A NOVEL MODEL FOR SECURING SEALS USING BLOCKCHAIN AND DIGITAL SIGNATURE BASED ON QUICK RESPONSE CODES

MAY WEZA[1], M. M. EL-GAYAR[1,2], AHMED ABO ELFETOH[3] AND MOHAMMED ELMOGY[1,*]

[1]Information Technology Department, Faculty of Computers and Information, Mansoura University, 35516, Mansoura, Egypt

[2]Faculty of Computer Science and Engineering, New Mansoura University, New Mansoura, Egypt

[3]Information Systems Department, Faculty of Computers and Information, Mansoura University, 35516, Mansoura, Egypt

*Correspondence: Mohammed Elmogy, Email: melmogy@mans.edu.eg

ABSTRACT

In an era where personal identification, academic achievements, and other critical records are increasingly digitized, the integrity of such documents is paramount. Conventional validation methods, such as stamp seal imprints from authoritative bodies, are under siege by sophisticated counterfeiters, leveraging technological advancements to undermine document authenticity. This study introduces a groundbreaking dual-strategy framework to fortify the security of these stamp seals through orchestrated partial and full digitalization. Our multifaceted approach synthesizes an array of authenticity indicators—encompassing stamp seal images, digital signatures, watermarks, and distinct textual elements—within a robust feature extraction and analysis protocol. This protocol is meticulously engineered to validate the integrity of both physical and digital documentation. Central to our framework is integrating a decentralized blockchain platform, which serves as a bastion for the encrypted authenticity data, ensuring a tamper-resistant, transparent, and distributable ledger of the stamp seals without any reliance on intermediaries. Complementing this, we generate a Quick Response (QR) code for each document, which serves as a portal to interface swiftly and securely with the blockchain record. Our comprehensive testing yields an impressive 98% accuracy and security rate in document and stamp seal imprint verification, markedly enhancing retrieval speeds. The culmination of our research is establishing a rapid, secure, and immutable verification system that significantly eclipses traditional centralized methods, heralding a new standard in document security.

Keywords: *Forged Stamp Seal Imprint; Digital Signature; QR Code; Blockchain; Smart Securing Model*

1.INTRODUCTION

In the current era, due to the rapid technological and digital field development, many countries have turned to the complete digital environment of smart cities and dispense with the paper environment. This is because of its environmental and health problems and high cost. However, the comprehensive or almost complete digital environment includes many issues, the most important of which is how to secure it in an accessible manner without hacking. Every day worldwide, many fake paper or electronic documents are discovered. The proliferation of tools, such as highly advanced technology software, printers, and scanners that professional counterfeiters work on, has made it difficult for the average employee in government and private sectors to detect forged documents. In this manuscript, we have addressed and overcome several critical challenges related to securing documents and stamp seals, which can be summarized as follows [1-4]:

- Most security and protection methods are implemented through centralized systems, introducing various concerns, such as single points of failure, data unavailability due to loss, and increased vulnerability to attacks.
- Detecting forgery in stamp seals and maintaining the credibility of critical documents issued by government agencies is an ongoing challenge due to the expertise of forgers, who continually adapt their techniques to evade detection.
- Identifying forged documents or stamp seals can take time and effort, sometimes days or months, leading to significant disruptions and inefficiencies within organizations.

TABLE 1. SOME OF THE ESSENTIAL TERMINOLOGIES.

Terminology	***Dentition***	***Illustration Example***
Stamp seal mold	Copper or plastic cereal mold that is engraved to form a definite shape or design. In the case of creating governmental stamp seal mold, special securing software is used for engraving the country stamp seal emblem, which represents the country symbol.	
Stamp seal imprints	It is the imprint formed mechanically using the stamp seal mold on paper.	
Stamp seal printout image	It is the image of the stamp seal formed by printing it from a computer on secured paper. In this case, we have the stamp seal as a printout image in a partially digitalized system.	
Stamp seal electronic image	It is an image of the stamp seal on a completely digitalized electronic system without a printout.	
Blockchain Platform	Blockchain is a shared, immutable ledger that facilitates recording transactions and tracking assets in a business network.	

As shown in Fig.1, most countries worldwide still put their stamp seal imprint mechanically (Mechanical Stamping). To create an auto-ink genuine stamp seal mold, the Egyptian government uses a laser engraving technique operated by special security software to engrave the mold. Table 1 shows some of the essential terminologies.

Also, in partial digitalization in many countries, they use the stamp seal printout as an image formed by printing on security paper with quick response (QR) codes. Although the stamp seal printout is genuine, not forged, it is the printout from the most commonly used printer, laser, or inkjet. The term "security paper" refers to paper used in security printing. It has security features that identify or authenticate a document as original, such as security printing offset, watermarks, security fibers, ultraviolet (UV) reactive ink, optically variable device, i.e., kinegram and hologram, microprint, and many other security features. Security paper can be used in currency, passports, identity cards (ID), driving licenses, academic certificates, and other official documents. The security paper's importance is to be difficult to counterfeit and to facilitate fraud detection. There are minimum requirements each country should follow in securing their documents. But, a normal person or un-specialized employee can't detect the forgery of official documents in most cases. It needs a forensic expert.

Definition of the above mentioned security features used in creating secure paper as follow:

- Security printing offset: This type represents the background printing in all official documents, including passports, IDs, driving licenses, and currency.
- Watermark: It is created during the stage of paper pulping. The difference in fiber thickness forms many types and shapes of the watermark. Watermark is very difficult to be counterfeited as it is produced during the primary stage of paper manufacturing.
- Security fibers: Very thin fibers are embedded randomly during paper manufacturing. It can be red, blue, green, or any other color. It can be visible with normal light or invisible with normal light and appear under UV light. Security fibers are very difficult to counterfeit as they are produced during the primary stage of paper manufacturing.
- UV reactive ink: It contains one component that reacts with UV in its ingredients. UV reactive ink can be invisible under normal light and visible under UV light. Another type can be visible under normal light and change its color under UV color, i.e., the written ink is under normal light black and changes when exposed to UV light into red color.

- Microprinting: The printed text is very small and needs a magnification lens or microscope to appear clearly. It is seen as lines without magnification and can be read as text under magnification.

- Optical variable device (OVD): The most used types of OVD as security features are hologram and kinegram. A hologram is an anti-counterfeiting feature added to most documents and banknotes. It is used to refract light due to nanostructures that refract light by tilting the document or banknotes. When light fall on a flat surface, it appears in a 3D effect, so the light is changed to much different light, or the shape seems to be moved to form another shape.

The forgers attempt to create fake stamp seal imprints using various forgery techniques:

- The first type involves forgers trying to imitate real stamp seal mold by making fake versions with special chemicals or laser engraving. To examine the suspected stamp seal imprint in this situation, the forensic examiner needs a reference of a real stamp seal imprint.

- The second type by producing counterfeit stamp seal imprints by printing. Forgers use many printing techniques to imitate genuine stamp seal imprints, i.e., laser, inkjet, and screen printing. The three printing techniques create fake stamp seal printouts that should be examined and detected only using magnification lenses or microscopes.

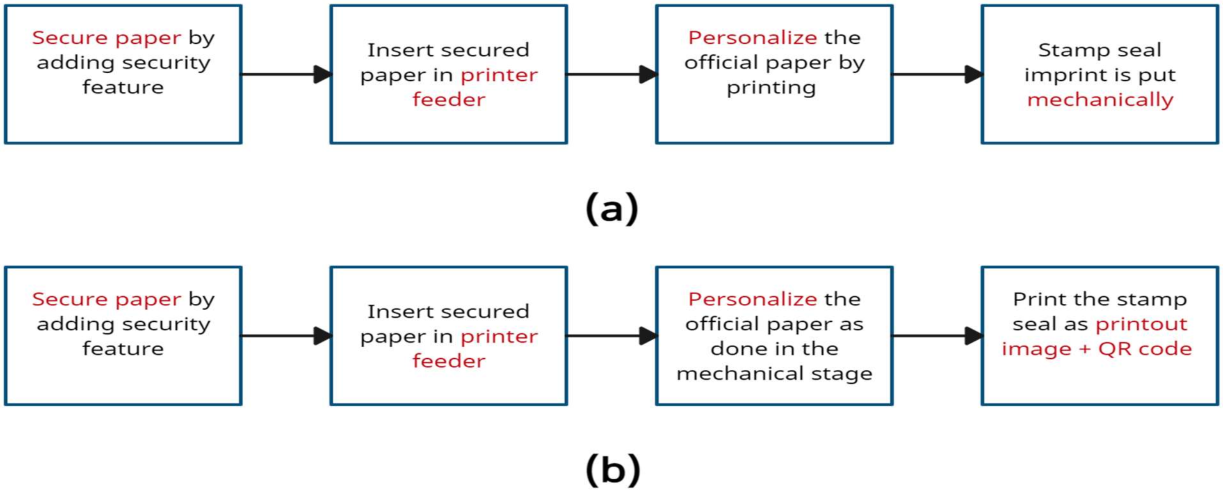

Secure paper by adding security feature
Insert secured paper in printer feeder
Personalize the official paper by printing
Stamp seal imprint is put mechanically
(a)
Secure paper by adding security feature
Insert secured paper in printer feeder
Personalize the official paper as done in the mechanical stage
Print the stamp seal as printout image + QR code
(b)

Figure 1. The stamp seal imprints and printout (a) Mechanical Stamping (b) Digital Stamping.

