Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 3, June 2026, pp. 2383~2391
ISSN: 2302-9285, DOI: 10.11591/eei.v15i3.10945

Cybersecurity in property digitisation: a taxonomy and evaluation of current security methods

Anuradha Uppar[1,4], Nagaveni Veerakyatharayappa[2], Parvathi Chikkanna[3]
[1]Department of Computer Science and Engineering, BGS College of Engineering and Technology, affiliated to Visvesvaraya Technological University, Bengaluru, India
[2]Department of Computer Science and Engineering (Data Science), AMC Engineering College, affiliated to Visvesvaraya Technological University, Bengaluru, India
[3]Department of Artificial Intelligence and Data Science, BGS College of Engineering and Technology, affiliated to Visvesvaraya Technological University, Belagavi, India
[4]Department of Computer Science and Engineering, Sambhram Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Jun 30, 2025
Revised Mar 18, 2026
Accepted Apr 1, 2026

Keywords:

Cyberthreats
Document
Land
Real estates
Security

ABSTRACT

The proliferating methods of digitization for documents related to real estate, land, property, and tax, encountered with critical security challenges. Such documents, which have an inclusion of high-value information, such as transaction history, geographic boundaries, tax assessment, and ownership details, are quite prime targets for various types of cyber threats. It is observed that with security domains advancing in faster pace, their implications towards securing such legal documents are questionable, especially in the presence of emerging lethal threats. This manuscript presents a comprehensive and highly compact exhibit of curated information about the effectiveness of all identified security solutions. The presented study has discussed the taxonomy of six mechanisms of securing property-related digitized document. It was found that although the impersonation attacks and forgery can be addressed with multifactor authentication, digital signatures and blockchain, they are not reportedly found to be mitigating modern-day threats like social engineering, and insider collusion. The outcome of this study infers that hybrid approaches fusing with zero-trust models, anomaly detection, and artificial intelligence (AI) demands more resilient security system. The paper contributes towards some novel findings of widely deployed security solutions, research trends, and gaps which will offer definitive guidelines towards designing a novel solution.

Corresponding Author:

Anuradha Uppar
Department of Computer Science and Engineering, Sambhram Institute of Technology
MS Palya, Jalahalli East, Vidyaranyapura, Bengaluru-560075, Karnataka, India
Email: anu.charana@gmail.com

1. INTRODUCTION

Conventionally, a real-estate, tax, property, or land document is a type of information that consists of legally binding context, such as regulatory approval, tax assessment, transaction history, geographic boundaries, and ownership details. This document essentially serves as official evidence towards compliance with administrative, financial, and legal purposes and evidence of valuation and ownership. On a large scale, all these documents are in the form of paper (hard copies), which is now witnessing a wave of digitisation. There are significant challenges associated with security towards the digitisation of tax documents, property, and land-related legal documents. Conventional storage and verification methods are progressively becoming less useful with the increasing landscape of threats. Therefore, securing such types of digitised documents is

essential owing to the long-term influence of such records, legal significance, and high value [1]. During cyberthreats, it may result in property-related fraudulent activities, viz., tax evasion, duplicate sales, and title forgery, by manipulating the records. There are various reported forms of attacks already reported towards various types of documents [2]-[4]. The victim may instantly lose ownership of their highly valuable assets, suffer reputational damage or encounter prolonged legal disputes. If there are any successful attempts of unauthorised access, it will lead to significant financial loss to the owner, illegal encroachment of land, and transfer of fraudulent property. On a bigger scenario, such a form of malicious event could also weaken the trust of the public in the systems developed by the government itself, while it could enable corruption and disrupt both the local and global market of real estate. It is also noted that the unavailability of verifiable and secure documents could eventually hinder the development of infrastructure, while it can adversely influence the national growth of the economy by delaying the initiative of urban planning. It will also lead to social displacement and unrest if such threats persist for the nation. The real reasons for such threats could originate from system weakness, human factors, and technological vulnerabilities. The existing system is found to be highly dependent on centralized server, which leads to a single point of attack by cyberthreats very easily. The existing credential management system offers weaker authentication as well as access control methods that further create a security breach by unauthorised users. Different types of loopholes, exploitation, duplication, and errors also arise from degraded interoperability between inconsistent standards of data and government agencies. Such problems are now identified by the research community and addressed using widely-adopted security solutions, which is combination of monitoring methods, access control systems, and cryptographic tools [5]. Usage of attribute-based access control (ABAC), role-based access control (RBAC), public key infrastructure (PKI), and digital signatures are some widely adopted approaches towards authentication and content verification for rightfully proving the ownership of a digitised document. Apart from this, a detailed record of every activity towards the document is performed using a logging system and audit trails that offer post-incident investigation, accountability, and transparency. Some security solutions are used as a standalone way, while some are used in integration with others to offer more customised security features. However, with evolving types of cyber threats, it is quite clear that the effectiveness of all these widely adopted security solutions is questionable.

