THE USE OF INNOVATIVE TECHNOLOGIES FOR THE PREVENTION AND DETECTION OF CRIMES RELATED TO DOCUMENT FORGERY

**HANNA VALIHURA[1], IHOR NOVIKOV[2], MARIIA DIAKUR[3],
OLENA YUSHCHYK[4], VLADYSLAV KUTSENKO[5]**

[1]Interregional Academy of Personnel Management, Ukraine

[2]Rivne Scientific Research and Forensic Center of the Ministry of Internal Affairs of Ukraine, Ukraine

[3]Yuriy Fedkovych Chernivtsi National University, Department of Criminal Law, Ukraine

[4]Yuriy Fedkovych Chernivtsi National University, Department of Criminal Law, Ukraine

[5]National University "Zaporizhzhia Polytechnic", Department of Criminal, Civil and International Law, Ukraine

E-mail: [1]innapench@gmail.com, [2]igornovikov@gmail.com, [3]dyakurmariia@chnu.edu.ua,
[4]olenayuschyk@chnu.edu.ua, [5]kutsenkovlad@ukr.net

ABSTRACT

The relevance of the study is underscored by the proliferation of digital forgery and the need for comprehensive solutions to ensure the authenticity of documents and their legal validity in notarial proceedings. The aim of the study is to substantiate and validate the architecture of preventive forgery detection with increased invariance, compatibility and cryptosecurity. The research employs methods as follows: technological typification, comparative analysis, technical and architectural decomposition, functional enhancement, and simulation prediction. An analysis encompassing 33 services and 7 technology classes revealed that complex SSI solutions exhibit the highest level of completeness. The optimized Microsoft Entra Verified ID demonstrates a reduction of 44.7% in latency, 61.6% in anchoring time, and 57% in cloud usage, alongside a 2.5% enhancement in detection accuracy − thereby substantiating the effectiveness of protocol level forgery resistance. The scientific novelty lies in the development of a SSI architecture that integrates BBS+, ZKP and Edge AI thereby harmonizing crypto resilience, offline validation, and an elevated degree of interoperability. Prospects for future research include the development of a prototype SSI architecture designed for the field testing of efficiency, scalability and resilience under real operational load and variable network conditions, as well as evaluating its suitability for electronic notarial proceedings.

Keywords: *Cryptographic Signatures; Blockchain Anchoring; Decentralized Identifiers (DID); Zero-Knowledge Proofs; Decentralized Storage*

1. INTRODUCTION

Due to the escalation of digital threats, document forgery has become pervasive, jeopardizing the legal integrity, security of identity, the sustainability of digital governance and the validity of electronic notarial acts [1], [2]. The application of modern technologies — such as cryptographic signatures, blockchain registration, AI/ML analytics, decentralized identifiers (DID), Zero-Knowledge Proofs, and content-oriented storage —due to architectural data invariance fosters a new paradigm for countering forgery [3], [4], [5]. However, existing solutions predominantly emphasize post-fact authentication, which is resource-intensive and often ineffectual given the intricate nature of forgeries [6], [7], [8]. This underscores the imperative for the advancement of complex Self-Sovereign Identity (SSI) architectures capable of implementing the principles of preventive verification through multi-level digital certification, selective data disclosure, lay anchoring, and offline identification utilizing evidence-protected cryptographic mechanisms [9], [10].

The purpose of the study is to formalize and empirically verify the architectural model of preventive detection of document forgery characterized by an enhanced level of invariance, interoperability and cryptographic resilience.

To achieve the specified goal, the following tasks were undertaken:

– to typify services based on their functional features;

– to conduct a comparative analysis of the technical and functional characteristics of the above services;

– to decompose the target architecture across structural levels;

– to develop a model for the functional enhancement of the architecture;

to evaluate the performance of the optimized model through simulation predictions.

2. LITERATURE REVIEW

Let us consider the contemporary landscape of scientific advancements pertaining to the deployment of innovative technologies aimed at the prevention and detection of crimes related to document forgery.

Sukhija et al. [11] substantiate the feasibility of employing machine learning and deep learning methodologies to identify print sources, authorship of digitized manuscripts, and the detection of digital forgeries. Their research systematically categorizes both active (extrusion features, digital signatures) and passive (texture analysis, frequency-spatial features, noise artifacts) techniques as tools of preventive digital forensics.

In contrast, Li et al. [12] delve more profoundly into the subject and substantiate the efficacy of a passive multi-category document forgery detection algorithm built on spatio-frequency domain analysis and multiscale feature fusion. The proposed model, which integrates frequency transformations, an attention mechanism, HRNet, and a multi-level supervision module, facilitates the localization and typification of forgeries, achieving an enhancement in accuracy (F1 score) of 5.73%.

Furthermore, Karale [13] asserts the feasibility of employing blockchain technologies for the verification of academic and professional documents, underscoring the immutability, decentralization, and transparency inherent in these systems. The study explores the integration of decentralized applications (dApps), smart contracts, InterPlanetary File System (IPFS), and cryptographic hashing as mechanisms to ensure authenticity, reduce costs, and mitigate forgery risks.

A similar solution was developed by Kale et al. [14], who introduce the Doc Chain system, which facilitates the verification of electronic medical records through blockchain technology and the Web3.storage platform. By comparing document hash identifiers, this system provides cryptographically secure records' authentication and personalized linking to patients, thereby enhancing data security and traceability.

