immutable blockchain audit trails, the framework establishes defense-in-depth protection that significantly exceeds the security guarantees of single-factor or centralized authentication systems.

The theoretical framework establishes a rigorous foundation integrating zero-trust principles, blockchain technology fundamentals, multi-level access control models, biometric authentication systems, and OTUP mechanisms. The proposed architecture operationalizes these concepts through five interconnected layers that collectively provide comprehensive security coverage across identity verification, policy enforcement, audit logging, and continuous monitoring. Security analysis demonstrates robust resistance to replay attacks, brute-force attempts, credential theft, and biometric spoofing through temporal constraints, blockchain-based credential reuse prevention, liveness detection, and multi-factor verification requirements. Privacy preservation mechanisms protect sensitive biometric and identity data through template protection, selective disclosure, zero-knowledge proofs, and distributed computation that minimizes unnecessary data exposure.

Performance evaluation reveals that the architecture achieves superior security effectiveness metrics while maintaining acceptable operational latency for enterprise cloud deployments, though the framework introduces moderate computational overhead compared to traditional centralized systems. The identified trade-offs between security assurance, system complexity, and operational performance are justified in high-value environments where unauthorized access costs significantly exceed authentication delay impacts. Future research directions include integration of artificial intelligence for adaptive security policies, implementation of advanced privacy-enhancing technologies such as zk-SNARKs and homomorphic encryption, development of

interoperability standards for legacy system integration, and investigation of quantum-resistant cryptographic primitives to ensure long-term security. This research demonstrates that blockchain-integrated, biometric-driven, zero-trust architectures represent a viable and necessary evolution in cloud security, providing the strong authentication, continuous verification, transparent accountability, and privacy preservation required to protect modern distributed computing environments against sophisticated adversaries while maintaining operational feasibility for enterprise deployment.

References:

[1] Shrivastava, A., Praveen, R. V. S., Aida, R., Vemuri, K., Vemuri, S. S., & Husain, S. O. (2025, August). A Comparative Analysis of Graph Neural Networks for Social Network Data Mining. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[2] Chauhan, P. R., Vanitha, P., Agnihotri, K., Praveen, R. V. S., Kumar, S., & Praveena, S. (2025, May). Analysing Social Entrepreneurship and Financial Inclusion for Women Empowerment Using an F-GNN and AXGB Hybrid Approach. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-6). IEEE.

[3] 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.

[4] Eswari, S., Nadgaundi, S. K., Praveen, R. V. S., & Trakroo, K. (2025, November). Hybrid Genetic Algorithm–Fuzzy Logic Framework for Optimized Seed Quality Assessment and Yield Enhancement. In 2025 5th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 1074-1079). IEEE.

[5] Radhakrishnan, P., Manoranjithem, V., Garapati, R. S., Singh, S., & Praveen, R. V. S. (2025, November). Random Forest–XGBoost Hybrid Model for Early Detection of Breast Cancer in Medical Imaging Datasets. In 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN) (pp. 1-6). IEEE.

[6] Sundaramoorthy, P., Praveen, R. V. S., Puli, B., Tiwari, A., Kanimozhi, S., & Keerthana, N. V. (2025, October). Decentralized Anomaly Detection in IoT Networks Using Federated Learning Models. In 2025 International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU) (pp. 1-6). IEEE.

[7] Shrivastava, A., Praveen, R. V. S., Al-Asady, H. A. J., Yadav, K., Kalra, R., & Khan, A. K. (2025, September). Cloud-Native AI: Optimizing Machine Learning Workloads for Scalability and Performance. In 2025 IEEE International Conference on Advances in Computing Research On Science Engineering and Technology (ACROSET) (pp. 1-6). IEEE.

[8] Kumar, S., Praveen, R. V. S., Aida, R., Varshney, N., Alsalami, Z., & Boob, N. S. (2025, September). Enhancing AI Decision-Making with Explainable Large Language Models (LLMs) in Critical Applications. In 2025 IEEE International Conference on Advances in Computing Research On Science Engineering and Technology (ACROSET) (pp. 1-6). IEEE.