Various related work has been studied to understand the existing flow of implementation towards securing digitised documents. The work of Saadi *et al.* [6] has discussed about various protective methods towards resisting security vulnerabilities mainly associated with graphical password protection. As most of the digitised documents are expected to migrate on cloud system, the work presented by Arif *et al.* [7] offers a discussion of various types of trust-based and privacy-preserving methods for securing such digitised contents from cyberthreats. Zabukovšek *et al.* [8] have presented a discussion towards document management system that can be improved using a maturity model with respect to its life cycle. Ege *et al.* [9] have presented a discussion towards usage of digital signatures for document security, where the authors have discussed about electronic and token signatures for document signing. The study shows a better scope of the token signature. Ahmed *et al.* [10] have used encryption based method towards resisting forgery attacks on important documents, where the ciphering is carried out considering a hologram generated from a computer. Adoption of a fractal grid towards securing printed documents has been presented by Nazarkevych *et al.* [11]. Further, the work of Lu *et al.* [12] has presented a model that is capable of identifying malicious documents.

After reviewing the above-stated related work, various research problems have been identified as follows: i) conventional methods of digital storage for documents doesn't offer an assured tamper-proof data integrity which is mainly due to inedequet methods for records immutability, ii) majority of systems associated with tax, real-estates, and land purchasing/selling, are highly centralized that leads to insider threats, single point failure, and inferior resistivity against cyberattacks, iii) available of massive number of sophisticated tool allows counterfeiting of digitized content while wider usage of digital signature and watermarking is actually outdated, iv) document digitization will demand usage of multiple system from different region which may be incompatible system increasing challenges in cross-verifying transactions, taxes, and ownership, v) there are higher chances of manipulation and unauthorized viewinh in current system of access control of digitalized documents, and vi) it is almost impossible for any normal users (which could be any legal bodies or citizen) to verify any history of alterations or any form of access events to the digital content. Most importantly, there is no review study presented towards understanding the effectiveness of various security methods towards protecting such a specific form of digitised documents of property.

Therefore, the aim of the proposed study is present a comprehensive, yet compact, and updated insights of various security approaches and their effectiveness towards protecting digitised documents related to land/property, irrespective of any geographical region. The value-added contribution of this study are as follows: i) the study presents a taxonomy of current security solutions that has never been presented before in line of document security methods towards property management, ii) the study also presents key strength of

each models along with a critical insight towards the attack which they can stop as well as attacks that they cannot stop, iii) an updated and exclusive research trend has been studied with respect to number of publications towards various addressed problems, types of digitized contents, and different security methods to offer a birdview insight on current state of publications, and iv) finally, the paper presents research gap stating the underpresented problems that has not yet received significant attention. The organisation of the paper is as follows: section 2 presents the adopted research methods, while the accomplished results are discussed in section 3, and the conclusion is presented in section 4.

2. METHOD

The proposed system adopts preferred reporting items for systematic reviews and meta-analyses (PRISMA) methodology in order to carry out structured analysis of existing security methods, as shown in Figure 1. A specific set of keywords has been considered towards the search strategies for facilitating reproducibility and transparency. These keywords are 'access control real estate document', 'blockchain lang registry', 'land ownership+cybersecurity', 'property digitisation', and 'document security'. All the records are checked for any form of duplicates, followed by filtering out the duplicates. The second stage is about screening the duplicate-removed records with respect to title and abstract. This stage is then further extended to review the complete text, especially on the research methodology, algorithm, and result sections of each paper, to arrive at a final set of documents. The final documents must comply with the inclusion and exclusion criteria that are complied with on each step. The inclusion criteria formulated are to choose journal articles that were published in the year 2020 till current year of 2025. They should also have been published in Q1/Q2 research journals that are indexed by Web of Science or Scopus, and should have written in English. The papers should have a complete discussion of methodology as well as results. The exclusion criteria are any articles that do not have empirical validation, non-English articles, incomplete studies, and conference papers. The proposed review work is restricted to Q1/Q2 to ensure rigorous, peer-reviewed and enriched quality investigation. Although a slight bias can be introduced by this criterion due to the non-inclusion of other forms of journals.

