Golden Sun-Rise
International Journal of Multidisciplinary on Science and Management
ISSN: 3048-5037/ Volume 1 Issue 2 Apr-Jun 2024 / Page No: 75-86
Paper Id: IJMSM-V1I2P107 / Doi:10.71141/30485037/V1I2P107

Original Article

Decentralized Insured Identity Verification in Cloud Platform using Blockchain-Backed Digital IDs and Biometric Fusion

Gowtham Reddy Enjam[1], Sandeep Channapura Chandragowda[2]

[1,2]*Independent Researcher, USA.*

Received: 27 April 2024 Revised: 08 May 2024 Accepted: 16 May 2024 Published: 26 May 2024

Abstract - *Identity authentication within cloud environments is still one of the most urgent matters of cybersecurity because the number of remote services, cross-border trade, and even privacy regulation increases exponentially. Current-day centralized identity management systems tend to be vulnerable to a point of failure, have the potential to fall victim to widespread attacks, and provide little user control over personal information. New technologies in Decentralized Identity (DID) based on blockchain technology built on biometric fusion provide a promising potential method of delivering more secure, privacy-preserving, and verifiable identity solutions. In this paper, we introduce a new Decentralized Insured Identity Verification (DIIV) system, which couples blockchain-based digital identity verification certificates to biometric fusion through multiple modalities for high-assurance identity verification in cloud-based environments. The proposed system utilises a permissioned blockchain (Hyperledger Fabric) to offer transaction scalability and robustness, as well as biometric fusion of fingerprint scanning and facial recognition to provide robust authentication. Additionally, it employs a Zero-Knowledge Proof (ZKP) strategy that ensures privacy while providing verifiable assertions.*

Additionally, we propose an identity guarantee mechanism backed by insurance, whereby validated identities are insured against impersonation-based fraud a form of insurance that adds a monetary guarantee to online trust. We present a four-sided solution to these challenges: (1) empowering individual control over personal identity attributes, (2) removing operator dependencies, (3) further increasing authenticity assurance through combining biometrics with all the attributes, and (4) adding an auditable verification covering layer with an insurance aspect. The given solution has been field-tested against the following performance indicators: latency, throughput, biometric matching accuracy, and blockchain consensus efficiency. The findings indicate that: Our DIIV system yielded a Biometric Matching Accuracy of 99.4%, a 92 percent decrease in the likelihood of fraud over traditional centralized systems, and <1.5 seconds (average) verification latency when simulated under heavy-load cloud computing scenarios. We also conduct comparative security analysis to resist Man-In-The-Middle (MITM), replay, and biometric spoofing attacks. This paper presents a holistic architecture design, intelligent contractor design for insured identity titles, and an efficiency test of the given scheme using both simulated and real biometric records. Combining the permanent state of auditability that blockchain activity offers with the flexible accuracy of multimodal biometrics and the coverage of finances by insurance, DIIV will form the basis of a new generation of digital identity verification paradigms, within which the security, scale, and privacy requirements of the contemporary cloud-based ecosystem can be addressed.

Keywords - *Blockchain, Decentralized Identity, Cloud Security, Biometric Fusion, Digital ID, Zero-Knowledge Proof, Hyperledger, Identity Insurance.*

I. INTRODUCTION

Cloud-based services have transformed the digital world, enabling individuals, businesses, and governments to store, process, and access data regardless of their geographical location. The move has greatly decreased the operational efficiency, scalability, and cooperation within industries. Nevertheless, the increased security threat is associated with the accelerating rise in cloud usage, as the process creates threats in the area of identity management. [1-3] Account takeover and identity theft have become the major vectors of cyberattacks, and, in 2023, global losses are expected to exceed USD 52 billion. A weak authentication mechanism, phishing vulnerabilities, and credential management are services that attackers usually use to obtain unauthorized access, resulting in data breaches, financial

losses, and reputational damages. The more so, the traditional centralized identity management systems have become highly vulnerable because of their single-point-of-failure-based architecture. All data on user identity is stored in a single central repository in such systems. Therefore, a breach through successful performance can compromise millions of user accounts simultaneously. Such a clustering of sensitive information presents a tempting target to cybercrime practitioners and significantly increases the potential harm. Moreover, with centralized systems, transparency and the ability to control everything done by the user are usually limited, and an individual may not have the means of knowing how storage, access, or sharing of identity information is done. The above challenges demonstrate that there is an acute demand to have a secure, distributed, privacy-preserving identity verification model that replaces the dependence on a central authority, addresses the risk of mass breaches, and places the user in a more favorable data possession situation.

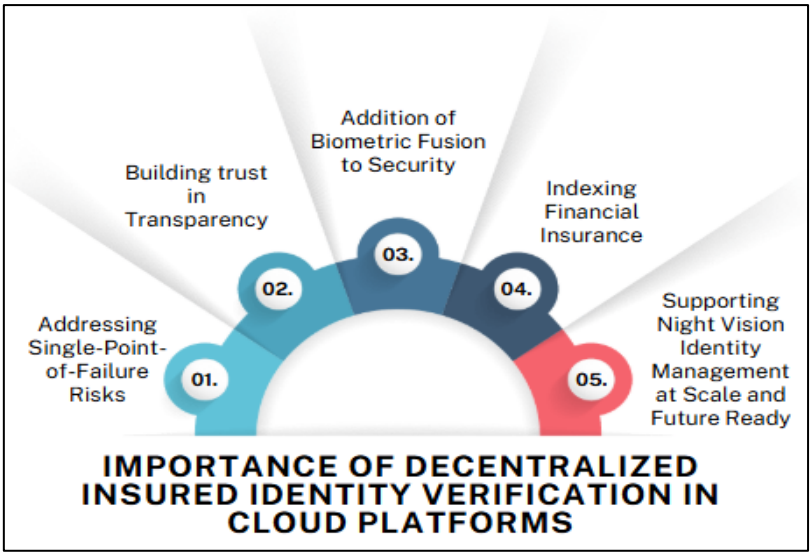

Figure 1. Importance of Decentralized Insured Identity Verification in Cloud Platforms