In the previous figure, illustration diagram (a) shows how the stamp is put mechanically on security paper and this is the most common way of stamping in most countries. Some countries use the way which is shown in illustration diagram (b) in which the stamp and QR code are inserted in the official document as an image created by printing (Digital Stamping). Although using security paper in both of the two ways reduces forging, thousands of forged documents have been discovered per day with forged security paper and forged stamp seal imprints.

To overcome these challenges, document verification should be a mandatory checking step for both paper and digital documents to get around this problem. The data must be stored to be impossible to change, hack or spoof to achieve document authentication. Also, the storage data must be decentralized, multiplexed, and distributed across an entire network of computer systems allowing all participants to verify the stored data or records. Document verification can be achieved optimally by applying Blockchain technology [1,7,8]. We can summarize the main contributions of this article in the following points:

- ✓ We propose a smart securing model to secure documents, stamp seals, and store them as a block through a decentralized blockchain platform.
- ✓ Encrypting the data of the stamp seals, such as the data of the concerned employee, the institution number, the date of issuance, and other data, in addition to the stamp seal image in a DIGITAL SIGNATURE WAY, DUE TO THE DIFFICULTY OF OBTAINING OR FALSIFYING IT.
- ✓ Generate a QR code to access encrypted information quickly and securely. After that, the authorized parties can remove the encryption and see the data. QR codes allow us to perform a hybrid system for accessing the electronic or paper-based system.

✓ The stamp seal image and the source details of the stamp seal data in the blockchain provide a shared, stable, and transparent history of the stamp seal without relying on any third party.

Blockchain does not need a centralized authority to operate. The blockchain network, instead, requires its participants to verify and authenticate the activities that occur in it. The entire process is done on a consensus mechanism basis, making the blockchain a trustless, secure, and reliable technology for digital transactions. A consensus mechanism is a protocol that ensures that all the blockchain network participants follow the agreed rules to confirm blocks to be recorded on the chain [5,6]. Many consensus mechanisms of different principles enable the network participants to follow those rules. Fig. 2 shows the taxonomy of consensus algorithms [6].

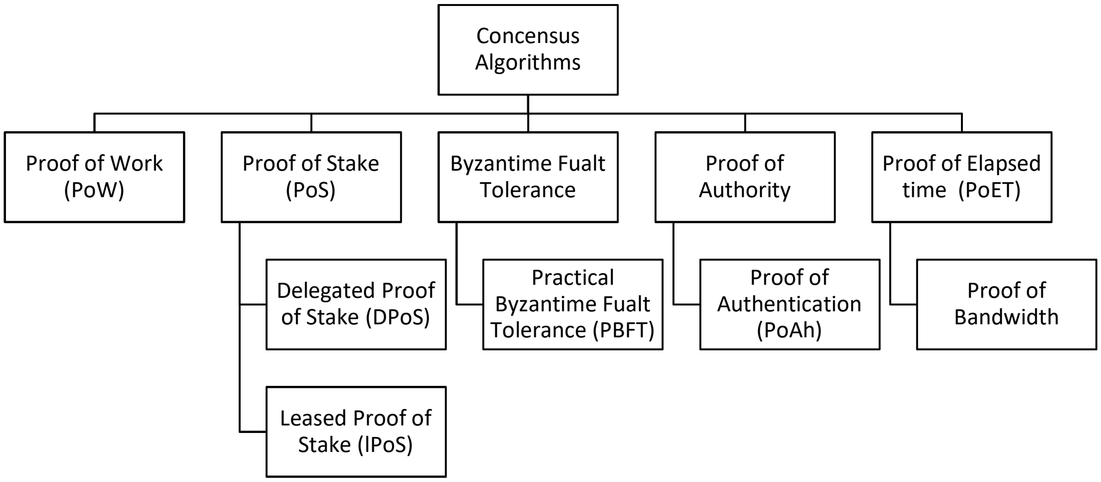

Concensus Algorithms
Proof of Work (PoW)
Proof of Stake (PoS)
Byzantime Fualt Tolerance
Proof of Authority
Proof of Elapsed time (PoET)
Delegated Proof of Stake (DPoS)
Practical Byzantime Fualt Tolerance (PBFT)
Proof of Authentication (PoAh)
Proof of Bandwidth
Leased Proof of Stake (lPoS)

Figure 2. The taxonomy of consensus algorithms.

The bedrock of trust in official documentation, from personal identification to academic credentials, rests on the assurance of authenticity—a confidence severely undermined by the surge in counterfeit documents. At the same time, the "what" of our research addresses the urgent need for a robust framework to secure stamp seal imprints, and the imperative "why" delves into the broader implications of these advancements. Our motivation stems from the escalating threat that documents forgery poses to personal identity safety, institutional integrity, and national security. The repercussions of inauthentic records are profound, spanning from individual losses to systemic failures in sectors that hinge on unassailable documentation.

We aim to preempt the counterfeiters' next move, stay ahead in the cybersecurity arms race, and bolster trust in document veracity at a global scale. As governmental and private entities seek to digitize their archives and transactional processes, the urgency for a secure, decentralized, and fail-proof system becomes not just a technological pursuit but a societal imperative. Our approach is designed not only to outpace the evolving sophistication of forgeries but also to integrate seamlessly with the digital transformation initiatives of modern governance. By anchoring our model in blockchain technology and digital signatures, we address the critical "why": to furnish a resilient, transparent, and efficient method for verifying stamp seals and documents that underpin our social fabric and legal frameworks. In doing so, we secure a fundamental cornerstone of societal transactions and provide a beacon of trust in an increasingly digital world.

The issue of stamp seal imprint forgery is indeed a global problem, and traditional methods of verification, such as forensic examination, are time-consuming and require specialized expertise. Moreover, the high volume of forged documents used in governmental transactions emphasizes the need for a more efficient, accessible, and reliable method of document authentication. Our proposed model aims to address these challenges by providing a novel way not only to secure stamp seal imprints and the entire document data but also to facilitate easier, faster, and more reliable authentication of official documents. By implementing our model, the role of the forensic expert becomes less frequent in the examination of stamp seal imprints, as the authenticity of an official document can be verified by any individual dealing with the document in less than a minute.

The scope of our work is outlined as follows:

- Development of a dual-strategy framework for securing stamp seal imprints in both traditional paper-based and fully digital environments.
- Implement a robust feature extraction and analysis technique tailored to assess the authenticity of physical and digital documents.
- Utilization of a decentralized blockchain platform for the encrypted storage of authenticity indicators.
  - Generation of secure QR codes to facilitate rapid access to the blockchain record and verification of documents.

The limitations and future works of our study are outlined as follows:

- Exploration of cross-chain interoperability for the blockchain component.
- Investigation of the environmental impact of blockchain technology and its long-term sustainability.
- Examination of the legal implications and regulatory considerations in different jurisdictions.

The rest of this manuscript is separated into five parts. Part II reviews some of the previous work in this research field. Part III represents the methodology. Part IV represents the proposed model and explains the different stages of the proposed algorithms. Part V describes the experimental results of some test cases and the discussion section. Finally, Part VI will provide the conclusion of the work.

