TABLE XIII Applied Technologies, Tools and Approaches in Various Studies

Study	Applied Technologies, Tools and Approaches
Mamun A et al. [18]	IPFS, Blockchain, Smart Contracts, GPg4win, Encryption
Patil P et al. [3]	Ethereum Blockchain, Smart Contracts, Remix IDE, Solidity, Public/Private Cryptographic Key Pair, Hash Functions, Voting Mechanism
Kumar M et al. [4]	Digital Signatures, Hash Functions, Public/Private Cryptographic Key Pair, Asymmetric Encryption, QR Codes, 2FA, Smart Contracts
Norvill R et al. [94]	Ethereum Blockchain, Smart Contracts, Geo-address validation API service, Name Checking Service, Daily Due Diligence Service, API Server
Moyano J et al. [91]	Ethereum Blockchain, Smart Contracts, Public/Private Cryptographic Key Pair, IPFS, Asymmetric Encryption, Symmetric Encryption, Digital Signatures, Secure Hash Algorithm (SHA), ERC-20 Token, Node.js
Dragan C et al. [95]	Off-Chain Storage, Public/Private key Cryptography, Symmetric Encryption, Digital Signature, Pseudo-Random Functions, Smart Contracts, PRF-Based Key Derivation, Certification Compliance
Ullah N et al. [75]	Hyperledger Fabric, JSON, Asymmetric Cryptosystem, Docker, REST API, Chaincode, Cryptographic Hash Functions
Kapsoulis N et al. [69]	IPFS, Public/Private key, Digital signatures, CRUD, Smart Contracts, Alastria Network
De Salve A et al. [82]	Ethereum, Solidity, SSI, Web of Trust (WoT), DIDs, Verifiable Credentials (VCs), Digital Wallets, ZKPs, Smart Contracts, Hyperledger Fabric, Spring Boot, Web3j, Goerli Testnet, Hyperledger Besu
Ferdous M et al. [6]	Hyperledger Aries, Hyperledger Indy, DIDs, VCs, SSI, Aries Mobile Agent React Native, Indicio Public Mediator, Node.js, Python, JSON-LD, BCovrin Dev Testbed
Gilani K et al. [29]	Ethereum Blockchain, Smart Contracts, DIDs, VCs, SSI, IPFS, Public/Private Cryptographic Key Pair, Solidity, Ganache CLI, Web3j, JSON-LD, Oracle, Single Sign-On (SSO) Mechanism
Dong C et al. [5]	Ethereum Blockchain, SSI, DID, VCs, Smart Contracts, Solidity, Remix IDE, JavaScript VM, Public Key Infrastructure (PKI), Merkle Tree, Digital Signatures, Hash Functions
Dieye M et al. [7]	Blockchain, ZKP (Schnorr Protocol, Fiat-Shamir Transformation), DID, Verifiable Claims, Electronic Identification And Trust Services (eIDAS), GDPR, Hash Functions, Selective Disclosure
Moya C et al. [68]	ZKPs (Feige-Fiat-Shamir, Guillou-Quisquater, and Schnorr), Python 3.10.4, SSI, Tkinter, TCP connection, public/private key, encryption, authentication system, brute-force attack simulation, MITM attack simulation
Konkin A et al. [67]	Ethereum-Based Blockchain, Masterchain, zk-SNARKs, Ring Signatures, ZKP, NIZK, Public Key Infrastructure (PKI), Digital Signatures, Hash-Based Message Authentication Code (HMAC), Certified GOST Crypto Algorithms, ZoKrates Framework
Malik S et al. [43]	Hyperledger Indy, Hyperledger Fabric, Sovrin, DIDs, VCs, ZKPs, Ciphertext Policy Attribute-Based Encryption (CP-ABE), JSON Web Tokens, Charm-crypto library, Digital Wallets, Cryptographic Signatures, Query Smart Contracts (QSC)