A more comprehensive solution utilizing similar technologies was proposed by Han and Son [15], who engineered a decentralized document management system (DDMS) that amalgamates blockchain, IPFS, and Shamir's secret sharing scheme to facilitate secure storage, access control, and verification of digital documents integrity. Experimental findings indicate a marked enhancement in protection against forgery and unauthorized access when compared to conventional DMS, while maintaining an acceptable performance level.

Another innovative solution employing the aforementioned cryptographic protection technology was introduced by Rizky et al. [16]. They devised a blockchain-based AlphaSign digital signature system that enables decentralized document verification, increases resilience to cyber threats, and mitigates the risks associated with phishing and falsification. By leveraging Agile Scrum methodologies and QR codes for automated verification, the system ensures robust data protection and transparency in document circulation, particularly against the backdrop of escalating cyber attacks on governmental and corporate entities.

Methods for identifying the graphic elements' forgery were examined by Song et al. [17], who propose an innovative two-branch CAFTB-Net neural network designed to detect forgeries in document images through an integrative approach that combines spatial analysis with noise domain processing. Leveraging the capabilities of the SRM filter, cross-attention mechanisms, as well as the synthesis of local and global features, the model attains impressive reliability metrics (F1 = 0.819/0.948; AUC = 0.933/0.764), surpassing existing digital forensics algorithms.

Next, Mirzanli et al. [18] introduced a hybrid methodology for detecting forged documents that employs UV—Vis and FTIR-ATR spectroscopy in conjunction with principal component analysis to classify ballpoint inks by color and brand. The findings underscore the remarkable discriminative capacity of FTIR-ATR, which, even with a limited sample size, facilitates the accurate identification of forgeries, thereby proving effective in laboratories equipped with minimal resources.

Likewise, aspects of the aforementioned technology were also investigated by Hao et al. [19], elucidating the efficacy of the synergistic application of Raman and video spectroscopy to timestamps in instances of document forgery. The proposed methodology facilitates the identification of temporal fluctuations in the composition and morphology of inks that occur subsequent to refilling, thereby ensuring a reliable fixation of the imprinting time and the fraud detection.

Advocates of digital methodologies for preventing forgery include Kunekar et al. [8], who implemented a cryptographically robust document verification system drawing upon the generation of a pseudo-random nonce and the computing a hash function derived from the concatenated contents of the document and the nonce, followed by the subsequent storage of the resultant hash. Accordingly, the transmitted document undergoes re-hashing on the verifier's end with the corresponding nonce. Such an approach enables the ascertainment of integrity or modification in a deterministic manner, thereby increasing the trustworthiness of the authentication process.

The abovementioned publications substantiate the growing role of innovative technologies in the detection and prevention of document forgery, encompassing a diverse array of approaches —from deep learning, spatial frequency analysis and spectroscopy to blockchain architectures and cryptographic integrity control methods. The proposed solutions enhance detection accuracy, strengthen resistance to alterations, ensure reliability of verification, and offer applicability under conditions of constrained resources or heightened cyber threats. This collective framework establishes a robust technical and technological foundation for combating documentary forgery, including guaranteeing the integrity of electronic notarial acts within decentralized digital environments.

3. METHODOLOGY

3.1. Research procedure

The flowchart of the present study is given below Figure 1: *The F*

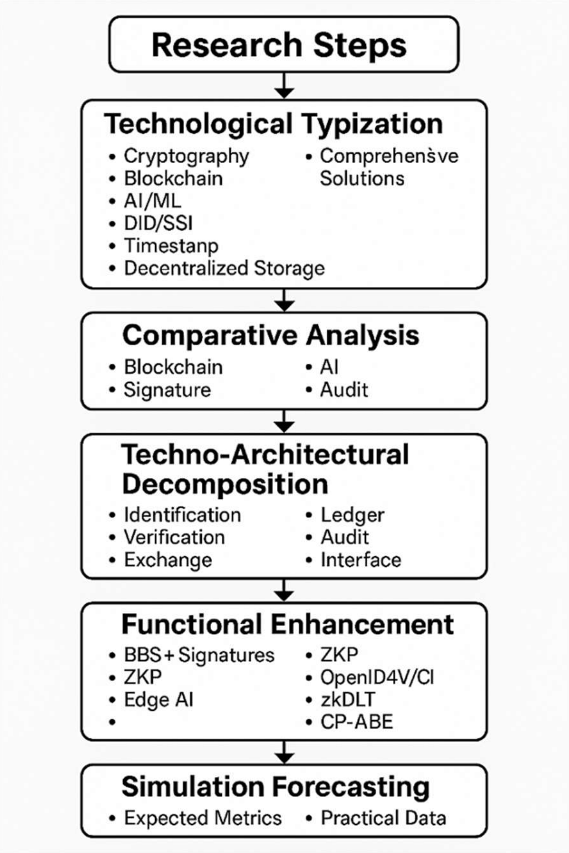

Figure 1: The Flowchart Of The Study
Source: created by the authors

3.2. Methods

In the present study, the following methods were used:

1. The method of technological typification involving the classification of services according to the type of technologies used (cryptography, blockchain, AI/ML, DID/SSI, timestamp, decentralized storage, complex solutions) to formalize each category's functional purpose.

2. The comparative analysis method entails the comparison of services according to five technical and functional criteria (blockchain, signature, AI, DID, audit) to identify the most comprehensive SSI architecture (Microsoft Entra Verified ID).