2. LITERATURE REVIEW

This section reviews the various technologies and methods used to share and secure documents. In addition, this part concentrates on the distinct styles used recently in many prestigious journals. For example, Singhal and Pavithr [9] presented a technique to prevent the circulation of fraudulent degree certificates using a smartphone application and a QR code. Authors used digital signatures to encrypt data, such as the holder's name, enrollment number, registration number, and total marks achieved, which university officials will sign. A user must use a particular smartphone application to verify the digital signature by scanning the QR code. Blockchain technology has been recognized as a promising solution to many challenges smart cities face. Blockchain's decentralized, secure, and transparent nature makes it an ideal technology to manage a wide range of services in a smart city [10]. Blockchain technology can be applied in various domains within a smart city, such as energy management as Blockchain technology is being used to develop decentralized energy grids where consumers can trade energy in a peer-to-peer manner, which enhances energy efficiency and sustainability [11], transportation as Blockchain technology can be used to create transparent and efficient systems for public transportation, parking, and traffic management [12], waste management as Blockchain technology can ensure transparency and efficiency in waste management by tracking waste from generation to disposal [13] and document verification and authentication as Blockchain technology is increasingly being used as a document verification and authentication tool. Its decentralized and immutable nature makes it a reliable technology for storing and verifying data, including images and other documents [14]. Blockchain technology can help overcome several challenges faced by citizens in smart cities including: Data Security and Privacy: Blockchain's decentralized nature can help enhance data security and privacy, a key concern in smart cities where large volumes of data are collected and processed [15]. Trust and Transparency: Blockchain can increase trust and transparency in public services by providing a tamper-proof and auditable record of transactions [16]. Efficiency and Automation: Smart contracts on blockchain can increase efficiency and automation of various city services, reducing bureaucratic delays and improving citizen services [17]. Academic Certificates: Blockchain technology is being used to verify the authenticity of academic certificates, reducing the risk of forgery [18]. Government Documents: Governments are looking into blockchain for the authentication of official documents, such as birth and marriage certificates [19]. Yermack [20] considered how blockchain affects institutional investors, auditors, small shareholders, managers, and other participants in corporate governance. The author presented the benefits of blockchain, such as cheaper; better liquidity, more precise record-keeping, and ownership transparency may dramatically shift the power balance among these generations. Sullivan and Burger [21] conducted a performance analysis of the use of blockchain in e-Residency can radically alter how identification information is managed and verified. The legal, policy and technological consequences of this development are examined in this study.

Pongnumkul et al. [22] conducted a performance analysis using two prominent private blockchain technologies, hyper ledger fabric and Ethereum. Hyperledger Fabric regularly beats Ethereum across all evaluation criteria, including execution time, latency, and throughput, according to the testing results based on different numbers of transactions. Furthermore, both platforms are still not competitive with existing database systems regarding performance in high-load circumstances. Xu et al. [23] presented the educational certificate blockchain (ECBC) system. This system can operate with low latency and high throughput. This system effectively provides data on time and is suitable for the infrastructure of decentralized electronic systems. But it does not offer sufficient security for information in terms of authenticity.

Saha [24] proposed a system that allows users to create digital signatures for documents and articles online and interact without using difficult methods. Rather than encrypting the entire text, this system creates signatures based on basic information in any document. But this system works on a central network that does not provide a fast environment for the availability of information, as it is considered a single point of failure and can be easily penetrated. Nguyen et al. [25] suggested a method for issuing immutable digital certificates that use blockchain technology to overcome the current limitations of traditional certificate verification systems, such as being more trustworthy and independent of a central authority. The results show that their proposed system is an acceptable ICT-based e-government solution, especially in managing certificates and diplomas. But this proposed system does not provide the speed and ease necessary for data availability on time.

Cheng et al. [26] proposed a system that can handle all kinds of official documents through blockchain technologies to provide a secure environment that cannot be changed or tampered. However, this system does not provide sufficient data confidentiality. Also, it cannot determine the source and reliability of the data. Khan et al. [27] proposed an intelligent system for the Dubai e-government private economy department that integrates new technologies to use the blockchain to make Dubai a more innovative city. Dubai's smart government has used blockchain technologies to make transactions more accessible and stable. But this system needs techniques to know the data source and detect its forgery.

Xu et al. [28] proposed an electronic certificate catalog sharing system (ECCS) that relies on the blockchain consortium to improve the efficiency and accessibility of e-government delivery service by implementing time and data immutability in the blockchain. According to the security analysis, ECCS can protect the privacy of certificates and electronic catalogs from unauthorized individuals. But the system needs to ensure data integrity and authentication of data sources. Suma [29] Massive amounts of court-generated data, security records, legislation, trade code, and other sources won't be misused or corrupted because of the security and privacy mechanism based on blockchain that is explained. The suggested system secures the reliability and credibility of data exchange through communication channels using the Rivest, Shamir, and Adleman (RSA) mechanism. However, this solution does not offer quick access to data using a QR code at any time or location.

Geneiatakis et al. [30] studied whether the e-government service can be decentralized using the blockchain. The authors propose a system that supports commodity exchanges across the European Union. The results indicate that the implemented system can meet the standards related to productivity and information availability. However, the system cannot detect counterfeiting or the reliability of the sources. Bharadi et al. [31] introduced a blockchain-based system to create trust and integrate different subunits of local public service systems. The existing system used the Azure blockchain workbench to connect these modules and keep them in sync and confident.

Xie et al. [32] used blockchain technology and smart contract to build a decentralized certificate system. Some certificate management, issuance, authentication, and revocation functions were implemented using smart contracts. In addition, the signer, certificate prototype, and certificate data were embedded in a smart contract, making it easy to query and validate certificates. However, this system does not maintain the confidentiality of the data. He et al. [33] proposed an access control for data sharing to avoid security issues over the cloud. The authors used an attribute-based hierarchical scheme with blockchain technology as an access control scheme. However, this system does not maintain confidentiality. Also, the authors did not say which blockchain platform was used.

Sun et al. [34] constructed an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records. They used a ciphertext policy attribute-based encryption system, IPFS storage environment, and blockchain technology. Gao et al. [35] used blockchain technology to handle the problems in Notarial Office (NO). This system was built on top of the

Hyperledger Fabric. Furthermore, they used smart contracts to substitute manual procedures, create additional ledgers to offload different transactions, and encrypt sensitive data as necessary.

Das et al. [36] used blockchain technology to improve data integrity in document management for construction applications by using smart contracts for irreversible and irrevocable workflow logic, blockchain ledgers to record document changes, and a blockchain-based data structure or document version history integrity. Anwar et al. [37] constructed SCi-B (Student-Centered iLearning Blockchain) framework, a new learning model innovation that is possible using Blockchain technology. To organize and record all transactions, competencies, and teaching that can deliver intensive assessments through digital certificates for the academic world and the world of work, SCi-B is an innovation in the learning paradigm where all activities use blockchain. Therefore, SCi-B significantly increases confidence in the results that have been received.

In the review chapter, Sharma et al. [38] examined blockchain concepts and outlined numerous blockchain myths and realities. This chapter tries to separate misconceptions from facts by emphasizing that many industries can use blockchain technology. The chapter is intended to considerably aid users in comprehending the ideas, being aware of the blockchain myths and realities, and gaining comprehension of some of the prevalent misconceptions. Pambudi et al. [39] proposed blockchain-based methods to solve Indonesia's problem of widespread diploma forgery. Time can be saved by requiring authentication from the company's users. Odeh et al. [40] proposed an approach model which is presented for a private blockchain-based software program that uses Hyperledger fabric, one of the well-liked blockchain technologies, to digitize supporting paper documents. Furthermore, a verification approach utilizing facial and text recognition technologies is suggested to further assure the legitimacy of information access. The primary goal is to preserve all personal documents, including identification cards, licenses, and birth certificates, in one location that is always accessible.

Biswas et al. [41] proposed exam delivery system through peer-to-peer (P2P) networks based on blockchain in addition to distributing certificates and marksheets to students when posting exam results. This avoids the upkeep of results records maintained by colleges, universities, education sectors, etc., yet, it promotes the submission of phony certificates and supports proofs of degrees claimed by students. Pu and Lam [42] perform a comprehensive analysis of the advantages of blockchain for digital certificates using various case study techniques to fully understand the potential of blockchain for digital certificates in a holistic view.

Sharma et al. [43] proposed a secure blockchain-based system to create, preserve, and verify healthcare certificates. To develop and verify medical credentials, the PA is a communication channel between the backend blockchain network and application entities, including hospitals, patients, doctors, and IoT devices. Utilizing the idea of smart contracts, it also guarantees several security features, including secrecy, authentication, and access control. Also, we suggest evaluating our model against attacks such as DoS, phishing and forgery attacks such as those demonstrated in these references [44].