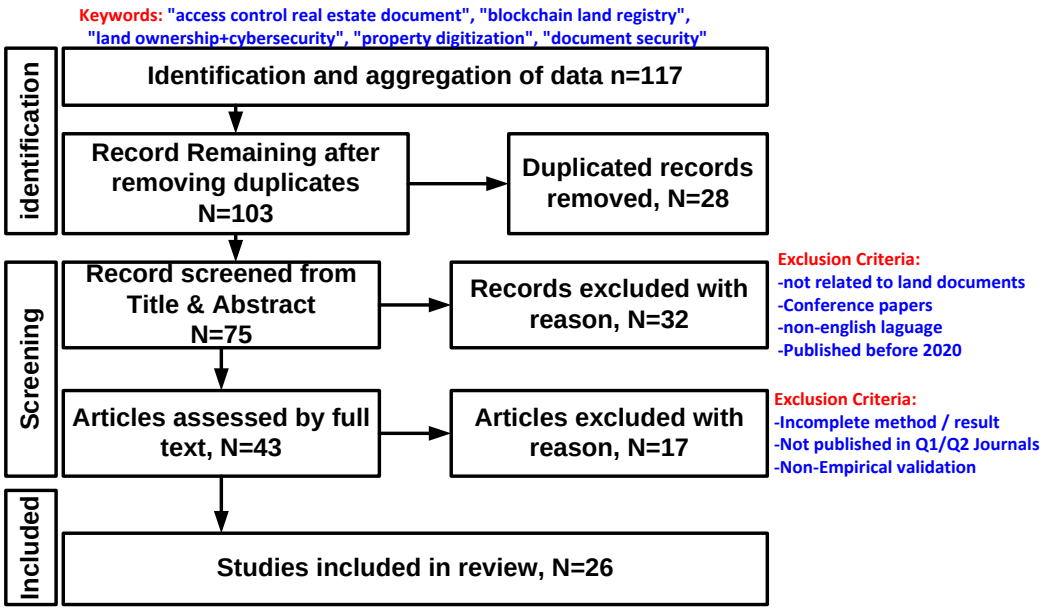

Figure 1. PRISMA method adopted

3. RESULTS AND DISCUSSION

After reviewing manifold research articles, it was noted that vulnerabilities exist within current literature, irrespective of increased awareness towards document digitisation and cybersecurity. The proposed review work contributes towards closing such a knowledge gap by evaluating current security methods towards document digitisation. The findings could eventually confirm that there is no standalone approach to address all evolving attack vectors. Adoption of research methodology in the prior section has assisted to witnessed increasing number of research works towards existing security methods. However, irrespective of

maximised proliferation of digitisation, existing methods have remained insufficient towards addressing emerging cyber threats. The majority of the existing system has higher dependencies on conventional access control methods or centralised databases that are found vulnerable to cyber threats, unauthorised modifications, and insider threats. The most commonly adopted watermaking and digital signatures often address issues about document authenticity, and still, none of the existing techniques is found to be robust against complicated forgery attacks. Apart from this, there is a weaker version of audit trails as well as restricted transparency that not only jeopardises accountability but also hinders the trust associated with document management. Lack of interoperability over jurisdictions and inadequate standardisation further degrade the cross-verification system as well as secure information exchanges. Hence, there is a potential need for privacy-aware computation, tamper-resistant, advanved solution such as secure multi-party computation, zero-knowledge proofs, and blockchain for offering an assurance of resiliency, confidentiality and integrity. Interestingly, artificial intelligence (AI), being such a dominant solution for security problem is yet to establish its stronger hold in this domain of problems, in contrast to other conventional security solutions.

3.1. Identified taxonomy of security solution

There is various research work being carried out towards securing digitised land records, related financial documents, and real estate documents. However, it is quite a challenging task to categorise them. Hence, this section presents the discussion of an identified taxonomy of existing security solutions on the basis of purpose, technological domain, and function. Figure 2 highlights the identified taxonomy, which states that there are 6 types of current solution exercised. The first type is known as a data integrity and tamper prevention technique that offers a solution via smart contract [13], watermarking and digital signature [14], and an immutable storage solution using blockchain [15]. The second type is known as an authentication and access control technique, which mainly emphasises identity verification [16] and an access system [17]. The third essential category is cybersecurity infrastructure that uses intrusion detection/prevention systems [18], cloud security [19], and data encryption [20]. Further there are various conventional schemes e.g.; i) spatial and boundary verification which mainly uses geographic information systems (GIS) based land information [21] and remote sensing/drones [22], ii) surveillance, monitoring, and forensics that basically uses audit trails [23] and security information towards threat management [24], and iii) document digitization and management which performs secure digitization [25] and enterprise content management [26].