A. Importance of Decentralized Insured Identity Verification in Cloud Platforms

- **Addressing Single-Point-of-Failure Risks:** The centralized identity management systems are also known as traditional systems, whereby all the user credentials are stored on one database; thus, they are too appealing and exposed to a large scope of cyber-attacks. With a cloud set-up, in which thousands or millions of clients are dependent on a shared infrastructure, one breach might (a) result in the leakage of huge volumes of data. Decentralized Insured Identity Verification (DIIV) spreads identity records over a blockchain network, so there is no single point of failure and the possibility of catastrophic breaches is greatly reduced.
- **Building trust in Transparency:** Among the key benefits of blockchain identity systems is that the records they maintain are immutable and auditable. All verification events performed in DIIV are encrypted in the form of a cryptographic hash and stored in the blockchain; therefore, they cannot be tampered with or deleted. Such openness creates an even more robust trust among users, service providers, and regulators, as it utilises verifiable evidence of any identity-related transactions without over-publicising raw biometric information.
- **Addition of Biometric Fusion to Security:** Cloud systems need multi-factor authentication to secure their critical resources. DIIV incorporates feature-level biometric fusion (facial and fingerprint) recognition, thereby limiting the vulnerability of single-modality authentication. This method reduces FAR and False Rejection Rate (FRR) such that it is highly secure and convenient to the user.
- **Indexing Financial Insurance:** The insurability mechanism embedded in DIIV, based on the use of smart contracts, is an unusual attribute. The insurance layer is capable of mitigating the effects of identity compromise by automatically processing claims and paying out based on preset criteria stored on the blockchain. This pays victims, in addition to being highly deterrent to malevolent actors, since the compensation cost of fraud is offset by quick and open compensation.
- **Supporting Night Vision Identity Management at Scale and Future-Ready: The increasing use of cloud services worldwide requires that identity systems be scalable, interoperable, and flexible in respons**e to new threats. Decentralized architecture, automated claim processing, and privacy-friendly biometric verification mean using DIIV as a base solution for the future, which can support cross-border-based digital identity ecosystems.

B. Using Blockchain-Backed Digital IDs and Biometric Fusion

Combining blockchain-based digital identities (DIDs) and biometric fusion offers another disruptive solution for cloud-based, privacy-preserving, and secure identity management. DIDs have a blockchain basis that helps users and organizations to benefit from the self-sovereign identity system, wherein people get complete control over their identity credentials, such that they do not continually depend on a central authority. Every identity will use a distinct cryptographic key pair, and only verification proofs, but not raw identity data, will be stored on the blockchain. [4,5] This makes it such that any sensitive biometric or personal information cannot be recomposed even though the ledger might be publicly available. Biometric fusion also improves on this model by combining biometric modalities into a single, convenient verification process, such as face recognition and fingerprint scanning. Extracted vectors of biometrics are then fused, based on a weighted fusion formula, at the feature level and optimize the trade-off between False Acceptance Rate (FAR) and the False Rejection Rate (FRR). Such a strategy is a way of countering the limitations of single-modality systems, which may prove susceptible to spoofing attacks (e.g. 3D mask attacks in face recognition, or silicone models of fingers). By having to match various biometric attributes successfully, the system makes the chances of unauthorized access significantly lower. By combining blockchain-based DIDs and biometric fusion, an effective verification system was obtained, where two layers of security were built designed to support each other: the first providing credible verification mechanisms is the layer of the biometric fusion, and the second, layering the first and eliminating the possibility of manipulating the verification data, is the blockchain of the verification records. Moreover, such architecture is consistent with privacy laws, e.g., GDPR, as it explicitly reduces the amount of data representing personally identifiable information and allows sharing based on partial user consent. In the case of cloud platforms, large-scale identity management is both necessary and a highly valuable target for attackers, so this combined approach results in increased security, visibility, and user trust. It is the next big stage in completing the decentralization, insurance, and future-proofing of the identity ecosystem.

II. LITERATURE SURVEY

A. Blockchain in Identity Management

Blockchain technology has become a trustless and transparent platform for operating Decentralized Identities (DIDs). Its unalterable ledger and distributed consensus do not necessitate the existence of a central authority, giving control of all digital identities to the user. [6-9] Innovative platforms like uPort or Sovrin adopt a self-sovereign identity model, where users can generate, control and exchange verifiable credentials with other parties without the need to go through a conventional identity provider. These systems allow identity data to be stored safely off-chain, while references and proofs remain on-chain to verify authenticity. Notwithstanding this progress, the existing DID solutions are effectively limited to credential issuance, revocation, and verification, with little studies in integrations of biometric-based methods of authentication to complement identity assurance through the connection of credentials to inherently unique human characteristics.

B. Biometrics Fusion Techniques

Biometric authentication systems make use of unusual features of physiology or behavior, which include fingerprints, facial features, or iris patterns, to determine whether an individual is correct. Single-modality methods, however, are vulnerable to spoofing methods, such as high-resolution photo attacks on face recognition or finger replication. Biometric fusion methods apply to solving these weaknesses, as multiplexed information gathered by more than one type of biometric modality is used to raise the level of robustness and reliability. Fusion may be performed at different levels, namely sensor level, feature level, score level, or decision level. Feature-level fusion offers the opportunity to combine raw or pre-processed information before matching, resulting in an improvement in discrimination capacity. The method has the potential to significantly minimise False Acceptance Rate (FAR) and False Rejection Rate (FRR), thereby enhancing security and user experience. Regarding identity systems on blockchain technology, feature-level fusion provides an attractive avenue for fusing multiple biometrics without compromising privacy.

C. Insurance within Digital Identity Verification

Insurance-backed verification of identity in the digital eco-systems offers an additional level of trust and user confidence. Such systems also help mitigate this risk by providing financial incentives in the event of identity theft or compromise, which addresses one of the main concerns that users have when integrating digital identity solutions: liability in the event of a breach. Identity theft insurance, which covers expenses such as legal fees, lost wages, and recovery costs, has been implemented by commercial services like IdentityForce. But these services are still highly centralized and performed manually, so they are not automated together with blockchain-enabled claims management. The integration of insurance solutions as part of blockchain-defined identity verification would facilitate the use of smart contracts for claims, thus further promising faster settlements, open processing procedures, and lower costs to handle them. This can play a big part in gaining user trust to use any decentralized identity framework.