3. The method of technical and architectural decomposition consists of a layer-by-layer detailing of including identification, verification, exchange, ledger, audit and interface modules.

4. The method of functional enhancement involves the formulation of an optimization strategy through the integration of new technologies (BBS+

Signatures, ZKP, Edge AI, OpenID4VCI, ZKDLT, CP-ABE) at each architectural level.

5. The simulation forecasting method encompasses the calculation of anticipated performance metrics of the optimized architecture, drawing upon the technical characteristics of the implemented solutions, as well as a comparative analysis with basic practical data.

3.3. Sampling

The sample of this study consists of modern solutions for the detection and prevention of crimes related to document forgery, a total of 33 services (

Table *1.*)

Table 1. The Study Sample

Name of the service	Brief description	Ref
DocuSign	E-signature service	https://www.docusign.com/
Adobe Sign	Digital Signature Platform	https://www.adobe.com/sign.html
SignRequest	Online document signing	https://signrequest.com/
Notarize	Online notarization	https://www.notarize.com/
Signicat	Signature and identification in the EU	https://www.signicat.com/
Validated ID	Qualified signature and ID	https://www.validatedid.com/en
IDnow AutoIdent	Automatic identification	https://www.idnow.io/
Blockcerts	Blockchain-certification of documents	https://www.blockcerts.org/
VeriDoc Global	Verification via blockchain	https://www.veridocglobal.com/
AlphaSign	Signature and QR on the blockchain	https://www.alphasign.io/
OriginStamp	Timestamp via blockchain	https://originstamp.com/
KILT Protocol	SSI on the Polkadot blockchain	https://www.kilt.io/
Vottun	Verification and certification	https://vottun.com/
ProofSpace	Decentralized Data Verification	https://proofspace.id/
Certik Verify	Security and verification of smart contracts	https://www.certik.com/products/kyc
DocuSeal	Blockchain-Verification PDF	https://www.docuseal.co/
Onfido	AI Document Verification	https://onfido.com/
Jumio	ID Verification Platform	https://www.jumio.com/
IDnow	AI analysis of person and document	https://www.idnow.io/
Microsoft Entra Verified ID	AI + DID + claims verification	https://www.microsoft.com/security/business/identity-access/microsoft-entra
CAFTB-Net	Neural network to detect fraud	https://github.com/topics/caftb-net
Hyperledger Indy	DID Network for SSI	https://www.hyperledger.org/use/hyperledger-indy
Sovrin	Self-Government Identity Infrastructure	https://sovrin.org/
uPort	DID to Ethereum	https://www.uport.me/
Trinsic	SSI and DID tools	https://trinsic.id/
Civic	Mobile Identification	https://www.civic.com/
TrustGrid	Decentralized ID for organizations	https://www.trustgrid.com/
OpenTimestamps	Timestamp without disclosing content	https://opentimestamps.org/
Vottun Timestamp	Blockchain timestamps	https://vottun.com/
IPFS	Content-Oriented Storage	https://ipfs.tech/
Filecoin	IPFS Saving App	https://filecoin.io/
Web3. Storage	Hosting on IPFS with API	https://web3.storage/
DocChain	Storage of medical records	https://github.com/kale123/DocChain

Source: created by the authors

3.4. Tools

In this study, the following set of metrics was used to evaluate the effectiveness of digital solutions for detecting and preventing crimes related to document forgery (

Table 2).

Table 2: Performance Metrics Of The Services Related To Document Forgery Detection And Prevention

Metric (unit)	Mathematical apparatus	Measurement methods
Average verification latency (ms)	$\Delta t = \frac{1}{n}\sum_{i=1}^{n}\left(t_i^{verify} - t_i^{request}\right)$, where n is the number of transactions	Measured as the average time between the moment of the verification request and the receipt of the n verification result transactions
Average anchoring time (s)	$\overline{T}_{anchor} = \frac{1}{m}\sum_{j=1}^{m} T_j^{commit}$, where m is the number of DID entries	Defined as the average time elapsed from the creation of DID to its entering in the ledger
Cloud resource consumption (%)	$C_{cloud} = \left(\frac{U_{cloud}}{U_{total}}\right) \times 100\%$, where U is the used computing resources	U_{cloud} is the number of CPU/calls/cloud storage; U_{total} is the total resource capacity (including edge components)
Falsification detection accuracy (%)	$Accuracy = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) \times 100\%$	TP — true positive, TN — true negative, FP/FN — false results; tested on validation sample
Confidentiality level (1-5)	$S_{privacy} = f\left(ZKP,\ BBS+,\ Data\ Min.\right) \in [1,5]$, where f — expert or normalized rating scale	Expert scale assessing the use of selective disclosure, anonymity, encryption and ZKP
Interoperability (%)	$Interop = \left(\frac{k_{\text{applicable standards}}}{k_{\text{all relevant standards}}}\right) \times 100\%$	For example: support for W3C VC, DidComm, OID4VCI, JSON-LD, BBS+, OIDC, etc.
Offline availability (1-5)	$A_{offline} = f\left(Edge\ AI,\ Credential\ Caching\right) \in [1,5]$	Rated by the number of functions that maintain full or partial performance without access to the network
Time to fully restore access (sec)	$T_{recovery} = t_{restore} - t_{failure}$	Measured as the time from loss of access (e.g. key) to full restoration of access using a backup system (Shamir, Cloud Backup, etc.)