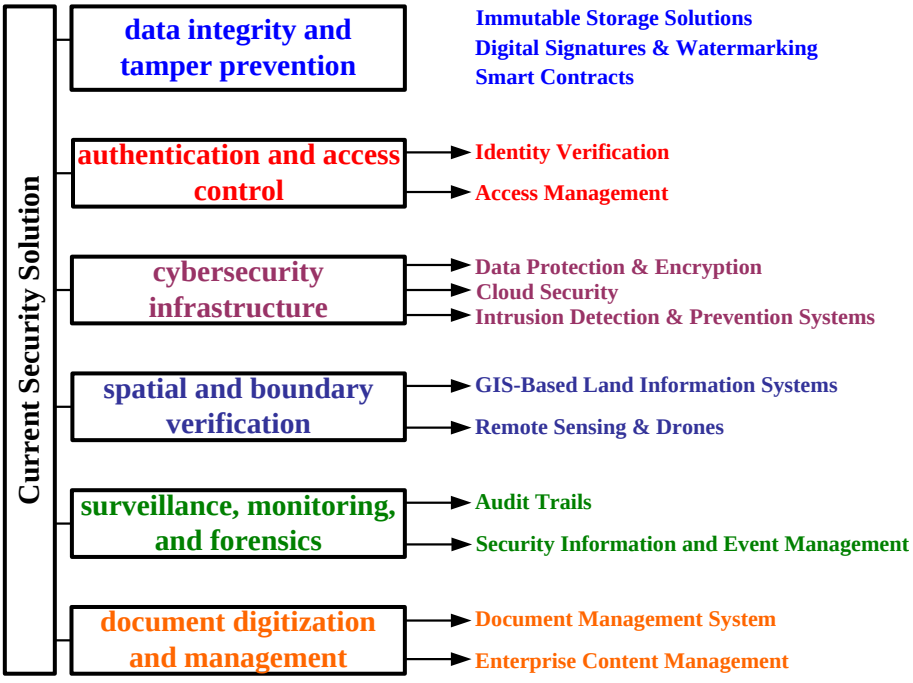

Figure 2. Taxonomy of current security solution

3.2. Insight towards effectiveness of the existing solution

There is no denying the fact that existing security solutions have made their best attempts, with an increasing number of research works dealing with different types of fraudulent activities. Table 1 highlights the effectiveness of the current solution, which eventually shows that there are specific methods that address all the threat types. There are fewer studies considering a layered defence system where multiple methods are combined. It can be noted that although access control has strengthened over a period of time, misuse and theft of such essential documents are still a bigger concern. Although ownership disputes have been significantly controlled by current solutions, it doesn't prevent any form of fraudulent activities. The evolving forms of attacks, e.g., legal loopholes, insider collusion, and social engineering, are quite difficult to resist by the majority of existing solutions. In short, the current form of security solutions is found to be quite productive towards resisting impersonation attacks, document forgery, and tampering. However, they are witnessed with sub-optimal performance towards resisting modern forms of all evolving threats.

Table 1. Effectiveness of current security methods

Current methods	Key strength	Controlled threats	Uncontrolled threats
Blockchain	Tamper proofed	Document forgery	Frauds by corrupt officials
Digital signatures	Tamper detection	Impersonation attack and unauthorized document editing	Social engineering and private key theft
Smart contract	Eliminates intermediaries enforced automatically	Counterfeited sales and payment-related frauds	Error in contract code
RBAC	Segregation of duties	Internal threats, unauthorized access to the system	Collusion attack and credential theft/sharing
Biometric authentication	Non-transferable assurance of identity management	Impersonation attack	Biometric spoofing
Multifactor authentication, e-KYC	Controls online fraud, user-verification on multiple layers	Remote fraud attempts and counterfeited user accounts	SIM swapping and social engineering
Document management system	Audit trails, access control, and secure digitization	Theft/loss of physical document	Ransomware and data corruption
Encrypted cloud storage	Disaster recovery and secure access	Remote data breaches	Insider misuse of cloud permission
Audit logging	Forensic study and real-time monitoring	Stealthy data access	Zero-day exploits
GIS mapping	Land grab/encroachment detection and precise spatial data	Boundary disputes	Fraudulent in legal ownership and errors in the base data of the survey
Title insurance	Financial protection from any title defects	Historical record gaps and disputes of ownership	Only address financial loss and doesn't resist frauds
Immutable backup	Secure archiving	Fraudulent claims	Manipulation of the legal system

In order to facilitate the deeper quantitative findings, various research articles have been reviewed to find their degree of adoption. There are 35% of research papers using blockchain model, while 22% of research articles use digital signatures, and 14% has used audit trail mechanism. Biometric system adoption has been noted to be 12% in current research. The most significant findings suggest that there are only 6% of studies that have used biometric authentication combined with blockchain methods. This trend of adoption frequency recommends that there are various effective strategies of layered defences that still remain underutilised. It was seen that blockchain methods significantly minimised malicious events of forgeries by 48% recorded in national level of land registries. Apart from this, impersonation attacks have been minimised by 38% upon the adoption of multifactor authentication. These learning outcomes exhibit the demands for more extensive validation towards an integrated framework supporting real-world implementation.