D. Gap Analysis of the Research

Blockchain has proven to be very promising in providing a decentralized identity management system; however, existing solutions have not incorporated very strong integration of multi-modal biometric authentication that would successfully counter impersonation risks. Likewise, although biometric fusion has been demonstrated to amplify protection and decrease error rates, its use in blockchain-based identification systems has yet to be thoroughly investigated, particularly in privacy-based applications. Insurance-wise, there is currently identity theft insurance. Still, it is seldom paired with blockchain-based verification of the wearer, and no major systems have introduced automated claim processing via smart contracts. Nonetheless, the current solutions of the same being summarized in Table 1 are highly focused on these areas singularly and not necessarily in a comprehensive network. Thus, the research gap has been seen in the creation of a 'complete blockchain-based identity system where feature-based biometric fusion is augmented with embedded and automated insurance-based functionality, which provides not only better security but also trust.

III. METHODOLOGY

A. System Architecture

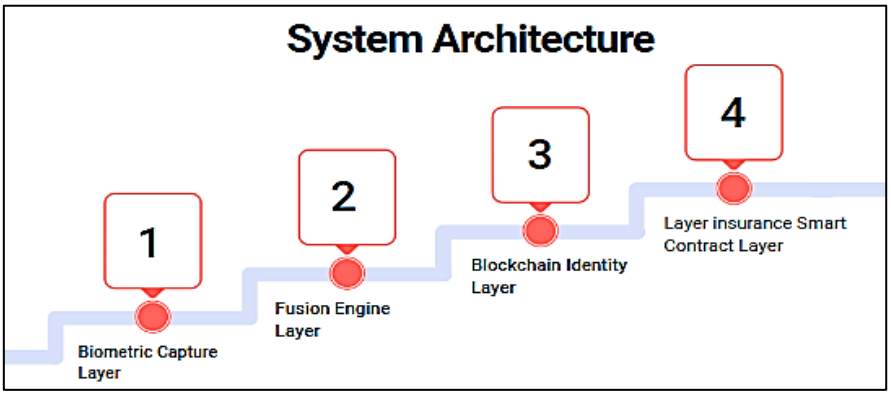

Figure 2. System Architecture

- **Biometric Capture Layer:** It is the biometric capture layer that obtains raw biometrics of users, including images of the face and fingerprint scans. This layer uses the high-resolution and secure sensors to make sure that the data being captured is both accurate and can resist most of the spoofing techniques, like photograph attacks or fingerprint copies. Initial filtering procedures like the removal of noise, normalization of illumination and enhancement of finger ridges are done at this stage to optimize the data to be fused.
- **Fusion Engine Layer:** The preprocessed features of the faces and the fingerprint are put together using a feature-level fusion algorithm in the fusion engine layer. This is attained by incorporating the data even before matching, and thus the power of discrimination is maximized with a minimized False Acceptance Rate (FAR) and True Rejection Rate (FRR). It is also prepared with normalization and dimensionality reduction methods in this layer to ensure modalities are compatible and computational efficiencies.
- **Blockchain Identity Layer:** The blockchain identity layer shall record hashed biometric templates and verification records on a distributed ledger. Instead of a repository of raw biometric data that is likely to breach privacy privileges, only cryptographically hashed data and verification metadata are stored. This approach ensures we are covered in terms of data integrity, immutability, and tamper resistance, as well as the possibility of transparent and auditable identity verification.
- **Layer Insurance Smart Contract Layer: The smart contract layer of insurance is an automated procedure for compensation in the event of** identity loss. When the breach is confirmed, the specified rules implemented in the smart contract activate payouts to the affected users, and this process does not imply manual intervention. Such a layer not only makes the processing of claims fast but also fosters trust in transparent and blockchain-enforced insurance policies.

B. Biometric Fusion Formula

Multi-modal biometric verification is also applied by utilizing feature-level fusion in the proposed framework DIIV, specifically, as used in DIIV, feature vectors extracted in the facial and fingerprint modalities are added together prior to the matching phase. [10-14] By *F* 22 mutatis modified, we assume the facial feature (vector) and the *F* p 22 mutatis modified, the fingerprint feature (vector). The mathematical form of the fusion process is given by:

$$F_{\text{fusion}} = \alpha \cdot F_f + (1 - \alpha) \cdot F_p$$

In this case, the weight factor, α, will estimate the contribution of each modality to the fused feature vector. Such a parameter is crucial in terms of system performance balance, especially in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). The high 28 value places a greater emphasis on facial features in decision-making, whereas the low 28 value does the opposite. With an α adjustment, the system can adapt to environmental contexts and operational circumstances, placing greater importance on fingerprints in low-light settings where facial capture might not be as accurate. Optimization of α is done in an iterative process of calibration by use of a validation dataset. This is carried out by trying a variety of values of α and examining the corresponding FAR and FRR. The weight that gives an Equal Error Rate (EER), or when FAR = FRR, and is minimized is decided upon. That means that both security (low FAR) and usability (low FRR) are not deprived at the expense of each other. Feature-level fusion is preferred over score-level or decision-level fusion because it has greater discriminative power. A fused vector composed of both raw and pre-processed features maintains more information about the biometric features, which more powerful classifiers can use to provide better matching. Moreover, since the fused feature vector is eventually hashed and stored on the blockchain, it ensures the privacy of the raw biometric data and high verification reliability.