[9] Vasanti, G., Rani, M., Gupta, P., Praveen, R. V. S., Kumar, A., & Ramasamy, D. (2025, September). Fuzzy–Logistic Regression Approach for Analysing Consumer Behaviour and Shopping Preferences in E-Commerce. In 2025 2nd Asia Pacific Conference on Innovation in Technology (APCIT) (pp. 1-6). IEEE.

[10] Kumar, R. S., Gajbhare, B. P., Praveen, R. V. S., Bugge, B. P., & Dhivya, R. (2025, September). Fuzzy Logic and Neural Networks for Intelligent Battery Management Systems in Electric Vehicles. In 2025 IEEE 4th International Conference for Advancement in Technology (ICONAT) (pp. 1-7). IEEE.

[11] 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.

[12] 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.

[13] Chittakula, R., Kalpanadevi, D., Praveen, R. V. S., Pragadeeswaran, S., & Amsa, M. (2025, September). An Adaptive AI Model for Intelligent Fraud Detection and Customer Engagement in Digital Banking. In 2025 IEEE 4th International Conference for Advancement in Technology (ICONAT) (pp. 1-6). IEEE.

[14] Padmaja, A. R. L., Mani, M. S. R. M., Thangam, A., Praveen, R. V. S., Tikhe, K., & Sharma, M. S. (2025, September). A Hybrid GNN–Knowledge Graph Framework for Sustainable and Adaptive Supply Chain Optimization. In 2025 IEEE 4th International Conference for Advancement in Technology (ICONAT) (pp. 1-6). IEEE.

[15] Sreelatha, B., Rajamohanan, R., Kalaiarasi, G., Praveen, R., Bugge, B. P., & John, T. J. (2025, September). A Novel Decision Tree and LSTM Powered Intelligent Agent System for Early Detection of Vegetable Plant Diseases. In 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1617-1622). IEEE.

[16] Suganya, V., Vijayakumar, L., Annur, E. A., Praveen, R. V. S., Bharathi, A., & Amsa, M. (2025, September). A Hybrid LSTM-Fuzzy Inference Model for Uncertainty-Aware Stock Market Forecasting. In 2025 International Conference on Electronics and Computing, Communication Networking Automation Technologies (ICEC2NT) (pp. 1-6). IEEE.

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

[18] Rachapally, O., Kopparthi, G. S., Praveen, R. V. S., Tiwary, R., Pandey, V., & Shete, N. (2025, September). A GRU-CNN Based Framework for Real Estate Price Prediction and Transaction Analysis. In 2025 International Conference on Computing and Communications (COMPUTINGCON) (pp. 1-6). IEEE.

[19] Shrivastava, A., Hundekari, S., Praveen, R., Husain, S. O., Kumar, R., & Nijhawan, G. (2025, September). Adversarial ML Defense Framework for Real-Time Threat Detection in Industrial IoT (IIoT). In 2025 International Conference on Computing and Communications (COMPUTINGCON) (pp. 1-7). IEEE.

[20] Lora, S., Ramya, S., Priya, S., Praveen, R. V. S., Tharini, C., & Pathak, P. (2025, August). Hybrid CNN-RNN Model for Identifying and Classifying Literary Themes and Structures in English Novels. In 2025 IEEE 2nd International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS) (pp. 1-6). IEEE.

[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] Gurrala, R. R., Ravish, M., Shukla, R., Praveen, R. V. S., & Pandey, V. (2025, August). A Heterogeneous Graph Neural Network Combined with a Rule-Based System for Financial Fraud Detection and Prevention. In 2025 5th Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-6). IEEE.

[23] Nutalapati, P., Dhavale, S. M., Shrivastava, A., Praveen, R. V. S., Vemuri, H. K., & RiadHwsein, R. (2025, August). IoT and Machine Learning-Enhanced Energy Management in Enabled Smart Grids for Predictive Load Balancing. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[24] Thayumanavan, K., Kumar, A., Praveen, R. V. S., Bhendale, M. A., & Agnihotri, K. (2025, August). Hybrid Transformer Based Framework for Enhanced Financial Market Analysis and Online Trading Forecasting. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[25] 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.