3.3. Current research trend

The outcome of the current research trend is showcased in Figure 3 with following inference: i) number of publications has drastically dropped down since 2022 (n=36) as noted from Figure 3(a) while IEEE, Springer, and Elsevier has remained the preferred choice of publication in contrast to others, ii) problems towards data integrity (n=42) has received extensive attention while blockchain based biometric verification is least one to find (n=10) as noted from Figure 3(b), iii) more emphasis is given to secure title deed type of documents (n=50) while land-use document security has not recived much attention (n=6) as noted from Figure 3(c), and iv) standalone blockchain methods have increasingly found more publications (n=60) while AI-based methods has yet to gain a pace (n=5) as noted from Figure 3(d).

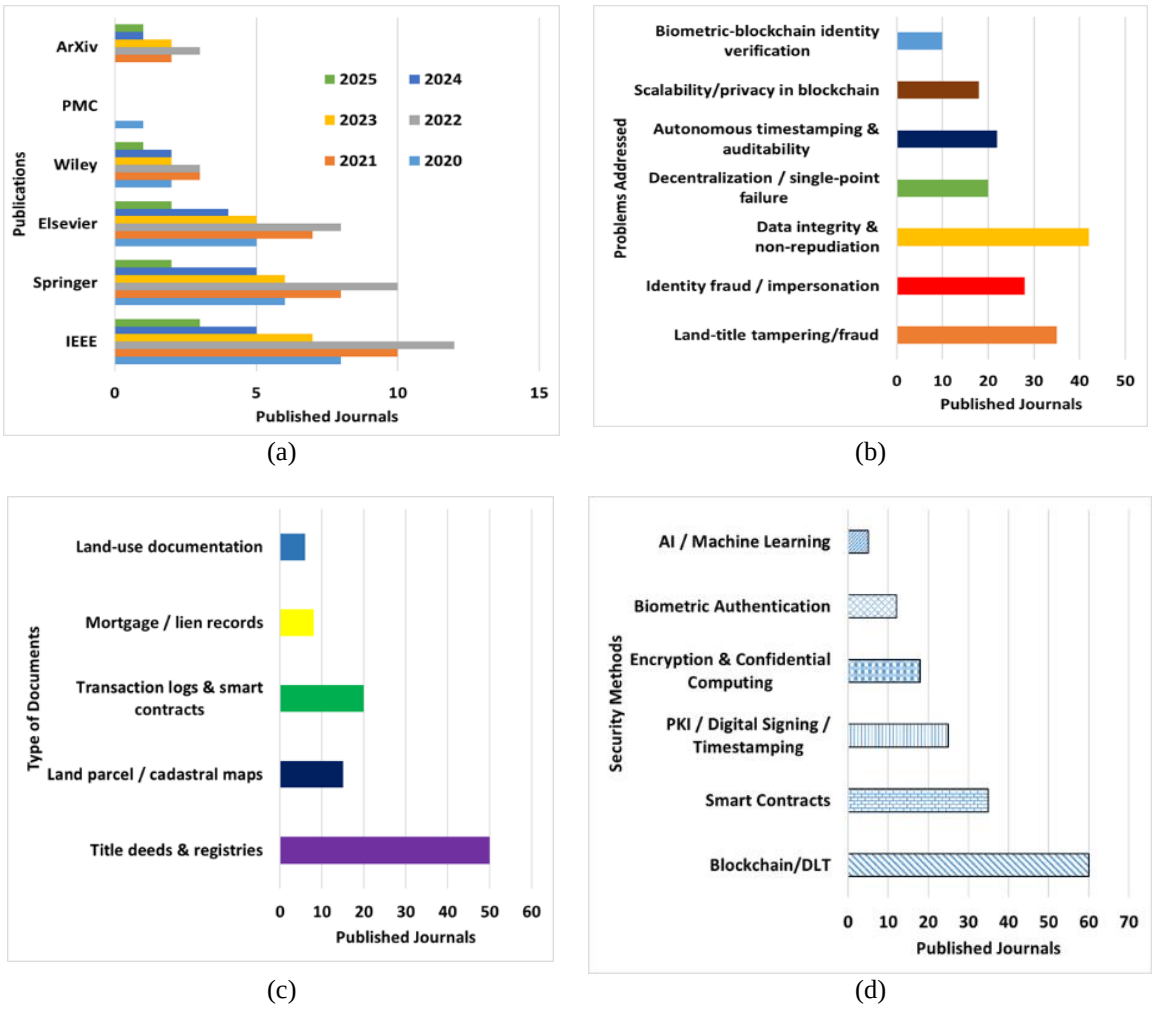

Figure 3. Visuals of identified research trend; (a) year-wise publication trend from 2020–2025, showing a declining pattern post-2022, (b) security problems addressed by existing literature, with data integrity leading the count, (c) types of digitized property documents studied, highlighting preference for title deed security, and (d) distribution of security methods adopted, with blockchain dominating over AI-based approaches