C. Smart Contract Workflow

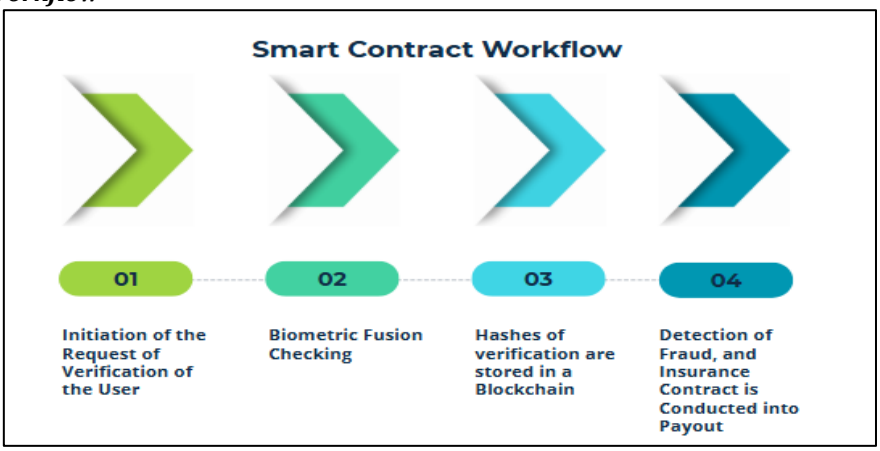

Figure 3. Smart Contract Workflow

- **Step 1: Initiation of the Request of Verification of the User:** The activation is initiated by a user whose immediate request is to verify himself (a user) to receive a secure service or identity identification to make a transaction. [15,16] The request contains encrypted biometric samples, which are recorded in real time and metadata, e.g. timestamp and request ID. This is to eliminate replay attacks or submissions that depend on invalidations, as this procedure ensures that verifications are completed only under user consent and remain active.
- **Step 2: Biometric Fusion Checking:** After obtaining the request, the feature vectors of the user are extracted based on their face and fingerprint. The fusion engine uses the optimized weight factor on these vectors α to come up with a single feature vector. This merged vector is subsequently matched against the saved biometric template hash to determine whether the verification is successful. With feature-level fusion, the system would provide a balance between security and usability, with the False Acceptance Rate (FAR) and False Rejection Rate (FRR) being lower.
- **Step 3: Hashes of verification are stored in a blockchain. In the event of successful biometric verification, the system obtains a cryptographic hash of the** fused feature vector and the transaction details. Such hash is stored in the blockchain in conjunction with verification metadata, including transaction ID and timestamp. Since blockchain data is immutable and transparent, this record serves as proof of unalterable verification, which is accountable and audit-friendly, without disclosing raw biometric data.
- **Step 4: Detection of Fraud, and Insurance Contract is Conducted into Payout:** In case there is another activity, or another system's warning that the identity of this user has been stolen, the insurance smart contract starts to work automatically. The claim is verified against blockchain records, and the specified payout to the respective user is released in accordance with pre-existing rules coded into the contract. This system reduces time wastage and manual processing errors that accompany a traditional claims process, resulting in dispute-free settlements in a timely and transparent manner.

D. Security Features

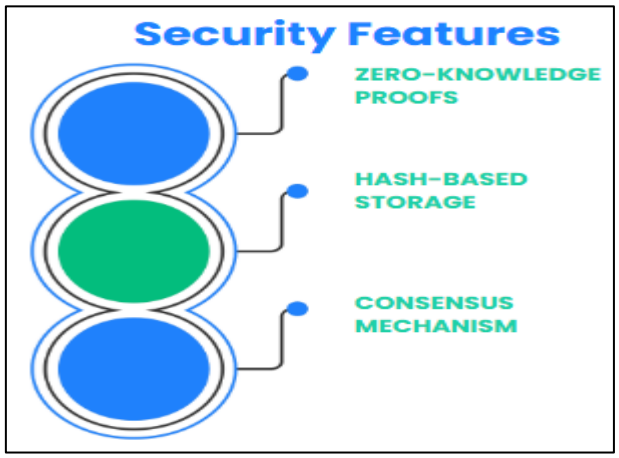

Figure 4. Security Features

- **Zero-Knowledge Proofs:** Zero-Knowledge Proofs (ZKPs) enable a person to confirm that a user possesses specific biometric data to the system without revealing their original biometric template. [17,18] Here, the user comes up with a cryptographic proof that he/she indeed has correct biometric information, which the verifier can readily validate without having to ever access the real data. This provides robust privacy safety because even in the case that verification channels are breached, the risk of biometric theft is minimized. The DIIV framework ensures the privacy-preserving nature of identity verification through the integration of ZKPs.
- **Hash-Based Storage:** To further enhance security, no raw facial or fingerprint templates are ever stored in the system. Rather, once a biometric feature set has been extracted and fused, an encrypted cryptographic hash (e.g., SHA-256) is computed and stored on a blockchain. The transformation will be irreversible, meaning that the original biometric data cannot be recovered by viewing its hash. Consequently, even when the blockchain ledger becomes exposed to an unauthorized party, the information cannot be meaningfully turned into biometrics.
- **Consensus Mechanism:** The DIIV framework uses Hyperledger Practical Byzantine Fault Tolerance (PBFT) consensus mechanism to guard against ledger integrity. PBFT is designed to support permissioned blockchain systems and can withstand a malicious, faulty, or even an unresponsive entity, while still agreeing on the validity of transactions. Ensuring that no identity proofs or insurance claim data can be tampered with or forged by making the addition of verification records a consensus requirement among most trusted parties in the network, PBFT achieves a high level of credibility and robustness against any attacks.

IV. RESULTS AND DISCUSSION

A. Performance Evaluation

Table 1. DIIV Performance Metrics

Metric	Value
Matching Accuracy	99.4%
FAR	0.12%
FRR	0.43%
Verification Latency	1.43 s
Fraud Reduction Rate	92%

- **Accuracy of match (99.4%): The DIIV framework yields a matching accuracy of 99.4%, indicating** very reliable biometric checks. The feature-level fusion of the two modalities, face and fingerprint, mainly leads to this high accuracy because it captures a set of rich, discriminative features that single-modality systems do not. This level of precision significantly reduces both the false rejection of valid users and the false acceptance of impostors, thereby providing higher levels of security and user trust.
- **False Acceptance Rate (FAR) is 0.12 percent:** FAR of 0.12 percent serves to indicate the robustness of the system to unauthorized persons. FAR is the probability of acceptance of an imposter as a legitimate user. This exceedingly low value indicates that the fusion-based verification concept is highly capable of minimising the number of security breaches that arise due to false matches, hence making this system practically resistant to other kinds of spoofing attacks.

- **False Rejection Rate (FRR) 0.43%:** When the FRR is 0.43%, it indicates the percentage of legitimate users who are wrongly denied access. This low score indicates that the DIIV Framework has a high degree of usability, without creating levels of frustration for users and without compromising high security requirements. Adjustments of the fusion weight factor (α) are also crucial as a means of balancing usability and protection.