Pauwels P et al. [44]	ZKP, SSI, DIDs, VCs, JSON Web Tokens (JWT), Cryptographic Accumulators, Predicate Proofs, Compound Proofs
Fugkeaw S et al. [22]	CP-ABE, Blockchain, IPFS, Smart Contracts, Digital Signatures, Symmetric Encryption, Public Key Infrastructure (PKI), AES Encryption, Attribute-Based Access Control, ZKPs, Hash Functions
Soni A et al. [97]	Big Data Analytics, Fuzzy Matching, MapReduce, Hadoop, NoSQL, Data Mining Frameworks, Optical Character Recognition (OCR)
Takaragi K et al. [72]	ZKP, Delegatable Anonymous Credential (DAC), Privacy-Enhanced PKI, Bulletproofs, Secure Kernel for Supply Chain (SK4SC), Central Bank Digital Currency (CBDC), NIZKP
Schlatt v et al. [87]	Hyperledger Indy, SSI, DIDs, VCs, Cloud Agents/Wallets, Smart Contracts
Naik N et al. [88]	Attack tree model, Risk matrix, SSI, DID
Satybaldy A et al. [73]	Blockchain, SSI, VCs, digital wallets, DIDs, cryptographic keys, ZKP, selective disclosure, Hyperledger Indy, revocation registries, digital signatures, pairwise DIDs, smart contracts, PKI, GDPR, encryption
Satybaldy A et al. [83]	SSI, Blockchain, cryptographic proofs, digital wallet, VCs, DIDs, selective disclosure, ZKPs, JSON-LD, Hyperledger Indy, Ethereum, Sovrin, IPFS, GDPR, cryptographic keys, verifiable presentations
Parra Moyano J et al. [96]	Blockchain, Smart Contracts, PKI, Hash Functions, R3 Corda, JVM
Pralhad Rankhambe B et al. [92]	Smart Contracts, Ethereum, Hyperledger Fabric, PKI, Cryptographic Hashing, Digital Tokens, Plasma Framework, Asymmetric Key Cryptography, IPFS
Kim B et al. [9]	DID, Decentralized Key Management System (DKMS), VC, Microservice Architecture (MSA), Blockchain, Kubernetes, Chameleon Hash (CH), Attribute-Based Encryption (ABE), Shamir Secret Sharing Scheme (SSSS), JSON, JSON-LD, CBOR, ED25519, SHA-512, Curve25519ZKP, Sovrin, Uport, Jolocom, Hyperledger Aries, Hyperledger Indy, WQL, MongoDB, SQL
Dhiman B et al. [62]	Ethereum Blockchain, Fully Homomorphic Encryption (FHE), Smart Contracts, ZKP, Secure Hash Algorithm (SHA), PKI, Paillier Cryptosystem Gas Optimisation, Filtering
Ding Y et al. [93]	Ethereum, Hyperledger Fabric, Fisco BCOS, CITA, Xuperchain, Superchain, Auto Agents, Cross-Chain Smart Contracts, AGRobot, Relay Chain Scheme, PKI, Digital Signatures
Mukta R et al. [84]	Blockchain, Smart Contracts, Ethereum, Sovrin, Hyperledger Fabric, DIDs, VCs, SSI, ZKP, Redactable Signatures, JWT, Flutter, Node.js, Web3.js, Merkle Tree, GGM Tree, Cryptographic Hash Functions,
Ramic S et al. [64]	Selective Disclosure, Merkle Trees, Boneh-Lynn-Shacham (BLS) Signatures, ZKP, Cryptographic Hash Functions, Verifiable Presentations, Aggregated Signatures, JSON
Yamamoto D et al. [65]	BBS+ Signature, VCs, Selective Disclosure, Linked Data, JSON-LD, RDF Graphs, Canonicalization Algorithms, ZKPs, DIDs
De Salve A et al. [85]	Selective Disclosure, SSI, DIDs, VCs, Ethereum Blockchain, JWT, Hashing Functions (HMAC, SHA3-256, SHA3-512), Digital Signatures, Cryptographic Proofs, PKI, Linked Data, ZKP