Source: created by the authors

5. RESULTS

According to the research flowchart (Figure 1*: The F*), we will perform the typification of sampling services (Table *1.*) in order to identify the applied modern technologies for the detection and prevention of crimes related to document forgery (Table *3.*).

Table 3. Typification Of Services For Detecting And Preventing Crimes Related To Document Forgery

Applicable technology	Brief description of technologies	Services
Cryptographic signature and digital authentication	Protection of authenticity, immutability and legal validity of the document	DocuSign, Adobe Sign, SignRequest, Notarize, Sign, Validated ID, IDNow AutoIdent
Blockchain registration and smart contracts	Fixing hashes, digital traces, and document data in an immutable distributed registry	Blockcerts, VeriDoc Global, AlphaSign, OriginStamp, KILT Protocol, Vottun, ProofSpace, Verify Certificates, DocuSeal
AI/ML and neural network analysis (anti-falsification)	Detection of fakes, anomalies and manipulations in the content of the document (image, text, structure)	Onfido, Jumio, IDNow, Microsoft Entra Verified ID
Decentralized identifiers (DID) and Self-certification (SSI)	Link a document to DID, verify the authenticity of the owner without centralized databases	Hyperledger Indy, Sovrin, uPort, Trinsic, Civic, Microsoft Entra Verified ID, TrustGrid
Timestamp services and proof of existence of the document	Fix when a document is created in a timeline without revealing its contents	OpenTimestamps, OriginStamp, Vottun Timestamp
Decentralized and content-oriented storage	Secure, unchanging storage of a document addressed through CID (Content Identifier)	IPFS, Filecoin, Web3. Storage, DocChain
Integrated solutions with multi-technology integration	Multi-level verification, Blockchain + AI + DID + Signature	AlphaSign, Blockcerts, Microsoft Entra Verified ID, ProofSpace, Sovrin

Source: created by the authors

Accordingly, 7 types of modern technologies used to detect and prevent document forgery have been identified. At the same time, complex solutions are of greatest scientific interest, accordingly, we will perform a technical-functional comparative analysis of data services (Table *4.*).

Table 4. Technological Comparative Analysis Of Complex Solutions For Detection And Document Forgery Prevention

Service	Blockchain technology	Digital signature	AI/ML component	DID/SSI mechanism	Timestamp/Audit technologies
AlphaSign	Ethereum + Web3.js + QR Anchoring	ECDSA (SHA-256), QR coding	AI QR Analytics + Authenticity Analysis	Partial support (W3C DID standard)	On-chain timestamp + offline logging
Blockcerts	Bitcoin/Ethereum (Plugin Architecture)	Open Badges + JSON signatures	Absent (fixation orientation)	VC + DID via Blockcerts profile	Merkle proofs + blockchain anchoring
Microsoft Entra Verified ID	Azure AD VC (based on DID + JSON-LD)	RSA/edDSA (based on Microsoft AD)	AI-Verification of Document ID (Entra ID)	Full VC + DID support from Microsoft	Ledger-backed time claims
ProofSpace	Ethereum/Polygon (SSI compatible)	Ed25519 + JWT in DID documents	AI anomaly detection module + OCR	Built-in DIF-compatible SSI framework	Timestamp tags in DID objects + IPFS audit
Sovrin	Hyperledger Indy (DLT permissioned)	CL-Schemes (Zero-Knowledge proofs, ZKP)	No built-in ML compatible with outside. modules	Full-featured SSI network with DID based on Indy	Audit log via verifiable claims in Tails file

Source: created by the authors

Drawing on the comparative analysis of technical and functional attributes (Table 4), it was ascertained that among the evaluated integrated solutions, Microsoft Entra Verified ID is the most effective. Notably, this solution offers a comprehensive integration of blockchain fixation (Azure AD VC, DID, JSON-LD), cryptographic signatures (RSA/EDDSA), artificial intelligence (AI-Verification of ID-documents), a robust system for verifiable attribute statistics (VC), and audit-tracing mechanisms grounded in ledger records. In contrast to AlphaSign, Blockcerts, ProofSpace, and Sovrin, this solution exhibits superior functionality, scalability, interoperability, and compliance to international standards within the field of digital document protection.

We undertook an exhaustive technical and architectural analysis of Microsoft Entra Verified ID

to elucidate technological solutions aimed at the identification and prevention of document forgery(
Table *5.*).

Table 5. Technical And Architectural Analysis Of Microsoft Entra Verified ID

Architectural level	Functional purpose	Key technologies
1. Identifier Layer	Generation of Decentralized identifiers (DIDs) for individuals, organizations, or devices; Formation of DID documents	W3C DID Core v1.0, ION Network (Bitcoin anchoring), DID:WEB, DID:ION, Public Key Infrastructure (PKI)
2. Verifiable Credentials Layer	Creation and management of verifiable certificates in JSON-LD format with cryptographic signature and metadata	W3C Verifiable Credentials, JSON-LD, Ed25519Signature2020, RSASignature2018, Linked Data Proofs
3. AI/ML Verification Layer	Automated verification of identification documents, detection of fakes using neural network models	Azure Cognitive Services, OCR, Liveness Detection, Face Matching, Convolutional Neural Networks (CNN), Transformer-based Models
4. Credential Flow Layer	Orchestration of VC issuance and verification between ecosystem participants (issuer → holder → verifier)	DidComm v2, VC Presentation Exchange, Verified ID SDK, JSON Web Tokens (JWT), API Gateway
5. Anchoring Layer	Invariably anchoring DID in a distributed network; providing a timestamp without data disclosure	ION (Layer 2 on Bitcoin), Sidetree Protocol, Merkle Trees, IPFS (optional for content)
6. Policy & Audit Layer	Manage audit conditions, track access to data, record events in audit logs	Azure Active Directory Conditional Access, Zero Trust Policy Enforcement, Revocation Registry, Time Claim Ledger
7. Wallet & UX LayerSSI	Interactive user interaction with the platform via mobile or desktop wallet	Microsoft Authenticator, QR Code, Deep Link DID URI, Mobile Wallet SDK, Verifiable Credential Presentation