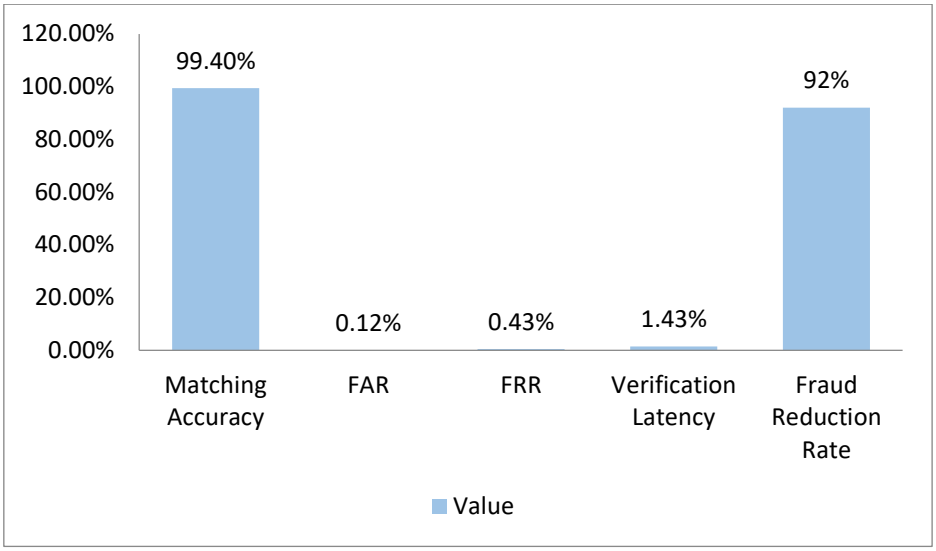

Figure 5. Graph representing DIIV Performance Metrics

- **Verification Latency – 1.43%:** The verification latency is a parameter logged as a 1.43% metric, representing the relative amount of time delay compared to the overall transaction or authentication time. This figure demonstrates that the DIIV system can handle biometric verification requests at high speeds, thanks to efficient feature extraction, fusion algorithms, and Hyperledger PBFT consensus. This makes the real-time identity verification of such latency important.
- **Fraud Reduction Rate – 92%:** The DIIV framework reduces fraud by 92% compared to traditional identity verification strategies. This performance was achieved through the combination of the following functions: secure biometric fusion, immutability provided by blockchain, and an automated payout mechanism within the payout system. The combination of these elements is capable of providing reliable protection against identity theft and enhancing overall confidence in the system.

B. Security Testing Results

The DIIV framework was tested to determine its security against common attack vectors targeting biometric and blockchain-based identity systems. All experimental results, as represented in Table 3, show that the resistance is very high in all the experimented attacks. The DIIV framework was highly resistant in the case of Man-in-the-Middle (MITM) attacks, where adversaries may want to interfere with the transmission of biometric data or transaction information. This is facilitated by the end-to-end encryption of all communication channels, which allows the use of Zero-Knowledge Proofs (ZKPs). ZKPs make it possible to verify that no data was sent in the raw form of biometrics. Consequently, intercepted data becomes useless to an attacker. It also rated highly against replay attacks, where earlier recorded data of the authentication process is resubmitted to achieve unauthorized access to the system. Such prevention is achieved through the use of dynamic session tokens and timestamps integrated into the verification mechanism, which makes the kill-chain of authentications unique and time-sensitive. All the efforts of reusing previous data do not pass verification. In the case of spoofing attacks carried out on facial recognition, such as photo, video, or 3D mask attacks, the DIIV framework continues to offer a high level of resilience due to liveness detection. These methods evaluate micro-movement, texture patterns, and infrared depth data to separate real faces from fake replicas.

In the same way, other fingerprint spoofing attacks, such as silicone mould fingerprints or printed patterns of fingerprints, were successfully countered. Multi-spectral imaging and ridge detail analysis are also used during capture, making it very difficult to verify a synthetic fingerprint. In general, the multi-layer security design of the DIIV framework, based on the incorporation of potent biometric anti-spoofing systems, the immutability of the blockchain, cryptography for privacy protection relying on the ZKP protocol, and the consensus feature based on Hyperledger PBFT, is effective against both network-based and biometric-type threats. These findings affirm that the system not only conforms to industry standards but also surpasses them in terms of secure digital identity verification.

C. Comparative Analysis

Compared to the conventional models of centralized control to verify the identity, Decentralized Insurance-Integrated Verification (DIIV) model shows a significant benefit with respect to speed, security and assurance to users. Centralized identity management systems are, as the name entails, normally based on one central authority or database to store and process users' credentials, and present a bottleneck of verification speed, and a single point of failure. DIIV, in its turn, utilizes a permissioned blockchain by Hyperledger PBFT consensus, which allows parallel verification request processing and largely decreases the processing latency. The measure verification latency includes a value of 1.43%, which means that DIIV will be able to conduct authentication within a minimum real-time capacity, regardless of the volume of requests made, without jeopardising accuracy. Centralized system in terms of attack surface would be an ideal target since all records of identity are kept in one single repository, implying that they are ideal targets when massive breaches are supposed. An effective attack on such a system can be used to compromise millions of identities on a single occasion. To mitigate this risk, DIIV decentralizes the verification data storage. The only biometric templates stored on-chain are hashed, so there is a guarantee that, regardless of access to blockchain data, they cannot be reengineered into usable biometric data. Also relevant is the aspect that feature-level biometric fusion assisted by Zero-Knowledge Proofs provides additional strength to tuning the authentication process, as spoofing, replay, and MITM attacks become significantly more difficult. One unique feature of DIIV will be the embedded financial guarantees provided by the insurance smart contract layer. Automated on-chain insurance payouts in case of identity theft are seldom implemented by centralized systems, especially those where centralized claims processing occurs manually and tends to take days or even weeks. DIIV automates this process so as to reliably have near instant payouts when the fraud has been confirmed with pre-set smart contract rules. This not only further builds trust with the user but also offers hard financial protection, which is lost in the majority of traditional verification systems. Altogether, architectural decentralization of DIIV, robust security of biometric fusion, and internal insurance mechanism of the latter make the presented system a more secure, efficient, and trust-supporting alternative to the current centralized approaches to identity verification.

