TABLE X Existing Research Focus for Identity Verification

Study	Research Focus	User Control	Analysis
Patil P et al. [3]	Preventing illegal activities in banks.	Voting mechanism for bank tampering prevention.	Improves efficiency and security. Requires inter-bank cooperation.
Mamun A et al. [19]	Document verification for banking.	Users control data sharing with multiple banks.	Saves time and money, but users must manage data sharing proactively.
Kumar M et al. [4]	Removing the need for third-party trust	Full control over KYC data.	Streamlines the KYC process, but involves complex coordination.
Moyano J et al. [67]	Dynamic information updates and dissemination among FIs.	Users manage data sharing.	Reduces costs and increases efficiency, but ensuring data consistency is challenging.
Ullah N et al. [82]	Speeding up KYC clearance and securing data sharing.	Users manage data updates.	Reduces redundancy and speeds up clearance, but requires significant initial setup.
Kapsoulis N et al. [69]	Effective and time-efficient KYC activities.	Users control data sharing.	Efficient KYC activities, but faces integration complexity.
De Salve A et al. [84]	Trust relationships in SSI.	Enhanced user control through SSI.	Enhances trust relationships, but complex multi-layer implementation.
Ferdous M et al. [6]	Developing the SSI4Web framework for SSI.	Users have full control over identity information.	Streamlines identity verification, but faces adoption barriers in existing systems.
Malik S et al. [45]	Privacy-preservation in trading activities.	Users control identity and trading activities.	Efficient trade verification, but requires extensive setup.
Schlatt V et al. [91]	Solving KYC challenges with blockchain-based SSI.	Users control KYC data.	Efficient KYC processes, but resource-intensive implementation.
Satybaldy A et al. [70]	Assessing and contrasting SSI systems.	Users manage their identities.	Enhances understanding of SSI systems, but complex implementation and interpretation.
Gilani K et al. [31]	One-time proof-verification mechanism.	Users manage proof verification.	Efficient identity verification, but depends on effective smart contract implementation.
Dong C et al. [5]	Access-level security and privacy protection.	Users manage access-level security.	Secure UAV delivery system, but involves technical challenges in edge computing.
Moya C et al. [89]	Study of ZKP protocols.	Users benefit from advanced cryptographic security.	Enhances security, but requires substantial computational resources.
Soni A et al. [95]	Know Your Customer process, challenges, and big data analysis.	Users manage large datasets.	Enhances data integrity and security, improves efficiency; implementation complexity and scalability issues.
Takaragi K et al. [79]	Customer privacy protection in CBDC systems.	Users benefit from strong privacy protections.	Ensures privacy, but complex implementation and performance overheads.
Naik N et al. [92]	Evaluating potential attacks and security risks.	Users benefit from systematic risk assessment.	Enhances security in SSI systems, but resource-intensive analysis and mitigation.
Satybaldy A et al. [92]	Addressing complexity and interoperability in digital verification.	Users manage document verification.	Secure verification, but complex interoperability challenges.
Pralhad Rankhambe B et al. [81]	Document verification using blockchain.	Users control document verification.	Reduces costs, but requires robust blockchain infrastructure.
Parra Moyano J et al. [80]	Reducing cost and improving user experience.	Users benefit from reduced costs and improved experience.	Increases transparency, but faces implementation complexity.
Kim B et al. [9]	Identifying security threats in DID services.	Users benefit from detailed security analysis.	Enhances security understanding, but addressing threats can be complex and resource-intensive.
Ding Y et al. [71]	Scalable cross-chain access control and identity authentication.	Users manage cross-chain interactions.	Efficient cross-chain interactions, but managing interoperability is complex.

by banks, enabling safe sharing with multiple financial institutions. These studies collectively demonstrate how blockchain-enabled eKYC systems are transforming identity verification by prioritizing user control, improving privacy and security, and empowering individuals to maintain autonomy over their personal data.

RQ3: iii) How does selective disclosure enhance privacy in identity verification, and which techniques are utilized?

The concept of selective disclosure in digital identity management and authentication systems is crucial for maintaining user privacy. In this systematic review, we tried to find out the contribution of selective disclosure to protect user privacy during identity verification. We also explore the approaches and supporting technologies for selective disclosure. Selective disclosure enhances security and efficiency by allowing users to share only the necessary information for a transaction, such as age, instead of full birth details. This approach reduces data misuse, minimizes digital footprints, and aligns with privacy regulations like GDPR, which advocate for minimal data processing. Advanced cryptographic techniques, such as Zero-Knowledge Proofs (ZKPs) [62], [87], verify claims without exposing additional data, building trust and safeguarding user privacy.

Techniques used to achieve selective disclosure: Several key approaches are utilized to achieve selective disclosure in the process of identification. This systematic review explores the