Source: created by the authors

Hence, the architecture of Microsoft Entra Verified ID (Table 5) implements a decentralized SSI infrastructure predicated on W3C Decentralized Identifiers (DIDs), Verifiable Credentials (JSON-LD), ION (a Layer 2 solution built atop Bitcoin), and the Sidetree Protocol. This framework ensures immutability, cryptographic authenticity, and the anchoring of DIDs. Certificates are endorsed using Ed25519Signature2020 or RSasigNature2018, transmitted via DidComm v2 with JWT serialization, while access policies are implemented through Zero Trust Conditional Access. The artificial intelligence and machine learning module leverages Azure Cognitive Services for Optical Character Recognition (OCR), biometric verification, liveness detection, and document forensics utilizing Convolutional Neural Networks (CNN) and Transformers. Timestamp validation is facilitated through Bitcoin transaction metadata, with auditing conducted via event-based verifiable logging. The user interface is realized through the Authenticator Wallet SDK, which supports DID URI routing, QR codes, and the Verifiable Presentation Flow, thereby ensuring comprehensive compatibility with W3C Verifiable Credentials, ISO/IEC 18013-5, eIDAS 2.0, and NIST SP 800-63 standards.

The Microsoft Entra Verified ID architecture is highly functional and meets leading SSI standards, but taking into account the latest trends in decentralized identities, artificial intelligence and confidential computing, the following areas of optimization can be identified (
Table *6.*).

Table 6. Optimization Solutions For The Most Effective Detection And Prevention Service Related To Document Forgery

Architectural level	Proposed optimizations	Technologies/approaches
1. DID identification	Expand support for highly scalable DID methods, including did:key, did:pkh, and did:jwk for easier integrations and better mobile compatibility	did:key, did:pkh, did:jwk, BBS+ keys
2. Certification (VC)	Implement BBS+ Signature Scheme to support selective disclosure and ZKP when verifying credentials without full disclosure	BBS+ Signatures, JSON Web Proof (JWP), ZK-VC
3. AI/ML verification	Integrate Federated Learning and Edge AI to authenticate documents offline on a user's device, reducing cloud dependency	ONNX Runtime, Federated Learning, TensorFlow Lite
4. Credential flow	Add DID Authentication support via OpenID4VCI and OpenID4VP for unified identification and interaction with wallets	OpenID for Verifiable Credential Issuance (OID4VCI), OpenID for Verifiable Presentation

5. Ledger fixation	Expand support for alternative DLT platforms (e.g. Ethereum L2, Polygon ID, zkRollups) with lower costs and faster finalization	zKevM, Polygon ID, Optimism, Arbitrum, ZK-Rollup
6. Access policies and auditing	Integrate policy-based selective access mechanisms using Attribute-Based Encryption (ABE) or Multi-Authority ABE to encrypt certificate content	CP-ABE, MA-ABE, Confidential Audit Logs
7. Wallets & UX	Add support for didactic UX mode for unskilled users, as well as the ability to cloud backup keys with secret distribution	UX Progressive Disclosure, Shamir Secret Sharing, Cloud Encrypted Backup SDK

Source: created by the authors

Optimizing the Microsoft Entra Verified ID (
Table *6.*) architecture will reduce latency and reliance on centralized resources by implementing Edge AI and Federated Learning for on-premises data verification. The use of BBS+ signatures and Zero-Knowledge Proofs will provide flexible selective disclosure of information while maintaining confidentiality. Connecting to alternative DLT platforms (e.g. zKevM, Polygon ID) will increase interoperability and reduce transaction costs. Additionally, UX improvements through progressive feature disclosure and key backups (e.g. through Shamir Secret Sharing) will increase the accessibility and reliability of user interaction.

In order to prove the feasibility of the proposed solutions, we will perform a comparative analysis of the calculation of performance metrics
*Table 2*for Microsoft Entra Verified ID and optimized architecture (
Table *6.*).

Table 7. Comparative Analysis Of Performance Metrics Calculation (

Table 2: Performance Metrics Of The Services Related To Document Forgery Detection And Prevention

Table 2) For Microsoft Entra Verified ID And Optimized Architecture (

Table 6.).