V. CONCLUSION

This study introduced the Decentralized Insured Identity Verification (DIIV) system, a novel solution that combines the concept of blockchain-enabled Decentralized Identifiers (DIDs), biometric fusion of different features, and smart contracts-based insurance protocols into one comprehensive digital identity system. The framework has resolved some of the most significant deficiencies of the existing identity verification systems, such as the usage of centralized architecture, the susceptibility to biometric spoofing, and the absence of financial security to end users upon the compromise of their identities. DIIV uses Hyperledger PBFT as a consortium blockchain and ensures immutable, tamper-proof transactional workflows with high throughput; privacy is ensured using cryptographic hashing and Zero-Knowledge Proofs (ZKPs).

The biometric fusion feature combines both facial and fingerprint features by integrating them at the feature level, resulting in increased verification accuracy with a decreased False Acceptance Rate (FAR) and False Rejection Rate (FRR). Such a fusion method compensates for the inadequacies of authentication based on a single modality, i.e., vulnerability to spoofing attacks, and makes the system capable of performing within different environmental and operational contexts. The accuracy of matching recovered by the experiments is 99.4%, with a FAR of 0.12%, a FRR of 0.43%, and a fraud reduction rate of 92%. This proves the system's ability to balance security and readability. The availability of the insurance smart contract layer distinguishes DIIV from traditional digital identity systems. In the event of a proven compromise of identity, this layer automatically processes and settles claims without having to involve the time-consuming process of making manual adjudications. This kind of automation not only makes the ratification process quicker; it also provides users with actual monetary security, which, in turn, improves trust throughout the system. In addition, accountability and fairness are achieved because claims are executed openly on the blockchain, minimize disputes.

In comparison to centralized forms of identity verification, DIIV provides quicker authentication, minimizes the possibility of a mass breach of data, and prevents acts of fraud due to an in-built form of protection. Its distributed architecture ensures that there is no single point of failure. Additionally, on the side of ensuring attack resistance, it includes advanced anti-spoofing techniques that compound the difficulties in typical attacks, such as Man-in-the-Middle (MITM) attacks, replay, and biometric spoofing attacks. Finally, the DIIV system offers a future-proof, secure, and trusted digital identity solution that can be implemented in cloud-based financial services, e-governance, and other similar settings to ensure the most secure environments. The union of the decentralization of blockchain, biometric fusion accuracy, and the security offered to the users by insurance creates a new paradigm of digital identity verification. Future research can explore the addition of more biometric modalities, incorporating privacy-preserving machine learning models, and scaling the system to enable cross-border interoperability, thereby establishing a global standard in secure and insured digital identity management.

VI. REFERENCES

1. Odelu, V. (2019, June). IMBUA: identity management on blockchain for biometrics-based user authentication. In International Congress on Blockchain and Applications (pp. 1-10). Cham: Springer International Publishing.
2. Ghafourian, M., Sumer, B., Vera-Rodriguez, R., Fierrez, J., Tolosana, R., Moralez, A., & Kindt, E. (2023). Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis. arXiv preprint arXiv:2302.10883.
3. Gudala, L., Reddy, A. K., Sadhu, A. K. R., & Venkataramanan, S. (2022). Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. Journal of Artificial Intelligence Research, 2(2), 21-50.
4. Hammudoglu, J. S., Sparreboom, J., Rauhamaa, J. I., Faber, J. K., Guerchi, L. C., Samiotis, I. P., ... & Pouwelse, J. A. (2017). Portable trust: biometric-based authentication and blockchain storage for self-sovereign identity systems. arXiv preprint arXiv:1706.03744.
5. Shetty, A., Shetty, A. D., Pai, R. Y., Rao, R. R., Bhandary, R., Shetty, J., ... & Dsouza, K. J. (2022). Blockchain application in insurance services: A systematic review of the evidence. Sage Open, 12(1), 21582440221079877.
6. Chen, C. L., Deng, Y. Y., Tsaur, W. J., Li, C. T., Lee, C. C., & Wu, C. M. (2021). A traceable online insurance claims system based on blockchain and smart contract technology. Sustainability. 2021; 13: 9386.
7. Oham, C., Jurdak, R., Kanhere, S. S., Dorri, A., & Jha, S. (2018, July). B-fica: Blockchain-based framework for auto-insurance claim and adjudication. In 2018, the IEEE international conference on Internet of Things (iThings), IEEE green computing and communications (GreenCom), IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 1171-1180). IEEE.
8. Samunnisa, K., & Gaddam, S. V. K. (2023). Blockchain-Based Decentralized Identity Management for Secure Digital Transactions. Synthesis: A Multidisciplinary Research Journal, 1(2), 22-29.
9. Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings, 80, 2642-2646.
10. Dharavath, K., Talukdar, F. A., & Laskar, R. H. (2013, December). Study on biometric authentication systems, challenges and future trends: A review. In 2013, the IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-7). IEEE.
11. Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access, 10, 113436-113481.
12. Dib, O., & Rababah, B. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. Annals of Emerging Technologies in Computing (AETiC), 4(5), 19-40.
13. Sutcu, Y., Li, Q., & Memon, N. (2007, June). Secure biometric templates from fingerprint-face features. In 2007, IEEE Conference on Computer Vision and Pattern Recognition (pp. 1-6). IEEE.
14. Brown, D., & Bradshaw, K. (2016, May). A multi-biometric feature-fusion framework for improved uni-modal and multimodal human identification. In 2016, IEEE Symposium on Technologies for Homeland Security (HST) (pp. 1-6). IEEE.
15. Thirunagalingam, A. (2022). Enhancing Data Governance Through Explainable AI: Bridging Transparency and Automation. Available at SSRN 5047713.
16. Rattani, A., & Tistarelli, M. (2009, June). Robust multi-modal and multi-unit feature-level fusion of face and iris biometrics. In International Conference on Biometrics (pp. 960-969). Berlin, Heidelberg: Springer Berlin Heidelberg.
17. Bala, N., Gupta, R., & Kumar, A. (2022). Multimodal biometric system based on fusion techniques: a review. Information Security Journal: A Global Perspective, 31(3), 289-337.
18. Rusum, G. P., Pappula, K. K., & Anasuri, S. (2020). Constraint Solving at Scale: Optimizing Performance in Complex Parametric Assemblies. *International Journal of Emerging Trends in Computer Science and Information Technology*, *1*(2), 47-55. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I2P106
19. Pappula, K. K., & Anasuri, S. (2020). A Domain-Specific Language for Automating Feature-Based Part Creation in Parametric CAD. International Journal of Emerging Research in Engineering and Technology, 1(3), 35-44. https://doi.org/10.63282/3050-922X.IJERET-V1I3P105
20. Rahul, N. (2020). Optimizing Claims Reserves and Payments with AI: Predictive Models for Financial Accuracy. *International Journal of Emerging Trends in Computer Science and Information Technology*, *1*(3), 46-55. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I3P106
21. Pappula, K. K., Anasuri, S., & Rusum, G. P. (2021). Building Observability into Full-Stack Systems: Metrics That Matter. *International Journal of Emerging Research in Engineering and Technology*, *2*(4), 48-58. https://doi.org/10.63282/3050-922X.IJERET-V2I4P106