[26] Patil, B. D., Praveen, R. V. S., Rambhatla, A. K., Trakroo, K., Singh, K., & Vishanth, R. (2025, August). Graph Neural Network Model for Intelligent Urban Traffic Flow Prediction and Smart City Mobility Management. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[27] Chandra, N. S., Rao, K. S., Praveen, R. V. S., Upadhye, N. A., & Kaliappan, S. (2025, August). Hybrid Auto-Encoder Framework for Water Pollution Prediction in Smart Cities. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[28] Victor, S., Kumar, K. R., Praveen, R. V. S., Aida, R., Kaur, H., & Bhadauria, G. S. (2025, August). GAN and RNN Based Hybrid Model for Consumer Behavior Analysis in E-Commerce. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[29] Srinivas, A. C. M. V., Hemavathi, U., Devi, G. U., Praveen, R. V. S., Vasumathi, G. G., & Saranya, R. (2025, August). Secure and Intelligent Framework for Kidney Stone Detection Using a CNN-XGBoost Hybrid Model with Blockchain Integration. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[30] Kumar, S., Shrivastava, A., Praveen, R. V. S., Subashini, A. M., Vemuri, H. K., & Alsalami, Z. (2025, August). Future of Human-AI Interaction: Bridging the Gap with LLMs and AR Integration. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[31] Choudhari, P., Tatiya, M., Praveen, R. V. S., Kaur, H., Vemuri, H. K., & MuhsnHasan, M. (2025, August). Enhancing Energy Efficiency in IoT Networks Using Deep Learning-Based Predictive Maintenance. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[32] Vijayakumar, L., Kannadasan, B., Hinge, P., Reddy, L. K. K., Praveen, R. V. S., & Kalidindi, N. (2025, September). Analysis and Prediction of Employee Turnover with Effective Feature Selection based on Lee–Carter and ANN Model. In 2025 2nd Asia Pacific Conference on Innovation in Technology (APCIT) (pp. 1-6). IEEE.

[33] 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.

[34] Dhanabal, S., Goswami, C., Praveen, R. V. S., & Vetriselvi, T. (2025). Shuffle-F-ZFNet: ShuffleNet Fuzzy Zeiler and Fergus network for data aggregation in WSN data communication. Wireless Networks, 31(6), 4111-4134.

[35] 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.

[36] Hundekari, S., Shrivastava, A., Mhsnhasan, M., Praveen, R. V. S., Labde, V. V., & Yadav, K. (2025). Link Prediction in Graph-Based Data: Techniques for Analyzing and Predicting Network Connections. In Graph Mining: Practical Uses and Instruments for Exploring Complex Networks (pp. 67-76). Cham: Springer Nature Switzerland.

[37] 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.

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

[39] Maharajan, K., Parasar, A., Khurana, P., Praveen, R. V. S., Sathiyanathan, S., & Priti, C. (2025, July). Enhancing Business Education Through AI-Powered Teaching Innovations in Quantitative Subjects Using Neural Architecture Search with Self-Attention. In 2025 International Conference on Communication and Smart Devices (ICCoSD) (Vol. 1, pp. 1-6). IEEE.

[40] Mishra, P., Kalburgikar, A., Praveen, R. V. S., Soujanya, K., Balamurugan, S., & Kalra, G. (2025, July). A Graph Neural Network-Based Hybrid AI Model for Detecting Fake Reviews and Fraudulent Sellers to Enhance Trust in E-Commerce. In 2025 3rd World Conference on Communication & Computing (WCONF) (pp. 1-7). IEEE.

[41] 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.

[42] 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.

[43] 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.

[44] Magdum, V. B., Adivarekar, P. P., Praveen, R. V. S., Kovalenko, A. B., & Kumar, B. S. (2025, May). Advanced Global Safety with Precision Disaster Prediction and Early Warning Systems Using HPReADS Models. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-6). IEEE.

[45] Akhmetshin, E., Parasar, A., Praveen, R. V. S., & Gupta, S. (2025, May). Accurate Forecasting of Teacher Performance and Behaviour in Higher Education Using RNN-XGBoost Multilayer Model. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-7). IEEE.