Performance Metrics (etc.)	Microsoft Entra Verified ID (basic architecture, practical values)	Optimized architecture (expected simulated values)
Average verification latency (ms)	380,0	210,0
Average anchoring time (s)	12,5	4,8
Consumption of cloud resources (calculation,%)	100,0	43,0
Falsification detection accuracy (%)	94,3	96,8
Confidentiality level (score 1–5)	3,0	5,0
Interoperability with other DID/VC systems (%)	72,0	91,0
Availability of offline use (score 1–5)	2,0	4,0
Time to fully restore access (sec)	180,0	35,0

Source: created by the authors

The results of the comparative analysis (Table 7.) empirically prove the superiority of the optimized architecture over the basic Microsoft Entra Verified ID model in all key technical and performance indicators. The integration of optimization solutions – such as support for scalable DID methods, BBS+ signatures, Zero-Knowledge Proofs, Edge AI, federated learning, multi-platform lagers, and attributive encryption – provided comprehensive enhancements in system performance.

Against this backdrop, the average verification latency in particular was reduced by 44.7 percent, the anchoring time by 61.6 percent, and the consumption of cloud computing resources by 57 percent. Nevertheless, the detection accuracy of forgeries increased by 2.5 percent, the level of confidentiality – by 66.7 percent, and the interoperability – by 26.4 percent. Notably, the availability of offline functionality doubled, and the time for full restoration of access is reduced by more than 5 times.

In sum, the aforementioned substantiates the effectiveness of the proposed multi-level optimization of the SSI architecture as a technological paradigm that enhances resilience against fraud, reducing the burden on the infrastructure, and expands the service's functional applicability for real-time scenarios and environments with limited network access.

5. DISCUSSION

We will evaluate the adequacy of the results obtained in relation to those reported in analogous publications.

In particular, Bae et al. [20] demonstrate that the efficacy of detecting fraud is contingent upon the models' linguistic adaptability, whereas the current study substantiates the advantages of a universal SSI architecture predicated on BBS+, ZKP, and Edge AI. This attests to the feasibility of protocol-level scalability as an alternative to language-specific model training.

Nogueira et al. [21] systematically categorize hybrid methodologies for detecting draud through the analysis of visual artifacts and semantic features. The present study, however, prioritizes the architectural integration of BBS+, ZKP, and Edge AI as means of cryptographic verification with minimal computing costs.

Zhang et al. [22] categorize methodologies for detecting digital identity forgery, particularly focusing on forgeries generated by deepfake technology, thereby illuminating key limitations of existing artificial intelligence solutions. In contrast, the current study implemented an architecturally integrated SSI model, utilizing cryptographic protocols and Edge AI as a technically sophisticated alternative for zero tolerance towards forgery, even at the stage of creating digital certificates.

Chaudhari and Charate [23] employ generative models and LayoutLM in conjunction with Explainable Artificial Intelligence (XAI) to identify financial discrepancies within synthetic datasets. Instead, the present study implemented an SSI architecture incorporating BBS+, Zero-Knowledge Proofs (ZKP), and anchoring mechanisms as a preventive mechanism for blocking ex ante falsifications, eliminating the need for post-factum classification.

Thanh Le [24] elucidates the efficacy of the SNN model in discerning handwritten signatures on Certificates of Origin, surpassing conventional CNN and ML algorithms across all accuracy metrics. The current study, instead, concentrates on preventing fraud even prior to the signature verification phase by employing cryptographic attestation through BBS+ and ZKP within a decentralized SSI architecture.

Gaikwad and Mizwan [25] examine the effectiveness of VGG19, EfficientNet-B2, and ELA-CNN in detecting faked images, achieving a classification accuracy of 72% on the CASIA 2.0

dataset. This research prioritizes an architecturally integrated methodology based on BBS+, ZKP, and SSI mechanisms, which mitigate the potential for falsifications even before the image identification stage.

Boonkrong [26] substantiates the feasibility of employing hash functions to detect alterations in electronic academic manuscripts, demonstrating 100% accuracy and exceptionally low verification latency (0.352 ms). It is worth noting that in the present study, the emphasis has shifted from post-factum verification to preventive measures against architectural counterfeiting through the implementation of BBS+ signatures, zero-knowledge proofs, and self-sovereign identity architecture featuring invariant anchoring registration.

Asyraf et al. [27] delve into the legitimacy and vulnerabilities of e-stamp duty as an electronic document verification tool, accentuating the risks of fraud that undermine the legal efficacy and trust in digital governance, whereas the present study focuses on technological assurance of legal credibility through SSI architecture, wherein BBS+ Signatures, zero-knowledge proofs, and distributed ledger technology (DLT) network anchoring guarantee the invariance and inadmissibility of document forgery.

Hao and Zheng [28] elucidate the efficacy of the DEIT model in detecting AI-generated forged signatures, achieving an the accuracy over 98% and an AUC reaching up to 100%. In contrast, the present study employs a cryptographic-deterministic SSI methodology, wherein BBS+ Signatures and ZKP render the creation of forgeries utterly impossible, regardless of their source of generation.

Luo et al. [29] introduce an RTM dataset alongside a model characterized by multi-modal fusion and contrastive training, aimed at enhancing the detection accuracy of realistic text forgeries within images. On the other hand, the current study advocates the architectural inadmissibility of text forgery by seamlessly integrating BBS+ Signatures, ZKP, and DID anchoring even at the stage of forming a verified digital document.

A comprehensive analysis of relevant publications confirms the dominance of post-factum falsification detection methods drawing upon the examination of linguistic, visual, structural, or semantic anomalies utilizing AI/ML, transformers, XAI, or HSI. On the other hand, the architecture proposed in the present study draws upon ex ante protocol-level forgery by way of using BBS+ Signatures, Zero-Knowledge Proofs, a decentralized anchoring system, cryptographic DIDs, as well as attributive encryption. This approach ensures cryptographically verified immutability, a high level of interoperability and offline accessibility, thereby establishing the technological foundation for the automated validation of electronic notarial acts with an increased level of legal reliability.