3.4. Critical research gap

The current investigation has explored that there are various approaches, e.g., digital authentication, PKI, and blockchain, that have received enough attention from academics. However, certain problems remain largely unaddressed. Figure 4 shows the core research gaps that demand more attention. There has been significant underutilization of an AI that is an emerging method towards detection fradulent effort in real-time. There is a lack of an effective and fine-grained security framework, considering a hybrid version of record that uses both digitised content and a hardcopy of the document. Such a type of model will facilitate offline validation of the paper deed, too, which is lacking at current times. Existing studies has inadequete emphasis on role-based abuse as well as insider threat, even when there is much work towards access control. There are lack of approaches, e.g., anomaly detection, zero-trust framework, and behavioural biometrics. Existing work has been carried out assuming a secure digital infrastructure with high bandwidth; however, they are not secure, offline compatible systems for land documentation where there is no internet. Problems associated with interoperability of the tax system, financial, legal, and land have witnessed no significant solutions for developing an end-to-end secured ecosystem. The existing studies towards multi-party ownership don't pay any attention towards dynamic controls, e.g., secured access to shared documents, consent mechanisms, or fine-grained privacy controls. Finally, there is a forensic auditing tool for generating evidence that can be considered admissible for audit trails. Although blockchain is immutable, it still lacks tamper-proof forensic recordings, metadata preservation, and court-ready evidence formatting.

There are particular scope towards innovation facilitated by each identified research gap. For example, the issues related to AI underutilization can be addressed in future by investigating anomaly-based detection using machine learning (ML) that are trained adopting behavioural cues and access logs. From the perspective of the hybrid framework, the offline validation can be improved by securing digitized document supporting QR-oriented document references. Adoption of zero-trust architecture along with a decentralised identity system is noted for mitigating role-based abuses. Further, interoperability can be addressed by developing cross-domain metadata and an open standard API towards legal dataset, tax, and property-related records, adhering to the guidelines of ISO/IEC 27037.

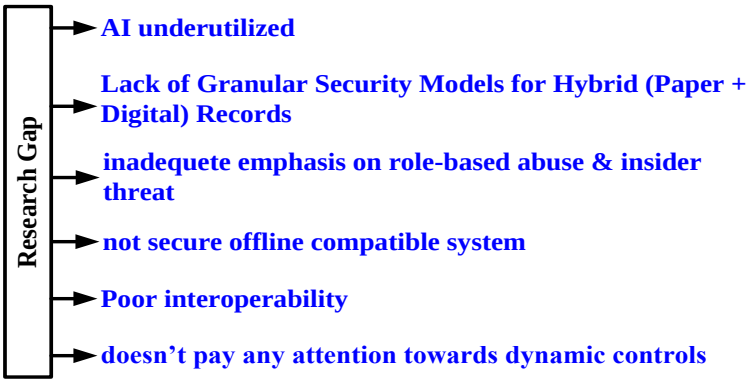

Figure 4. Critical research gap

3.5. Real-world deployment example

Before understanding the possible applicability of real-world deployment, it is necessary to realise certain practical world examples. A blockchain-based land registry system has been implemented in the Republic of Georgia in collaboration with the National Agency of Public Registry (NAPR) and bitfury. Such productive and innovative attempts facilitate immutability and digitisation of land titles minimizing possible fraud and enhancing 50% of transactions. Although such novel ideas have started as a pilot project in India, it doesn't run in a full-fledged manner. In order to deploy in the real world, there is a need for offline verification methods that are quite effective with low resources. It is best suited within the resources of smart cities, where multiple devices and services exist for further leveraging the security of land registries.

4. CONCLUSION

The proposed study facilitates discussion of evaluation towards a security mechanism and a comprehensive taxonomy for securing digitised land registry documents. Prime insights of the review work involves underexplored hybrid model, a lack of network-level threat modelling, a lack of supporting validation either in paper-based or offline-based, and low adoption of AI-oriented predictive tools. The rigorous analysis of existing studies with comparative assessment exhibits that current techniques (PKI and blockchain) mitigates basical security loopholes like tampering and forgery, while they are always inadequate against all evolving attacks like social engineering and collusion. The learning outcome of the study is found to offer potential implications towards both practice and academia. The critical research gap highlighted in this study opens up an avenue towards an interoperable system with hybrid authentication and anomaly detection for researchers. However, there is a need to transform the existing centralised and monolithic architectures towards better security policymaking and resilient systems.