Shah and Kotecha [45] proposed a blockchain-based framework for improving government services and citizen experience in a smart city. The framework focuses on ensuring transparency, trust, and security in the delivery of public services.

Pažur and Vlahinić [46] presented a blockchain-based system for digital document verification, which can be applied in various contexts, including smart city citizenship, to prevent document forgery and ensure trust in digital transactions.

Khatoon [47] proposed a secure and efficient digital identity management system for smart cities using blockchain technology. The system aims to enhance citizens' privacy, security, and trust in digital transactions.

Sylim et el. [48] presented a case study on the application of blockchain technology in genomics and public health registry, which could provide insights into how blockchain can be used to secure sensitive data and prevent forgery.

Chen et al. [49] provided a comprehensive overview of blockchain network consensus mechanisms and mining management. It can serve as a resource for understanding the underlying technology and its potential applications in smart city citizenship.

Chouhan and Singh [50] presented a blockchain-based digital document verification system designed explicitly for education certificates. The main goal of this study is to develop and evaluate a blockchain-based system for verifying education certificates. This would involve designing a system that can store and verify these certificates securely, transparently, and tamper-proof. The paper could offer insights into the practical applications of blockchain technology in document verification, which would be valuable to various stakeholders in the academic and technology sectors. Potential limitations of the study relate to the scalability of the proposed system, its security against advanced attacks, or its reliance on specific technological infrastructures that may not be universally available. The particular types of education certificates also limit the paper.

Zyskind et al. [51] presented a novel approach to storing personal data and identity information on a blockchain. This study's primary goal is to explore how blockchain technology can protect personal data, likely focusing on enhancing privacy and control for individuals over their personal information. Some limitations include the technical challenges of implementing such a system on a large scale, the regulatory implications of decentralizing personal data, and potential security vulnerabilities.

Khan et al. [52] delved into the innovative and disruptive potential of blockchain technology. Through a comprehensive review of the literature on the global governmental use of blockchain, they gained insights into various governments' current applications of this technology. This study also highlighted the advantages and obstacles that these governments encounter when integrating blockchain into their e-service provisions. The research focused on transforming a public sector entity in Dubai from a conventional platform to a blockchain-based system. The study should concentrate on tangible data from a selection of ongoing projects in the UAE that have employed blockchain technology to create services for the public sector. In addition, developing a tailored evaluation framework would be beneficial for collecting field data, facilitating a comparative study of different cases, and enabling the extrapolation of findings.

Al-Kodmany [53] aimed to identify and discuss major themes in contemporary urbanism in the Middle East and North Africa (MENA) region. It examines shifts in the conceptualization and practice of urban planning and design. The study contributes a conceptual framework for understanding "New Arab Urbanism" in the MENA region. It highlights postmodernism, globalization, consumerism, sustainability, heritage preservation, and new technologies. The paper provides a broad overview of New Arab Urbanism and does not provide an in-depth analysis of specific cities or case studies. It also focuses mainly on Gulf countries and does not adequately discuss urban trends in the wider MENA region.

Cardullo and Kitchin [54] examined the forms and extent of citizen participation in Dublin's smart city initiative. It analyses the rhetoric and reality of citizen engagement in Dublin's smart city agenda. The study contributes to debates around digital inclusion, citizen participation, and governance in smart cities. It assesses Dublin's efforts to involve and empower citizens through its smart city programs. But there are some limitations. The analysis is based on a particular point in time and does not track changes in citizen participation over the evolution of Dublin's smart city project. The study also focuses only on Dublin and does not make comparisons with other cities.

Physical documents, such as contracts, certificates, and official records, often rely on stamp seals to authenticate. Ensuring the authenticity of these documents is a critical challenge, as forgeries can lead to legal disputes, financial losses, and loss of trust in the institutions involved. Traditional methods of verifying the authenticity of stamp seals on paper documents can be time-consuming, error-prone, and reliant on human expertise. In smart cities, we need to demonstrate a detection and verification mechanism to ensure data integrity against phishing attacks [55]. [56]. Table II summarizes recent related works through several comparisons, such as distributed data availability, performing a hybrid platform (support electronic and paper-based systems), and performing data encryption to ensure data confidentiality and authenticity.

TABLE 2. SUMMARY OF RECENT RELATED WORK.

Study	Support Distributed Data Availability	Support Hybrid Platform	Support Digital Signature	Support Data Authenticity
Singhal & Pavihr [9]	×	√	×	√
Yermack [10]	√	×	×	×
Sullivan & Burger [11]	√	×	×	×
Pongnumkul et al. [12]	√	×	×	×
Xu et al. [13]	√	×	×	×
Saha [14]	×	×	√	√

Nguyen et al. [15]	√	×	×	√
Cheng et al. [16]	√	×	×	×
Khan et al. [17]	√	√	×	×
Xu et al. [18]	√	×	√	×
Suma [19]	√	×	√	√
Soupionis [20]	√	×	×	×
Bharadi [21]	√	×	×	×
Xie et al. [22]	√	×	×	√
He et al. [23]	√	×	×	×
Sun et al. [24]	√	√	√	×
Gao et al. [25]	√	×	√	×

3. METHDOLOGY

This study proposes a novel approach for securing stamp seal imprints by combining digitalization techniques and leveraging a decentralized blockchain platform. This section outlines our research methodology, including the development of the proposed approach, the data collection and sources, the evaluation of our method's effectiveness, and the validation of our results.

3.1 Development of the Proposed Model

Our research started with developing the proposed model for securing stamp seal imprints. The process involved the following steps:

3.1.1 Design of the digitalization framework

We designed a digitalization framework that allows for partial digitalization of paper-based systems and Full digitalizied. This framework integrates multiple authenticity indicators, such as stamp seal images, signatures, watermarks, and unique textual patterns.

3.1.2 Implementation of the feature extraction and analysis technique

We developed a robust feature extraction and analysis technique to assess the authenticity of documents based on the integrated authenticity indicators. This technique involves the use of advanced image processing and pattern recognition algorithms.

3.1.3 Integration of the blockchain platform

We integrated a decentralized blockchain platform to securely store encrypted data related to the authenticity indicators, providing a tamper-proof, transparent, and shareable record of the stamp seals without requiring third-party intermediaries.

3.1.4 QR code generation

We implemented a mechanism for generating a QR code for each document, which enables rapid and secure access to the corresponding blockchain record.

3.2 Data Collection and Sources

To evaluate the effectiveness of our proposed approach, we collected a dataset of various documents containing stamp seal imprints, signatures, watermarks, and unique textual patterns. The dataset included:

3.2.1 Authentic documents

We collected a sample of authentic documents, including contracts, certificates, and legal documents, with genuine stamp seal imprints and other authenticity indicators.

3.2.2 Forgeries

We collected a set of forged documents containing manipulated stamp seal imprints and other altered authenticity indicators.

3.3 Evaluation of the Proposed Approach

To assess the effectiveness of our proposed approach in identifying authentic and forged documents, we evaluated our model using performance metrics, such as QR readability, throughput, time-consuming accuracy, and query, to quantify the effectiveness of our proposed model.

3.4 Validation

To ensure the validity and reliability of our findings, we took the following steps:

3.4.1 Cross-validation

We performed k-fold cross-validation on our dataset to assess the robustness of our feature extraction and analysis technique and to minimize the risk of over fitting.

3.4.2 External validation

We sought feedback from domain experts, including document security and stamp seal authentication professionals, to independently assess our proposed approach's effectiveness and practicality.

4. PROPOSED MODEL

This section discusses the proposed model for securing the smart seal within important official papers. Fig. 3 shows the general steps of the proposed model. The proposed model contains three primary stages. At the source phase, the organization's seal and the employee's data are encrypted using the organization's private key to output the encrypted digest. Also, an encrypted digest is converted into a QR code to be verified easily with paper-based systems. At the blockchain platform phase, an encrypted digest as a transaction is formed into a block by the organization's node on the Ethereum open-source distributed network. Then, this block is linked to other transactions in a network to make tampering difficult. After being granted access control to this blockchain block from the blockchain platform in the verification phase, this block is divided into a hash digest and original data. The digest is decrypted using the organization's public key. At the same time, the actual data is hashed using the same hash function to produce the new digest. Then, the decrypted digest and the new digest are compared together. If the comparison result is true, the block is authenticated and reliable.