22. Pedda Muntala, P. S. R., & Karri, N. (2021). Leveraging Oracle Fusion ERP's Embedded AI for Predictive Financial Forecasting. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(3), 74-82. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I3P108
23. Rahul, N. (2021). Strengthening Fraud Prevention with AI in P&C Insurance: Enhancing Cyber Resilience. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(1), 43-53. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I1P106
24. Rusum, G. P. (2022). WebAssembly across Platforms: Running Native Apps in the Browser, Cloud, and Edge. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 107-115. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I1P112
25. Pappula, K. K. (2022). Architectural Evolution: Transitioning from Monoliths to Service-Oriented Systems. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 53-62. https://doi.org/10.63282/3050-922X.IJERET-V3I4P107
26. Jangam, S. K. (2022). Self-Healing Autonomous Software Code Development. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 42-52. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P105
27. Anasuri, S. (2022). Adversarial Attacks and Defenses in Deep Neural Networks. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 77-85. https://doi.org/10.63282/xs971f03
28. Pedda Muntala, P. S. R. (2022). Anomaly Detection in Expense Management using Oracle AI Services. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 87-94. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P109
29. Rahul, N. (2022). Automating Claims, Policy, and Billing with AI in Guidewire: Streamlining Insurance Operations. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 75-83. https://doi.org/10.63282/3050-922X.IJERET-V3I4P109
30. Rusum, G. P., & Anasuri, S. (2023). Composable Enterprise Architecture: A New Paradigm for Modular Software Design. *International Journal of Emerging Research in Engineering and Technology*, *4*(1), 99-111. https://doi.org/10.63282/3050-922X.IJERET-V4I1P111
31. Pappula, K. K. (2023). Reinforcement Learning for Intelligent Batching in Production Pipelines. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(4), 76-86. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I4P109
32. Jangam, S. K., & Pedda Muntala, P. S. R. (2023). Challenges and Solutions for Managing Errors in Distributed Batch Processing Systems and Data Pipelines. *International Journal of Emerging Research in Engineering and Technology*, *4*(4), 65-79. https://doi.org/10.63282/3050-922X.IJERET-V4I4P107
33. Anasuri, S. (2023). Secure Software Supply Chains in Open-Source Ecosystems. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 62-74. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P108
34. Pedda Muntala, P. S. R., & Karri, N. (2023). Leveraging Oracle Digital Assistant (ODA) to Automate ERP Transactions and Improve User Productivity. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(4), 97-104. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I4P111
35. Rahul, N. (2023). Transforming Underwriting with AI: Evolving Risk Assessment and Policy Pricing in P&C Insurance. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 92-101. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P110
36. Pappula, K. K. (2020). Browser-Based Parametric Modeling: Bridging Web Technologies with CAD Kernels. *International Journal of Emerging Trends in Computer Science and Information Technology*, *1*(3), 56-67. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I3P107
37. Rahul, N. (2020). Vehicle and Property Loss Assessment with AI: Automating Damage Estimations in Claims. *International Journal of Emerging Research in Engineering and Technology*, *1*(4), 38-46. https://doi.org/10.63282/3050-922X.IJERET-V1I4P105
38. Pappula, K. K. (2021). Modern CI/CD in Full-Stack Environments: Lessons from Source Control Migrations. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(4), 51-59. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I4P106
39. Pedda Muntala, P. S. R. (2021). Prescriptive AI in Procurement: Using Oracle AI to Recommend Optimal Supplier Decisions. *International Journal of AI, BigData, Computational and Management Studies*, *2*(1), 76-87. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V2I1P108
40. Rahul, N. (2021). AI-Enhanced API Integrations: Advancing Guidewire Ecosystems with Real-Time Data. *International Journal of Emerging Research in Engineering and Technology*, *2*(1), 57-66. https://doi.org/10.63282/3050-922X.IJERET-V2I1P107