5.1. Limitations

A limitation of the current study is that the values of key performance metrics (latency, anchoring time, cloud load, etc.) are obtained by modeling rather than verified empirically in a real environment. Additionally, the impact of distributed load, attacks by ecosystem participants, and performance variability depending on device type and DID method were not taken into account.

5.2. Recommendations

It is recommended to develop a pilot prototype of SSI architecture with integration of BBS+, ZKP and Edge AI for empirical verification of key performance metrics under real load conditions. It is also advisable to test the scalability of the solution on heterogeneous devices and in conditions of variable network access.

6. CONCLUSIONS

Summing up, as a result of the typification as well as a comprehensive technical and architectural analysis of 33 state-of-the-art services and 7 classes of technology, it was found that complex SSI solutions featuring multi-level integration of blockchain fixation, cryptographic signatures, AI/ML components, decentralized identity identification (DID), and auditing exhibit the highest degree of functional completeness. Among these, the Microsoft Entra Verified ID architecture proved to be the most effective. Following the implementation of the proposed optimizations (BBS+, ZKP, Edge AI, ZKRollup, ABE), it demonstrates a 44.7% reduction in average verification latency, a 61.6% decrease in anchoring time, a 57% reduction in cloud computing consumption, and a 2.5% enhancement in detection accuracy in terms of forgery. Hence, this substantiates the feasibility of moving to fraud resilient protocol-level architectures, which is critical for digital notarization mechanisms and ensuring the immutability of electronic acts with a high level of legal verification.

Scientific novelty. An optimized SSI architecture with BBS+ signatures, ZKP, Edge AI and multi-platform anchoring is offered, providing cryptographic stability and reducing dependence on the cloud while maintaining interoperability.

Practical value. The optimized solution reduces latency by 44.7%, cloud consumption by 57%, increases accuracy and confidentiality, making it suitable for scalable implementation in digital document verification systems.

REFERENCES:

[1] T. Voloshanivska, R. Shchokin, O. Pavlova, A. Y. Frantsuz, and M. O. Dei. "Reforming global criminal justice: Addressing corruption's impact on armed crime", *Journal of Law and Legal Reform*, Vol. 5, No. 3, 2024, pp. 1369-1404. doi: 10.15294/jllr.v5i3.4082.

[2] D. Dubey, R. Rohatgi, and S. R. Pathak. "Unveiling digital document manipulation: A case study in forensic examination", *Indian Journal of Forensic Medicine & Toxicology*, Vol. 18, No. 2, 2024, pp. 46-52. doi: 10.37506/w909cd74.

[3] V. Krykun, R. Shchokin, A. Kyryliuk, L. Halupova, and V. Grygoryeva. "The role of artificial intelligence in ensuring the efficiency and accessibility of justice", *Revista Brasileira De Alternative Dispute Resolution*, Vol. 06, No. 12, 2024. doi: 10.52028/rbadr.v6.i12.art13.ukr.

[4] R. Bharati, D. Jaiswal, P. Jadhav, P. Patil, S. Joshi, V. Lashkare, H. Patil, and P. Ahire. "Document generation and validation using blockchain", *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE (India), August 23-24, 2024, pp. 1-5. doi: 10.1109/iccubea61740.2024.10774827.

[5] Z. Peng, T. Wang, C. Zhao, G. Liao, Z. Lin, Y. Liu, B. Cao, L. Shi, Q. Yang, and S. Zhang. "A survey of zero-knowledge proof based verifiable machine learning", *arXiv preprint arXiv:2502.18535*, 2025. doi: 10.48550/arXiv.2502.18535.

[6] A. Diarra, T. F. Bissyande, and P. Poda. "Doc-Patch: An unsupervised approach for documents forgery detection", *2024 7th International Conference on Algorithms, Computing and Artificial Intelligence (ACAI)*. IEEE (China), December 20-22, 2024, pp. 1-7. doi: 10.1109/acai63924.2024.10899704.

[7] T. S. Fun, N. S. B. Ahmad Zulkifli, F. Sia, and L. P. Hung. "Enhancing electronic document security with lightweight digital signature", *2024 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET).* IEEE (Malaysia), August 26-28, 2024, pp. 591-596. doi: 10.1109/iicaiet62352.2024.10730678.

[8] P. Kunekar, R. Chandawar, A. Borade, P. Davare, A. Chalpe, and E. Dasarwar. "Optimizing cryptographic and image hashing for document verification", *SSRN Electronic Journal*, 2025, art. 5112131. doi: 10.2139/ssrn.5112131.

[9] S. K. Radha, A. Kuehlkamp, and J. Nabrzyski. "The future of document verification: leveraging blockchain and self-sovereign identity for enhanced security and transparency", *arXiv preprint*, 2024, pp. 107-122. doi: 10.5121/csit.2024.141910.

[10] E. Broshka, and H. Jahankhani. "Evaluating the importance of ssi-blockchain digital identity framework for cross-border healthcare patient record management", in: *Advanced sciences and technologies for security applications*. Cham: Springer Nature Switzerland, 2024, pp. 87-110. doi: 10.1007/978-3-031-72821-1_5.