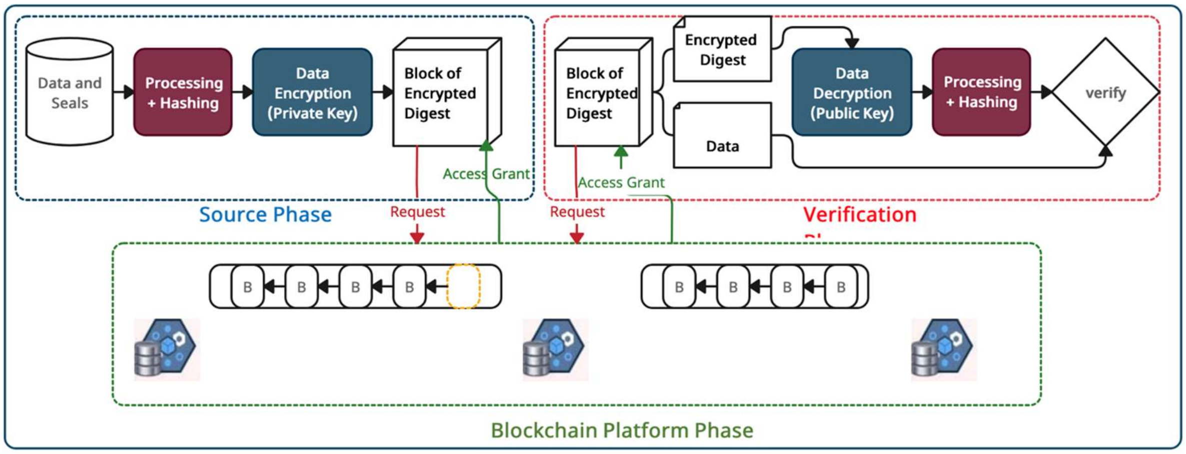


Figure 3. The general steps of the proposed model.

4.1 Source Phase

At this phase, the seal or document source (the official organization responsible for creating the document or seal). As shown in Fig. 4, this phase begins with entering the data of the concerned employee, such as the employee's name, the job code, and the organization code, to the hash function (i.e., SHA 256) for producing the hash value or the digest. There are four steps to ensure stability and uniqueness concerns when generating hash values from the stamp seal imprints. It's essential to develop a robust feature extraction and hashing algorithm that can reliably handle variations in the input images. The first step is image preprocessing to enhance the visibility of the stamp seal imprint by applying noise reduction filters, converting the image to gray scale, and applying adaptive histogram equalization. The second step is a stamp seal detection process to identify and isolate the region containing the stamp seal imprint using template matching. The third step is extracting and encoding the feature vector from the stamp seal imprint image. We use Fourier descriptors that capture the geometric properties of the stamp seal imprint. Also, we use Local Binary Patterns (LBP) and Gabor filters to characterize the texture patterns

Within the stamp seal imprint. Moreover, we use Speeded-Up Robust Features (SURF) as local features that are invariant to scale and rotation transformations [55]. Then, Normalize the feature vector using z-score normalization to ensure all values are within a specific range. The final step is converting the normalized feature vector into a byte-string or binary representation. Then, the cryptographic hash function using Locality-Sensitive Hashing (LSH) and SHA-256 is applied to the encoded feature vector. This function should take the byte-string as input and produce a fixed-size hash value. The choice of the hash function should provide sufficient security and collision resistance. After that, the digest is encrypted using the source's private key. Then, the encrypted digest is appended to the original data to produce the ledger block stored within the distributed network in the blockchain platform.

As shown in Fig. 5, Each block contains a set of essential data in its header, such as the block ID (BID), the encrypted hash value (BKH), a timestamp, the source's public key (puk), the usage policy, and a previous block pointer. Block's header is implemented in two different types (request and response for granting access to the blockchain platform) using JavaScript object notation (JSON) format, as shown in Fig. 6. Finally, if the status of the block is approved to be stored within the blockchain network, a QR code can be generated using the block's ID. The QR code can also be printed on the paper document inside the paper system.

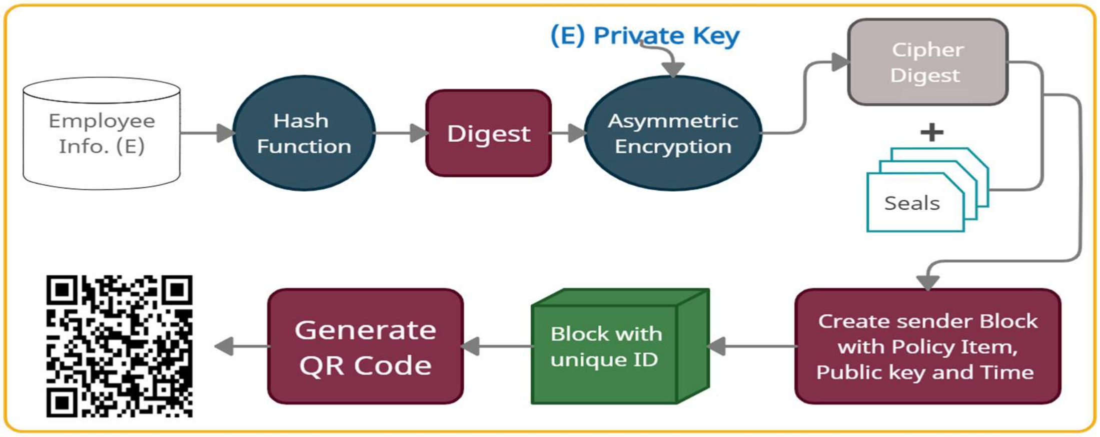


Figure 4. The block diagram of the source phase.

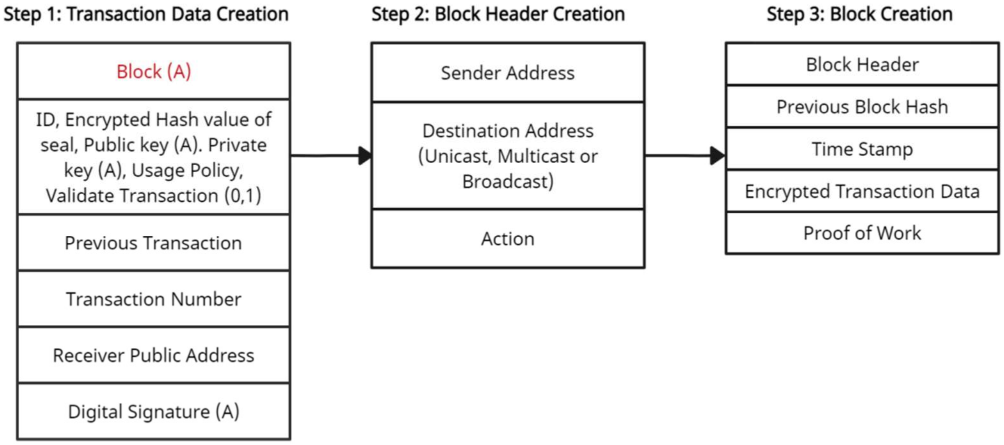
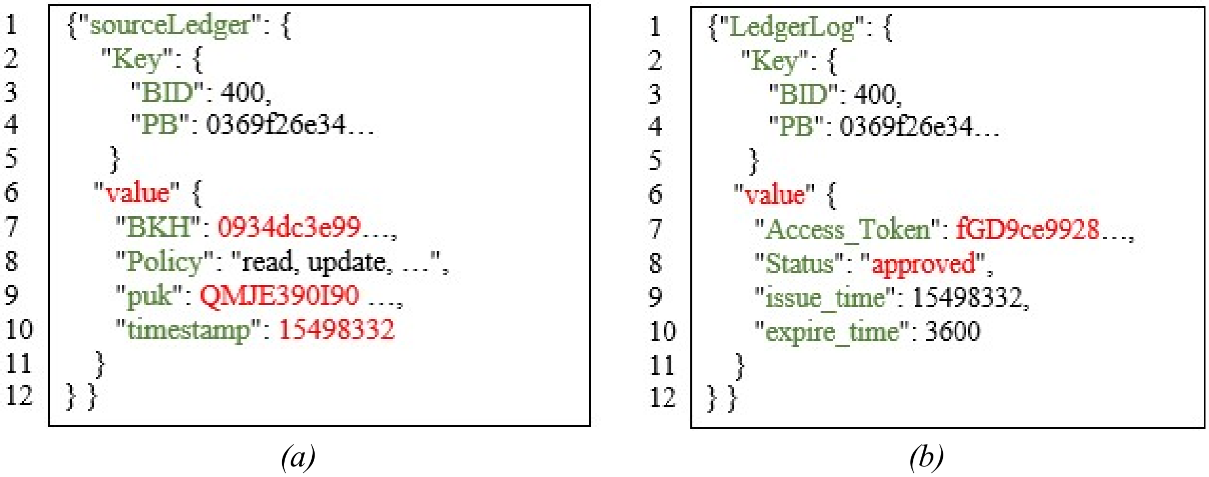