[46] NR, A. R., Rajasri, T., Praveen, R., Kalla, D., Bendale, S. P., & Venu, N. (2025, April). CAC

Training-A Unified Cybersecurity Training Program for Military Staff. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 569-573). IEEE.

[47] Kalaiselvi, M., Dasa, S. K., Malik, N., & Praveen, R. V. S. (2025, July). Intrusion Detection and Security Challenges in 6G Networks Using Stochastic Graph Neural Networks. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-6). IEEE.

[48] 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.

[49] Kumar, B. R., Ali, S. R. M., Praveen, R. V. S., Thangam, A., Malik, N., & Kalra, G. (2025, July). A Novel Optimized Hybrid LSTM-Based Dynamic Demand Forecasting Model for Resilient Supply Chains. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-6). IEEE.

[50] 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.

[51] Rajput, N., Praveen, R. V. S., Shrivastava, A., Kulshreshtha, K., Shakir, A. M., Hadi, A. A. A. K., & Majeed, D. A. (2025, July). Optimized K-Means Algorithm for Large-Scale Customer Segmentation in E-Commerce Platforms. In 2025 3rd International Conference on Cyber Resilience (ICCR) (pp. 1-7). IEEE.

[52] Manikandan, K., Moparthi, R., Praveen, R. V. S., Balasubramanian, K., KK, L., & Sivanantham, S. (2025, July). Lung Cancer Detection From CT Images Using Image Processing and Hybrid Neural Network Models. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-6). IEEE.

[53] Hundekari, S., Praveen, R. V. S., Shrivastava, A., Hwsein, R. R., Bansal, S., Hussain, H. A., ... & Jumaili, M. L. F. (2025, July). Privacy-Preserving Federated Learning Algorithm for Distributed Health Data Analysis. In 2025 3rd International Conference on Cyber Resilience (ICCR) (pp. 1-6). IEEE.

[54] Supraja, N. S., Praveen, R. V. S., Vemuri, H. K., Jaiswal, V. K., & Sista, S. (2025). Leveraging AI and ML in Central Bank Strategies for Financial Stability. Advances in Consumer Research, 2(4).

[55] Gudimella, A., Ram Gopal Peri, S. S. S., Praveen, R. V. S., Labde, V. V., Deshmukh, R., & Shrivastava, A. (2025). Green Finance and ESG Investing: Evaluating Impact on Corporate Valuation. Advances in Consumer Research, 2(3).

[56] Sujitha, B. B., Rao, C. V., Thiyagarajan, C., Shakhov, D., & Praveen, R. V. S. (2025, June). Intelligent Energy Consumption Estimation in IoT-Enabled Smart Homes Using a Hybrid CNN-GRU Model. In 2025 Second International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS) (pp. 140-145). IEEE.

[57] Kathiravan, M. N., Periyasamy, V. M., Kumar, P., Praveen, R., Chetana, S., & Surender, S. (2025, June). IoT-Integrated Graph Convolutional Networks and LSTM Models for Smart Plant Growth Monitoring in Controlled Environment Agriculture. In 2025 5th International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[58] Jose, N., Daruvuri, R., Puli, B., Sundaramoorthy, P., & Praveen, R. V. S. (2025, June). An integrated context-aware adaptive meta-learning system for accurate risk estimation of postpartum depression. In 2025 11th International Conference on Communication and Signal Processing (ICCSP) (pp. 323-327). IEEE.

[59] 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.

[60] 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.

[61] Praveen, R. V. S., Vemuri, H. K., Peri, S. S. S. R. G., Sista, S., Saxena, V., & Saxena, P. (2025). Enhancing Financial Literacy and Personal Investment Decisions Through AI and Machine Learning. Journal of Marketing & Social Research, 2, 268-280.

[62] 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.

[63] 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.

[64] 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.

Cite this article as: Dr. J. Mohammed Ubada., (2026). Blockchain-Integrated Multi-Level Access Control with Biometric-Driven One-Time User Password (OTUP) for Zero-Trust Cloud Security. International Journal of Emerging Knowledge Studies. 5(6), pp. 920–935.
https://doi.org/10.70333/ijeks-05-07-005