[11] R. Sukhija, M. Kumar, and M. K. Jindal. "Document forgery detection: A comprehensive review", *International Journal of Data Science and Analytics,* 2025. doi: 10.1007/s41060-025-00723-0.

[12] L. Li, Y. Bai, S. Zhang, and M. Emam. "Document forgery detection based on spatial-frequency and multi-scale feature network", *Journal of Visual Communication and Image Representation*, Vol. 107, 2025, art. 104393. doi: 10.1016/j.jvcir.2025.104393

[13] P. B. Karale. "Blockchain-based document verification: A comprehensive review. *International Journal of Advanced Research in Computer Science*, Vol. 16, No. 1, 2025. pp. 31-35. doi: 10.26483/ijarcs.v16i1.7183.

[14] A. Kale, B. Sura, A. Khandare, M. Rupani, and D. Sharma. "Blockchain-based patient document storage and access", in: *Technologies for Energy, Agriculture, and Healthcare*. London: CRC Press, 2024, pp. 176-184. doi: 10.1201/9781003596707-18.

[15] J. Han, and Y. Son. "Design and implementation of a decentralized document management system", *Expert Systems With Applications*, Vol. 262, 2024, art. 125516. doi: 10.1016/j.eswa.2024.125516.

[16] A. Rizky, R. W. Nugroho, W. Sejati, Mumpuni, and O. Sy. "Optimizing blockchain digital signature security in driving innovation and sustainable infrastructure", *Blockchain Frontier Technology*, Vol. 4, No. 2, 2025, pp. 183-192. doi: 10.34306/bfront.v4i2.717.

[17] Y. Song, W. Jiang, X. Chai, Z. Gan, M. Zhou, and L. Chen. “Cross-attention based two-branch networks for document image forgery localization in the Metaverse”, *ACM Transactions on Multimedia Computing, Communications, and Applications*, Vol. 21, No. 2, 2024, art. 55. doi: 10.1145/3686158.

[18] U. Mirzanli, P. Guzel, and N. Akbay. “Spectroscopic techniques and chemometrics for ink analysis: Document analysis application”, *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, Vol. 326, 2024, art. 125167. doi: 10.1016/j.saa.2024.125167.

[19] Y.-Y. Hao, Y.-C. Wang, G.-L. Zhou, Y.-W. Zhao, J.-Y. Xu, and X.-H. Chen. “Date determination using a combination of raman and video spectroscopy for the examination of forged documents containing pre-inked stamp impressions”, *Forensic Science International*, Vol. 368, 2025, art. 112388. doi: 10.1016/j.forsciint.2025.112388.

[20] Y.-Y. Bae, D.-J. Cho, and K.-H. Jung. “Visual complexity in korean documents: Toward language-specific datasets for deep learning-based forgery detection”, *Applied Sciences*, Vol. 15, No. 8, 2025, art. 4319. doi: 10.3390/app15084319.

[21] D. M. Nogueira, M. Simões, C. Ferreira, R. P. Ribeiro, D. Martínez-Rego, A. Cai, and J. Gama. “Survey on Detection of Fraudulent Documents”, *Authorea Preprints*. *TechRxiv,* 2025. doi: 10.36227/techrxiv.174362941.18385407/v1.

[22] C. J. Zhang, A. Q. Gill, B. Liu, and M. J. Anwar. AI-based identity fraud detection: A systematic review. *arXiv preprint arXiv:2501.09239*, 2025. doi: 10.48550/arXiv.2501.09239.

[23] A. V. Chaudhari, and P. Ashokrao Charate. “Synthetic financial document generation and fraud detection using generative AI and explainable ML”, *Journal of Recent Trends in Computer Science and Engineering*, Vol. 13, No. 2, 2025, pp. 45-59. doi: 10.70589/jrtcse.2025.13.2.6.

[24] L. Thanh Le. “Uncovering import document fraud: Leveraging the deep learning approach”, *Global Trade and Customs Journal*, Vol. 20, No. 1, 2025, pp. 3-10. doi: 10.54648/gtcj2025002.

[25] S. Gaikwad, and Z. Mizwan. “Detection of image forgery using deep learning”, *International Conference on Innovations in Computing and Applications (ICICA-24)*, Vol. 3253, No. 1, 2025, art. 030006. doi: 10.1063/5.0248327.

[26] S. Boonkrong. “Design of an academic document forgery detection system”, *International Journal of Information Technology*, 2024, 1-13. doi: 10.1007/s41870-024-02006-6.

[27] A. M. W. Asyraf, M. Arsy, and Y. A. Hamza. “Legal analysis of the position and impact of misuse of e-stamps in electronic documents: A civil law perspective”, *Advanced Private Legal Insights*, Vol. 1, No. 1, 2025. Available in: https://jurnal.fh.umi.ac.id/index.php/april/article/view/905 (14.05.2025).

[28] Y. Hao, and Z. Zheng. “Research on detecting ai-generated forged handwritten signatures via data-efficient image transformers”, *IEEE Access*, Vol. 13, 2025, pp. 7683-7690. doi: 10.1109/access.2025.3525808.

[29] D. Luo, Y. Liu, R. Yang, X. Liu, J. Zeng, Y. Zhou, and X. Bai. “Toward real text manipulation detection: New dataset and new solution”, *Pattern Recognition*, Vol. 157, 2025, art. 110828. doi: 10.1016/j.patcog.2024.110828.