The future work will be continued towards integrating ML and AI models for developing a context-aware security model with predictive architectures. It is anticipated that such a form of solution could eventually offer resilience towards potential forms of threats. This will also offer a new introduction of automated risk mitigation in platforms of essential document digitisation.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Anuradha Uppar	✓	✓	✓	✓	✓	✓		✓	✓	✓				
Nagaveni Veerakyatharayappa		✓				✓		✓		✓	✓	✓		
Parvathi Chikkanna		✓		✓		✓	✓	✓		✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] F. Naguji *et al.*, "GreenLand: A Secure Land Registration Scheme for Blockchain and AI-Enabled Agriculture Industry 5.0," *IEEE Access*, vol. 12, pp. 120994–121009, 2024, doi: 10.1109/ACCESS.2024.3451627.

[2] Y. Xu and Z. Li, "PIRB: Privacy-Preserving Identity-Based Redactable Blockchains with Accountability," *Electronics*, vol. 12, no. 18, pp. 1–23, Sep. 2023, doi: 10.3390/electronics12183754.

[3] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Ransomware detection, avoidance, and mitigation scheme: A review and future directions," *Sustainability*, vol. 14, no. 1, pp. 1–24, Dec. 2022, doi: 10.3390/su14010008.

[4] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, and G. Singh, "Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability," *Journal of Cloud Computing*, vol. 13, no. 1, p. 45, Feb. 2024, doi: 10.1186/s13677-024-00605-z.

[5] A. Mohammad, "Distributed Authentication and Authorization Models in Cloud Computing Systems: A Literature Review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 107–123, Mar. 2022, doi: 10.3390/jcp2010008.

[6] Z. M. Saadi, A. T. Sadiq, O. Z. Akif, and A. K. Farhan, "A Survey: Security Vulnerabilities and Protective Strategies for Graphical Passwords," *Electronics*, vol. 13, no. 15, pp. 1–30, Aug. 2024, doi: 10.3390/electronics13153042.

[7] T. Arif, B. Jo, and J. H. Park, "A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats," *Sensors*, vol. 25, no. 8, pp. 1–30, Apr. 2025, doi: 10.3390/s25082350.

[8] S. S. Zabukovšek, S. Jordan, and S. Bobek, "Managing Document Management Systems' Life Cycle in Relation to an Organization's Maturity for Digital Transformation," *Sustainability*, vol. 15, no. 21, p. 15212, Oct. 2023, doi: 10.3390/su152115212.

[9] O. Ege, M. Cagal, and K. Bicakci, "Usability of Token-based and Remote Electronic Signatures: A User Experience Study," *arXiv*, 2025, doi: 10.48550/arXiv.2505.18814.

[10] Z. E. Ahmed *et al.*, "A Complementary Approach for Securing and Anti-Counterfeiting of Valuable Documents Based on Encryption of Computer-Generated Hologram," *Sensors*, vol. 25, no. 8, pp. 1–17, Apr. 2025, doi: 10.3390/s25082410.

[11] M. Nazarkevych, I. Izonin, M. L. M. Gregus, and N. Lotoshynska, "An approach towards the protection for printed documents bymeans of latent elements with fractal grids and electronic determination of its authenticity," *Electronics*, vol. 9, no. 4, pp. 1–14, Apr. 2020, doi: 10.3390/electronics9040667.

[12] X. Lu, F. Wang, C. Jiang, and P. Lio, "A Universal Malicious Documents Static Detection Framework Based on Feature Generalization," *Applied Sciences*, vol. 11, no. 24, pp. 1–23, Dec. 2021, doi: 10.3390/app112412134.

[13] J. F. Santos, M. P. Correia, and T. R. Dias, "Blockchain-based Rental Documentation Management with Audit Support," in *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Berlin, Germany: IEEE, Oct. 2024, pp. 1–10, doi: 10.1109/BRAINS63024.2024.10732316.

[14] S. Sharma, J. J. Zou, and G. Fang, "A dual watermarking scheme for identity protection," *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 2207–2236, Jan. 2023, doi: 10.1007/s11042-022-13207-1.

[15] A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, pp. 1–20, Feb. 2024, doi: 10.1016/j.jisa.2023.103678.

[16] A. A. Agarkar, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L. Kulkarni, "Blockchain aware decentralized identity management and access control system," *Measurement: Sensors*, vol. 31, pp. 1–10, Feb. 2024, doi: 10.1016/j.measen.2024.101032.

[17] R. M. Zein and H. Twinomurinzi, "Information Sharing in Land Registration Using Hyperledger Fabric Blockchain," *Blockchains*, vol. 2, no. 2, pp. 107–133, Apr. 2024, doi: 10.3390/blockchains2020006.