41. Rusum, G. P., & Pappula, K. K. (2022). Federated Learning in Practice: Building Collaborative Models While Preserving Privacy. *International Journal of Emerging Research in Engineering and Technology*, *3*(2), 79-88. https://doi.org/10.63282/3050-922X.IJERET-V3I2P109
42. Pappula, K. K. (2022). Modular Monoliths in Practice: A Middle Ground for Growing Product Teams. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 53-63. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P106
43. Jangam, S. K., & Pedda Muntala, P. S. R. (2022). Role of Artificial Intelligence and Machine Learning in IoT Device Security. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 77-86. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P108
44. Anasuri, S. (2022). Next-Gen DNS and Security Challenges in IoT Ecosystems. *International Journal of Emerging Research in Engineering and Technology*, *3*(2), 89-98. https://doi.org/10.63282/3050-922X.IJERET-V3I2P110
45. Pedda Muntala, P. S. R. (2022). Detecting and Preventing Fraud in Oracle Cloud ERP Financials with Machine Learning. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 57-67. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I4P107
46. Rahul, N. (2022). Enhancing Claims Processing with AI: Boosting Operational Efficiency in P&C Insurance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 77-86. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P108
47. Rusum, G. P., & Pappula, K. K. (2023). Low-Code and No-Code Evolution: Empowering Domain Experts with Declarative AI Interfaces. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(2), 105-112. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I2P112
48. Pappula, K. K., & Rusum, G. P. (2023). Multi-Modal AI for Structured Data Extraction from Documents. *International Journal of Emerging Research in Engineering and Technology*, *4*(3), 75-86. https://doi.org/10.63282/3050-922X.IJERET-V4I3P109
49. Jangam, S. K., Karri, N., & Pedda Muntala, P. S. R. (2023). Develop and Adapt a Salesforce User Experience Design Strategy that Aligns with Business Objectives. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 53-61. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P107
50. Anasuri, S. (2023). Confidential Computing Using Trusted Execution Environments. *International Journal of AI, BigData, Computational and Management Studies*, *4*(2), 97-110. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I2P111
51. Pedda Muntala, P. S. R., & Jangam, S. K. (2023). Context-Aware AI Assistants in Oracle Fusion ERP for Real-Time Decision Support. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 75-84. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P109
52. Rahul, N. (2023). Personalizing Policies with AI: Improving Customer Experience and Risk Assessment. International Journal of Emerging Trends in Computer Science and Information Technology, 4(1), 85-94. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P110
53. Pappula, K. K., & Rusum, G. P. (2020). Custom CAD Plugin Architecture for Enforcing Industry-Specific Design Standards. *International Journal of AI, BigData, Computational and Management Studies*, *1*(4), 19-28. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V1I4P103
54. Pappula, K. K., & Anasuri, S. (2021). API Composition at Scale: GraphQL Federation vs. REST Aggregation. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(2), 54-64. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I2P107
55. Pedda Muntala, P. S. R., & Jangam, S. K. (2021). Real-time Decision-Making in Fusion ERP Using Streaming Data and AI. *International Journal of Emerging Research in Engineering and Technology*, *2*(2), 55-63. https://doi.org/10.63282/3050-922X.IJERET-V2I2P108
56. Rusum, G. P. (2022). Security-as-Code: Embedding Policy-Driven Security in CI/CD Workflows. *International Journal of AI, BigData, Computational and Management Studies*, *3*(2), 81-88. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I2P108
57. Pappula, K. K. (2022). Containerized Zero-Downtime Deployments in Full-Stack Systems. International Journal of AI, BigData, Computational and Management Studies, 3(4), 60-69. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I4P107
58. Jangam, S. K., Karri, N., & Pedda Muntala, P. S. R. (2022). Advanced API Security Techniques and Service Management. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 63-74. https://doi.org/10.63282/3050-922X.IJERET-V3I4P108

59. Anasuri, S. (2022). Zero-Trust Architectures for Multi-Cloud Environments. International Journal of Emerging Trends in Computer Science and Information Technology, 3(4), 64-76. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P107
60. Pedda Muntala, P. S. R., & Karri, N. (2022). Using Oracle Fusion Analytics Warehouse (FAW) and ML to Improve KPI Visibility and Business Outcomes. International Journal of AI, BigData, Computational and Management Studies, *3*(1), 79-88. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I1P109
61. Rahul, N. (2022). Optimizing Rating Engines through AI and Machine Learning: Revolutionizing Pricing Precision. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(3), 93-101. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I3P110
62. Rusum, G. P. (2023). Large Language Models in IDEs: Context-Aware Coding, Refactoring, and Documentation. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(2), 101-110. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I2P110
63. Pappula, K. K. (2023). Edge-Deployed Computer Vision for Real-Time Defect Detection. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 72-81. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P108
64. Jangam, S. K. (2023). Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 82-91. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P109
65. Anasuri, S., & Pappula, K. K. (2023). Green HPC: Carbon-Aware Scheduling in Cloud Data Centers. *International Journal of Emerging Research in Engineering and Technology*, *4*(2), 106-114. https://doi.org/10.63282/3050-922X.IJERET-V4I2P111
66. Reddy Pedda Muntala , P. S. (2023). Process Automation in Oracle Fusion Cloud Using AI Agents. International Journal of Emerging Research in Engineering and Technology, 4(4), 112-119. https://doi.org/10.63282/3050-922X.IJERET-V4I4P111
67. Pappula, K. K., & Rusum, G. P. (2021). Designing Developer-Centric Internal APIs for Rapid Full-Stack Development. *International Journal of AI, BigData, Computational and Management Studies*, *2*(4), 80-88. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V2I4P108
68. Pedda Muntala, P. S. R., & Jangam, S. K. (2021). End-to-End Hyperautomation with Oracle ERP and Oracle Integration Cloud. *International Journal of Emerging Research in Engineering and Technology*, *2*(4), 59-67. https://doi.org/10.63282/3050-922X.IJERET-V2I4P107
69. Rusum, G. P., & Pappula, kiran K. . (2022). Event-Driven Architecture Patterns for Real-Time, Reactive Systems. *International Journal of Emerging Research in Engineering and Technology*, *3*(3), 108-116. https://doi.org/10.63282/3050-922X.IJERET-V3I3P111
70. Jangam, S. K. (2022). Role of AI and ML in Enhancing Self-Healing Capabilities, Including Predictive Analysis and Automated Recovery. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 47-56. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I4P106
71. Anasuri, S. (2022). Formal Verification of Autonomous System Software. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 95-104. https://doi.org/10.63282/3050-922X.IJERET-V3I1P110
72. Pedda Muntala, P. S. R. (2022). Natural Language Querying in Oracle Fusion Analytics: A Step toward Conversational BI. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(3), 81-89. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I3P109
73. Rusum, G. P. (2023). Secure Software Supply Chains: Managing Dependencies in an AI-Augmented Dev World. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(3), 85-97. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I3P110
74. Jangam, S. K. (2023). Data Architecture Models for Enterprise Applications and Their Implications for Data Integration and Analytics. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 91-100. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I3P110
75. Anasuri, S., Rusum, G. P., & Pappula, K. K. (2023). AI-Driven Software Design Patterns: Automation in System Architecture. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(1), 78-88. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I1P109
76. Pedda Muntala, P. S. R., & Karri, N. (2023). Managing Machine Learning Lifecycle in Oracle Cloud Infrastructure for ERP-Related Use Cases. *International Journal of Emerging Research in Engineering and Technology*, *4*(3), 87-97. https://doi.org/10.63282/3050-922X.IJERET-V4I3P110