Step 1: Transaction Data Creation
Block (A)
ID, Encrypted Hash value of seal, Public key (A). Private key (A), Usage Policy, Validate Transaction (0,1)
Previous Transaction
Transaction Number
Receiver Public Address
Digital Signature (A)
Step 2: Block Header Creation
Sender Address
Destination Address (Unicast, Multicast or Broadcast)
Action
Step 3: Block Creation
Block Header
Previous Block Hash
Time Stamp
Encrypted Transaction Data
Proof of Work

Figure 5. The steps of block creation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(a)

```
{"sourceLedger": {
   "Key": {
     "BID": 400,
     "PB": 0369f26e34…
   }
  "value" {
    "BKH": 0934dc3e99…,
    "Policy": "read, update, …",
    "puk": QMJE390I90 …,
    "timestamp": 15498332
  }
} }
```

(b)

```
{"LedgerLog": {
   "Key": {
     "BID": 400,
     "PB": 0369f26e34…
   }
  "value" {
    "Access_Token": fGD9ce9928…,
    "Status": "approved",
    "issue_time": 15498332,
    "expire_time": 3600
  }
} }
```

Figure 6. The content of different block headers in the blockchain. (a) Content of the requested block header from ledger source to add new block into blockchain platform based on a JSON format. (b) Content of the response block header from ledger log to source ledger based on a JSON format.

QR code is a two-dimensional barcode with many benefits compared to other codes, such as single-dimension barcodes [57]. Also, it has a suitable mechanism for encrypting information. Furthermore, the QR code is fast, flexible, easy to read, and fault tolerant. The QR code's data capacity varies depending on the data it maintains; it can carry up to 2953, 4296, or 7,089 symbols for binary/byte formats, alphanumeric or numeric, respectively. However, a classic one-dimensional barcode can maintain a maximum of only 20 digits. Since our manuscript focuses on securing stamp seal imprints and documents using a decentralized blockchain platform along with QR codes, an efficient and secure compression algorithm that minimizes data size while maintaining data integrity is vital. Huffman, arithmetic, and adaptive compression algorithms are lossless data compression techniques, but they differ in their approach, complexity, and performance. We applied these algorithms to choose the suitable one. Huffman and arithmetic coding are entropy-based compression algorithms, with arithmetic coding generally providing better compression ratios than Huffman coding. However, these methods can be more computationally intensive and may only sometimes result in optimal compression for diverse data types. We found that Burrows-Wheeler Transform (BWT) as an adaptive compression algorithm provides better compression efficiency and adaptability for various data types. Fig.7 represents how binary images can be compressed and converted into QR codes using the BWT algorithm and XOR method.

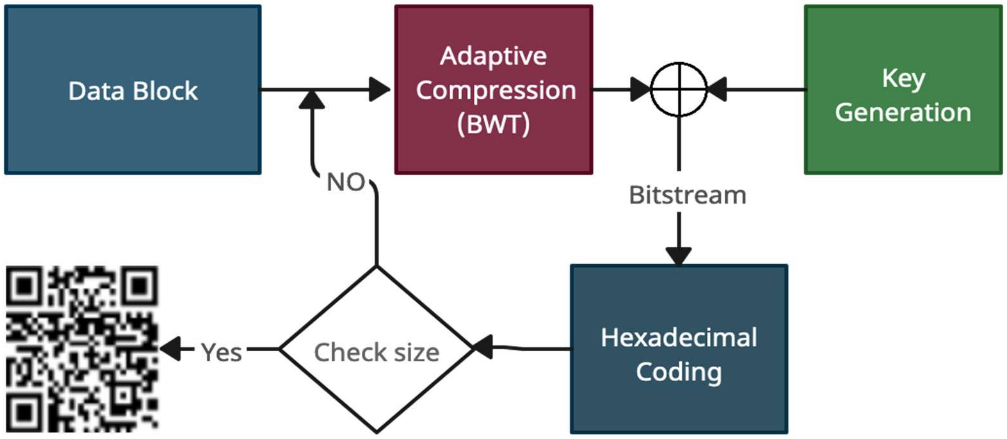


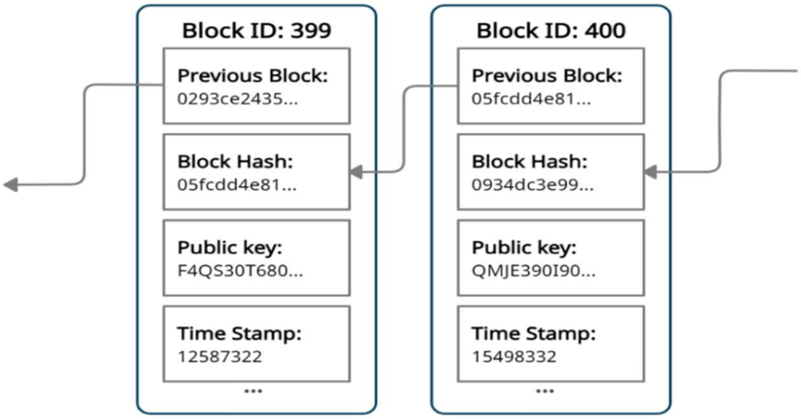
Figure 7. The generation of QR codes.

4.2 Blockchain Platform Phase

The blockchain concept was proposed in 2008 as an alternative to the inconvenient central database by Satoshi Nakamoto. Blockchain technology links many blocks as a distributed ledger of successful transactions through many nodes, making counterfeit or manipulating them difficult. This technology has been used in many fields, such as creating smart contracts, education, finance, and linking patients' health records. The first block in the Blockchain platform is called Genesis Block. Then each block is connected to a group of blocks that belong to the same ledger, as shown in Fig. 8. This technology was used because it provides decentralized transactions and proof of Stake [58,59]. Achieving a critical mass of users and participants is crucial for a blockchain network to function optimally and provide the desired benefits of decentralization, security, and trust. This challenge is more pronounced for newly established blockchain networks or those with niche applications. So, we suggest applying some strategies to overcome this limitation such as Interoperability to ensure that a blockchain network can effectively communicate and exchange information with other networks and systems, encouraging widespread adoption and facilitating the network's growth. Also, we can deploy collaboration and partnerships to engage with industry players, regulators, and other stakeholders can help foster an ecosystem that supports the growth and adoption of the blockchain network. Scalability has long been a challenge for blockchain technology, particularly in the context of public blockchains. As the number of users and transactions on a blockchain network increases, the resources required to maintain and validate the network also grow, leading to slower transaction times and increased costs. So, several solutions are used and developed to address this issue:

- Layer 2 approach: Plasma for Ethereum is built on top of the existing blockchain infrastructure, enabling faster and more cost-effective transactions without sacrificing security.
- Sharding: This approach divides the blockchain network into smaller, more manageable pieces called "shards." Each shard processes its transactions independently, increasing throughput and reducing congestion.
- Proof-of-Stake consensus algorithms: Switching from Proof-of-Work to Proof-of-Stake can improve scalability by reducing the computational power needed to maintain the network while ensuring security and decentralization.

Figure 8. Two blocks are connected via the previous block pointer.



In the previous stage, the inputs were the organization data with seals, and the outputs were a block or a group of blocks that contained the encrypted digest. But, this block needs approval to be appended in the blockchain platform via the ledger's log. Therefore, the primary role of this phase is to register the concerned block after performing the authentication process to verify its identity. So, Algorithm 1 determines each block's signature by ensuring that the encrypted digest encodes the original message with the secret key. To determine the identity of the source of information, we need three steps:

- Step 1: If the source chooses domain parameters (p, q and g), where p and q are N bits prime numbers. Then, the source can determine the private ($\mathrm{prk_{BID}}$) and public ($\mathrm{puk_{BID}}$) keys for the concerned Block ID using RSA or digital signature algorithm (DSA). Then, the extracted $\mathrm{puk_{BID}}$ is compared with the public key provided during the request.
- Step 2: Applying the proposed Algorithm 1 that accepts $\mathrm{puk_{BID}}$, $\mathrm{prk_{BID}}$ and original data ($\mathrm{M_{BID}}$) as input. Then, it produces a signature ($\mathrm{S_{BID}}$) by singing Eq. (1) as output. Hv is the hash value. k is a random value from 1 to q-1.

$$\mathrm{S_{BID}} = (\mathrm{puk_{BID}}, \mathrm{prk_{BID}})\mathrm{Sign}(\mathrm{Hv_{BID}}, \mathrm{k}, \mathrm{M_{BID}} \qquad (1)$$

- Step 3: Applying the proposed Algorithm 2 that takes ($\mathrm{sign_{BID}}$, $\mathrm{puk_{BID}}$, $\mathrm{puk_{BID}}$and $\mathrm{M_{BID}}$) as input. Then, the concerned block is accepted with an access token or rejected as output. Fig. 9 shows the sequence diagram for granting access to append a new block into the blockchain platform.