[18] K. M. Alam, J. M. A. Rahman, A. Tasnim, and A. Akther, "A Blockchain-based Land Title Management System for Bangladesh," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3096–3110, Jun. 2022, doi: 10.1016/j.jksuci.2020.10.011.
[19] R. Wang, C. Li, K. Zhang, and B. Tu, "Zero-trust based dynamic access control for cloud computing," *Cybersecurity*, vol. 8, no. 1, Feb. 2025, doi: 10.1186/s42400-024-00320-x.
[20] M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood, and M. Zhu, "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security," *IEEE Access*, vol. 12, pp. 26334–26343, 2024, doi: 10.1109/ACCESS.2024.3351119.
[21] B. Fetai, J. Tekavec, M. K. Fras, and A. Lisec, "Inconsistencies in Cadastral Boundary Data—Digitisation and Maintenance," *Land*, vol. 11, no. 12, pp. 1–19, Dec. 2022, doi: 10.3390/land11122318.
[22] E. Puniach, W. Gruszczyński, P. Ćwiąkała, K. Strząbała, and E. Pastucha, "Recognition of Urbanized Areas in UAV-Derived Very-High-Resolution Visible-Light Imagery," *Remote Sensing*, vol. 16, no. 18, pp. 1–21, Sep. 2024, doi: 10.3390/rs16183444.
[23] C. Regueiro, I. Seco, I. Gutiérrez-Agüero, B. Urquizu, and J. Mansell, "A blockchain-based audit trail mechanism: Design and implementation," *Algorithms*, vol. 14, no. 12, pp. 1–16, Nov. 2021, doi: 10.3390/a14120341.
[24] M. Sheeraz, M. H. Durad, M. A. Paracha, S. M. Mohsin, S. N. Kazmi, and C. Maple, "Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection," *Sensors*, vol. 24, no. 15, pp. 1–22, Jul. 2024, doi: 10.3390/s24154901.
[25] J. Xie, S. Xuan, W. You, Z. Wu, and H. Chen, "An Effective Model of Confidentiality Management of Digital Archives in a Cloud Environment," *Electronics*, vol. 11, no. 18, pp. 1–17, Sep. 2022, doi: 10.3390/electronics11182831.
[26] C. Amici, M. Rotilio, P. De Berardinis, and F. Cucchiella, "Framework for Computerizing the Processes of a Job and Automating the Operational Management on Site—A Case Study of Demolition and Reconstruction Construction Site," *Buildings*, vol. 12, no. 6, pp. 1–17, Jun. 2022, doi: 10.3390/buildings12060800.

BIOGRAPHIES OF AUTHORS

Anuradha Uppar is an Assistant Professor at Sambhram Institute of Technology, Bengaluru, currently pursuing her Ph.D. in Computer Science and Engineering at AMC, VTU. Her research focuses on the digitization of land records using blockchain technology. She holds an M.Tech. in Software Engineering and a B.E. in Computer Science Engineering. With teaching and mentoring expertise in cryptography, IoT, blockchain, and computer networks. She can be contacted at email: anu.charana@gmail.com.

Dr. Nagaveni Veerakyatharayappa from Bengaluru- Karnataka, India, obtained B.E. (Computer Science and Engineering) degree from Bangalore University in the year 2000. M.Tech. in Computer Science and Engineering from VTU Belagavi, Karnataka in 2006 and awarded Ph.D. in Exploring Parallelism and performance analysis on scheduling and DNS sequencing algorithms with multicore Architectures from Bharathiar University Coimbatore, Tamil Nadu in the year 2016 and guiding six research scholars from VTU, three scholars awarded Ph.D. She is currently working as Professor and HoD in CSE (DS), at AMC Engineering College, Bengaluru. Karnataka, India. She is a member of professional bodies such as LMISTE, IAENG, CSI, IFERP, and CSI- Bangalore Chapter. The research area of interest is HPC and IoT. She can be contacted at email: nagaveniveerakyatharayappa@gmail.com.

Dr. Parvathi Chikkanna from Bengaluru, Karnataka, India, obtained B.E. (Information Science and Engineering) degree from VTU, Belgaum in the year 2005, M.Tech. in CNE form VTU Belgaum in 2012 and awarded Ph.D. in design and development of energy efficient hierarchical routing protocol for wireless sensor network from VTU, Belgaum in 2019, and guiding one research scholar. She is currently working as Professor and HoD, Department of Artificial Intelligence and Data Science, BGSCET, Bengaluru, Karnataka, India. She is a member of professional bodies such as CSI, ISTE, and InSc. The research area of interest includes, wireless sensor networks, artificial intelligence and data science, big data, and machine learning. She can be contacted at email: pvc311925@gmail.com.