TABLE XIII Applied Technologies, Tools and Approaches in Various Studies (Continued)

Study	Applied Technologies, Tools and Approaches
Fotiou N et al. [66]	Selective Disclosure, VCs, ZKP, OAuth 2.0, BBS+ Digital Signatures, JSON-LD, Web of Things (WoT), Digital Signature Scheme, JSON Canonicalization (JCan), HTTP Proxy
Kalos V et al. [86]	SSI, VC, JSON, JSON-LD, Selective Disclosure Cryptographic Protocols, ZKP, Canonicalization Algorithms, Anonymous Credentials
Slamanig D et al. [63]	Proxy Re-Encryption, Redactable Signatures, Digital Signatures, Public Key Infrastructure(PKI)
Tian R et al. [90]	Erasure Coding (EC), Merkle B-tree (MB-tree), Blockchain, Selective Disclosure, VCs, Smart Contracts, Cryptographic Proofs,
Singh K et al. [61]	Hyperledger Fabric, Short Signature, Pairing, Elliptic Curve Cryptography (ECC), ECDSA, NIZKP, Schnorr PoK, Commitment Schemes, Bilinear Pairing, Java, Go, Hyperledger Fabric, Java SDK
Yang Z et al. [59]	Merkle Tree, AES Encryption, SHA1 Hashing, ZKP, Fiat-Shamir Heuristic, Bulletproofs, ECC Signature Algorithm, Smart Contracts, Consortium Blockchain, DID, Credential Hashing, Attribute-Based Verification, Digital Certificates, Minimal Disclosure Authentication
Mukta R et al. [76]	Hyperledger Fabric, Selective Disclosure, Redactable Signature, Smart Contracts, DIDs, VCs, SSI, GGM Tree, Merkle Hash Tree, Node.js, Web3.js, REST Server, Google Drive, Cryptographic Hash Functions, JSON-LD
Li Z [89]	Ethereum, Solidity, Web3, Java SDK, JPBC Library, BLS Aggregate Signature, DID, VC, Selective Disclosure
Yu Y et al. [77]	Ethereum blockchain, smart contracts, signature scheme, zero-knowledge proof of knowledge (ZKPoK), selective revocation, bilinear maps, pairing-based accumulators
Deniz Sarier N [70]	Blockchain, Biometric-based credentials, Selective Disclosure, ZKP, Dynamic Accumulators, Fuzzy Extractors, Merkle Trees, Schnorr Signatures, Encryption, Bitcoin, Ethereum, GDPR compliance mechanisms, Tamper-proof devices, Industrial IoT (IIoT)
Kaneriya J et al. [60]	Blockchain, Smart Contracts, Ethereum, Hyperledger, Sovrin, Selective Disclosure, DIDs, VCs, ZKP, Digital Signatures, IPFS, Attribute-Based Encryption (ABE), Consent Tokens, PKI, Merkle Trees, REST API, Web3.js, Solidity

TABLE XIV Smart Contract Support for Identity Verification

Study	Impact of Smart Contracts
Patil P et al. [3]	Automation and transparency, reduced manual intervention, enhanced auditability.
Kumar M et al. [4]	Secure and efficient verification, tamper-proof records, reduced fraud.
Moyano J et al. [91]	Dynamic updating, real-time dissemination, enhanced data accuracy.
Ullah N et al. [75]	Streamlined KYC process, increased efficiency, reduced operational costs.
Kapsoulis N et al. [69]	Privacy-oriented verification, robust access control, compliance with data protection.
De Salve A et al. [82]	Trust frameworks for SSI, user autonomy, decentralized identity management.
Gilani K et al. [29]	User-controlled management, selective disclosure, granular data sharing.
Dong C et al. [5]	Scalable authentication, cross-chain interoperability, improved security.
Moya C et al. [68]	Secure verification, privacy with ZKP, data confidentiality.
Malik S et al. [43]	Privacy-preserving management, enhanced security and traceability in supply chains.
Pralhad Rankhambe B et al. [92]	Optimized KYC process, automated verification, improved customer experience.
Ding Y et al. [93]	Efficient cross-chain verification, transparency, compatibility.
Dhiman B et al. [62]	Secure decentralized verification, homomorphic encryption, data confidentiality.

TABLE XV 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. [18]	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. [91]	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. [75]	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. [82]	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. [43]	Privacy-preservation in trading activities.	Users control identity and trading activities.	Efficient trade verification, but requires extensive setup.
Schlatt V et al. [87]	Solving KYC challenges with blockchain-based SSI.	Users control KYC data.	Efficient KYC processes, but resource-intensive implementation.
Satybaldy A et al. [73]	Assessing and contrasting SSI systems.	Users manage their identities.	Enhances understanding of SSI systems, but complex implementation and interpretation.
Gilani K et al. [29]	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. [68]	Study of ZKP protocols.	Users benefit from advanced cryptographic security.	Enhances security, but requires substantial computational resources.
Soni A et al. [97]	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. [72]	Customer privacy protection in CBDC systems.	Users benefit from strong privacy protections.	Ensures privacy, but complex implementation and performance overheads.
Naik N et al. [88]	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. [88]	Addressing complexity and interoperability in digital verification.	Users manage document verification.	Secure verification, but complex interoperability challenges.
Pralhad Rankhambe B et al. [92]	Document verification using blockchain.	Users control document verification.	Reduces costs, but requires robust blockchain infrastructure.
Parra Moyano J et al. [96]	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. [93]	Scalable cross-chain access control and identity authentication.	Users manage cross-chain interactions.	Efficient cross-chain interactions, but managing interoperability is complex.