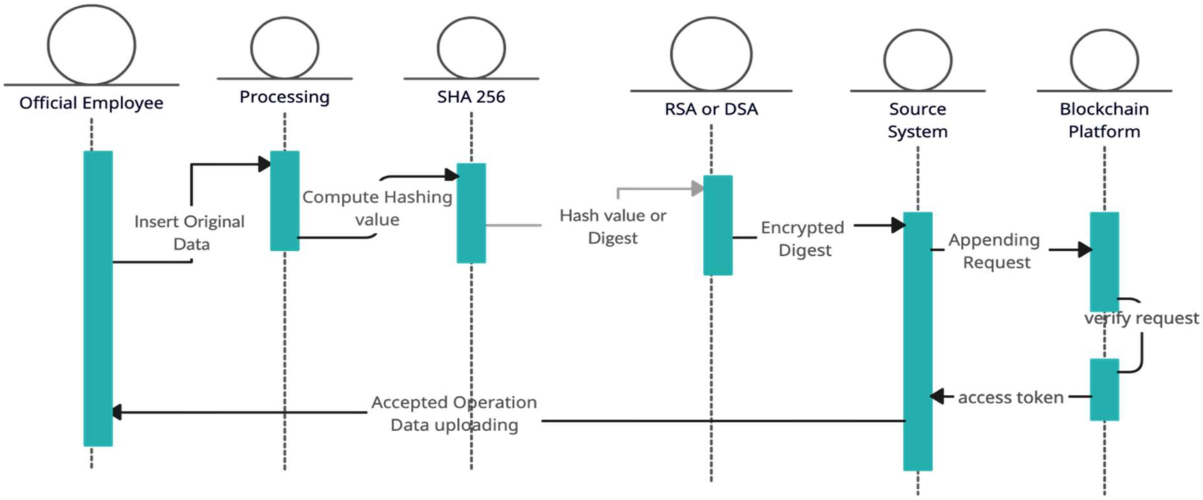


Figure 9. The Sequence Diagram For Granting Access To Append New Blocks Into The Blockchain Platform.

Algorithm 1: Generate block signature

```
ıput: $BID, puk_{BID}, prk_{BID}, prime\ q, M_{BID}$
Output: Signature $S$
Start Procedure
Initial $S \leftarrow null$
$if\ BID\ then$
    $Hv_{BID}$= SHA.new ($M_{BID}$). digest ()
    $k$= random. StrongRandom (). rand (1,  $puk_{BID}.q - 1$)
    $S1_{BID} = (puk_{BID})\ Sign(Hv_{BID}, k, M_{BID})$
    $S2_{BID} = (prk_{BID})\ Sign(Hv_{BID}, k, M_{BID})$
    $S_{BID} = S1_{BID} \vee S2_{BID}$
    Return $S_{BID}$
End IF
End Procedure
```

4.3 Verification Phase

In this phase, the destination must verify the document's seal. So, the destination can grant access to the seal on the document and QR code. Firstly, the stamp seal is processed using the same steps at the source, such as preprocessing, detection, feature extraction, encoding, and normalization. Then classify the stamp seal imprint as authentic or fraudulent using the SVM method. Then, Compare the model's classifications against the true labels. If the model classifies an authentic imprint as fraudulent, this is a Type I error (false positive). If the model classifies a fraudulent imprint as authentic, this is a Type II error (false negative). The following steps can be used to verify the seal on the smart document, as shown in Fig. 10:

- Step 1: Both seal on a smart document and the QR code generated by the source are received by the destination.
- Step 2: The QR code is scanned to get a unique ID to grant access and retrieve the unique block using this ID.
- Step 3: After successfully granting access to the unique block from the blockchain platform, the destination uses the public key associated with this block to decrypt the hash value (digest).
- Step 4: The received seal is is processed using the same steps at the source, such as preprocessing, detection, feature extraction, encoding, and normalization. Then classify the stamp seal imprint as authentic or fraudulent using the SVM method. Then it is entered on the same hash function to produce the new hash value (news digest).
- Step 5: The outputs from steps 3 and step 4 are compared together.
- Step 6: The seal or smart document is accepted if the comparison output is equal. Otherwise, the seal or smart document is rejected.

Algorithm 2: Verify request and grant access

Input: $BID, puk_{BID}, prk_{BID},$ Signature S, source, M_{BID}
Output: Status (SS) and access token (AT)

```
Start Procedure
 Initial $SS \leftarrow reject, AT \leftarrow 0$
 $if\ \ puk_{BID} \wedge prk_{BID} \in S\ \ then$
    $policy_{BID}$= JSON.GetPolicy(Source.$BID$)
    $Ledger_{Log}.update(policy_{BID})$
    $AT = rand$ ()
    $issue_{time} = time.now()$
    $expire_{tim} = 3600$
    SS = **Approved**
    **Return** $AT\ and\ SS$
 End IF
End Procedure
```

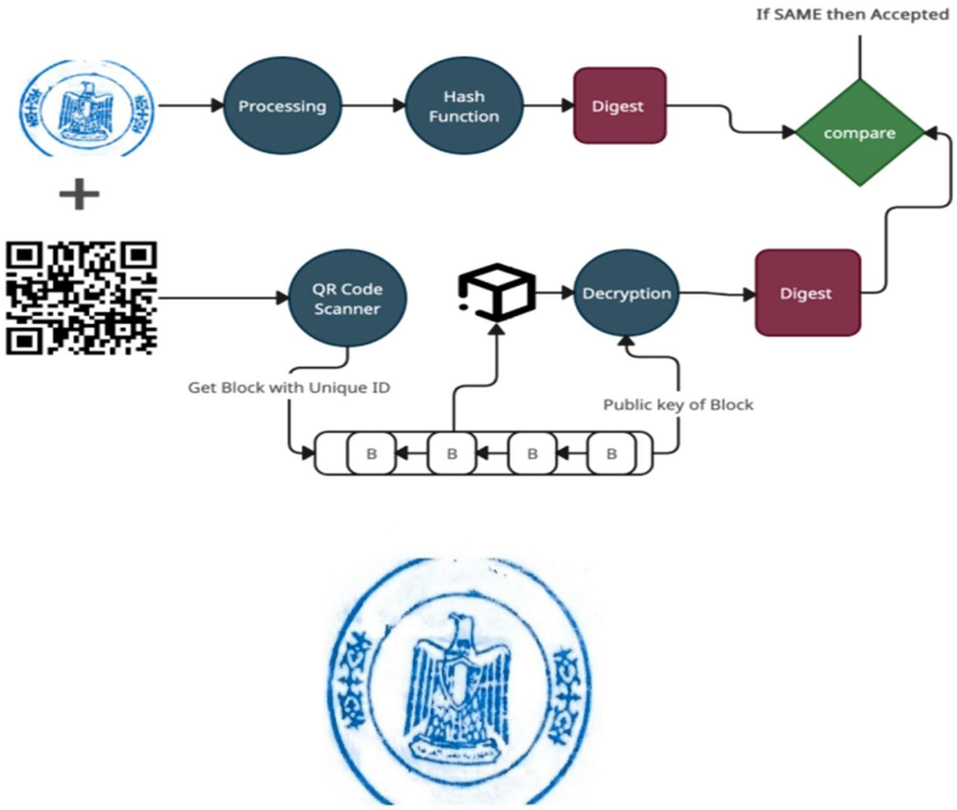


Figure 10. The steps of the verification phase.

5. EXPERIMENTAL RESULTS

5.1 Dataset

We have used many images of different Egyptian governmental stamp seal imprints, which we are extract results, and detect fraud. This is a real sample of the Egyptian governmental Stamp Seal, as represented in Fig.11.

5.2 Implementation Environment

At the source phase, we used a system with a hardware configuration listed in Table III. At the blockchain platform, we used different blockchain platforms, such as the Azure blockchain workbench, Ethereum, and Hyperledger platform. These tools permit inventors to deploy a blockchain ledger with a collection of appropriate services to evaluate different parameters on the blockchain platform, such as CPU, network, and disk usage. This manuscript used different numbers (5, 50, 100, and 200) of nodes or peers. Many programs were operated during the verification phase, such as Oracle virtual box 6.0, Kali Linux 2018.2 vbox-i386, x, QR-Code studio 1.0, and the Openssl library in Linux. The digital certificate was constructed using the 4096-bit RSA private key. After the digital certificate generation, the digital certificate and a unique ID of the smart document or stamp seal imprint file are delivered to the QR code generator.

Figure 11. The sample of the Egyptian governmental stamp seal imprints after erasing all its data because of confidentiality.

Table 3. The source hardware configuration.

Item	Specification
CPU	Intel Core ® i7 2.4 GHz
RAM	16 GB RAM
Hard disk	1 TB
Operating System	Windows 10 , CentOS

5.3 Evaluation Metrics

This manuscript's experimental data is more than 1 million transactions from more than 400 blocks. We compare the creation time of block and transaction throughput creation time of our proposed model with the Bitcoin model, which is remarkably better than Bitcoin. The following metrics are used to evaluate our model:

- QR code Readability: The QR code readability depends on different parameters, such as file size, compression rate, hash length, and execution time. Note that the input data can be of any size, while the output hash value is a fixed ratio of the original data.

- Transaction Throughput: It is the rate at which the blockchain executes valid transactions in a specified time period.

$$\text{Transaction}_{\text{throughput}} = \frac{\text{Total committed Transactions}}{\text{Total time of seconds}} \qquad (2)$$

- Creation time of block: It is time to create a new block in that blockchain. The identical amount of time it carries for block generation differs and relies on the ordeal of the hash. Bitcoin takes around 10 minutes, while Ethereum only takes around 14 seconds.

- Read throughput: It calculates how numerous read processes are conducted in a defined time period. Read processes differ from transactions in that the state has no change.

$$\text{Read}_{\text{throughput}} = \frac{\text{Total Read Operation}}{\text{Total time of seconds}} \qquad (3)$$

- Query: It is the ability to run ad-hoc operations or searches against the dataset contained within the blockchain.

- Accuracy: The proportion of true results (both true positives and true negatives) in the total number of cases examined. This metric used in the verification phase.

$$\textbf{Accuracy} = \frac{\boldsymbol{True\ Positives + True\ Negatives}}{\boldsymbol{Total\ Cases}} \qquad (4)$$

- True Positive Rate (TPR): Also known as sensitivity, recall, or hit rate, it measures the proportion of actual positives that are correctly identified. This metric used in the verification phase.

$$\mathbf{TPR} = \frac{\textit{True Positives}}{\textit{True Positives+False Negatives}} \quad (5)$$

- False Positive Rate (FPR): Also known as fall-out, it measures the proportion of actual negatives that are incorrectly identified as positives. This metric used in the verification phase.

$$\mathbf{FPR} = \frac{\textit{False Positives}}{\textit{False Positives} + \textit{True Negatives}} \quad (6)$$

5.4 Results

Table IV shows the result of test case I with some configurations such as file size (62960 bit), compression ratio, and hash length. Table V shows the result of test case II with some configurations such as File size (77630 bits), compression ratio, and hash length. Table VI shows the result of test case III with some configurations such as File size (12715 bits), compression ratio, and hash length. Table VII shows the result of test case IV with some configurations such as File size (84947 bits), compression ratio, and hash length.

Table 4. Result of the test case I with the file size of 62960 bits.

Iteration	180	150	120	115
Compression rate	16	32	48	64
Hash length	15	31	48	64
Execution Time (seconds)	0.886	0.926	0.933	0.918
QR				

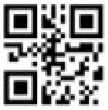
Table 5. Result of the test case II with the File size of 77630 bits.

Iteration	162	125	105	93
Compression rate	16	32	48	64
Hash length	16	32	46	63
Execution Time (seconds)	1.038	1.024	1.015	1.003
QR				

Table 6. Result of the test case III with the File size of 12715 bits.

Iteration	177	140	118	110
Compression rate	16	32	48	64
Hash length	15	32	46	64
Execution Time (seconds)	0.758	0.714	0.626	0.583
QR				

Table 7. Result of the test case IV with the file size of 84947 bits.

Iteration	225	190	182	173
Compression rate	16	32	48	64
Hash length	15	32	48	64
Execution Time (seconds)	1.373	1.296	1.227	1.188
QR				

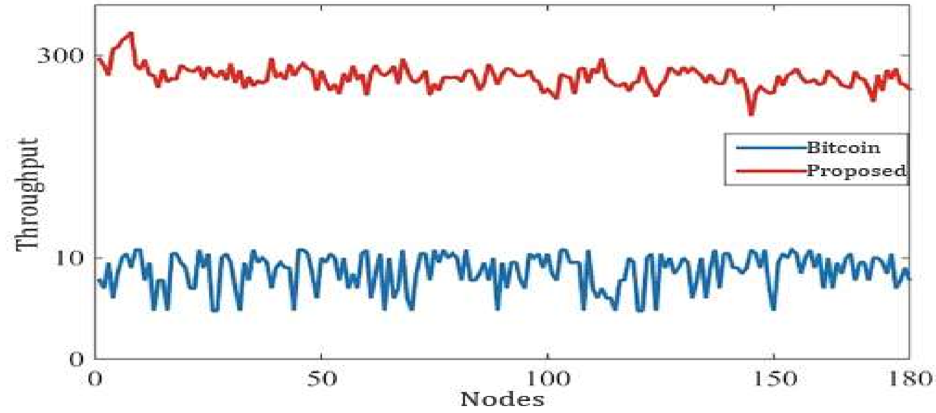


Figure 12. Transaction Throughput.

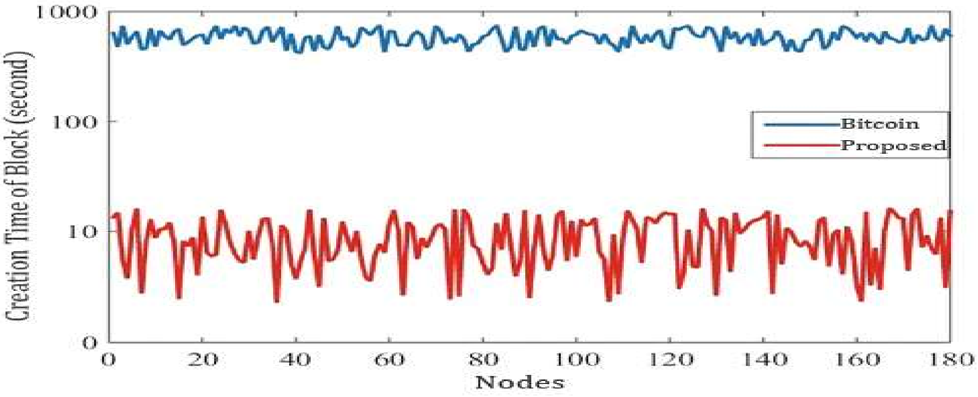


Figure 13. Creation time of the block.

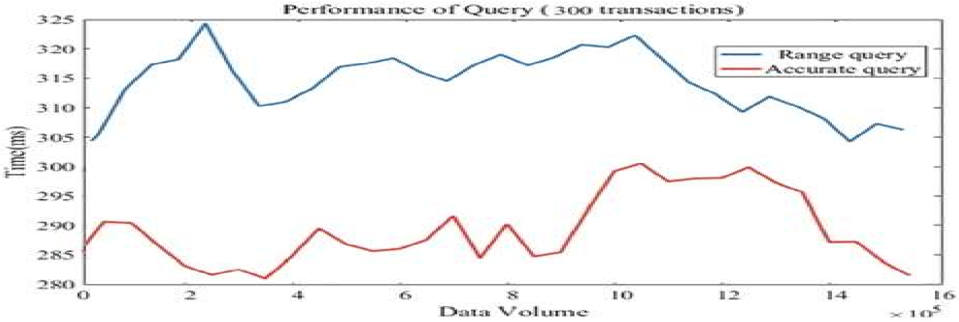


Figure 14. Query time of 300 Transactions.

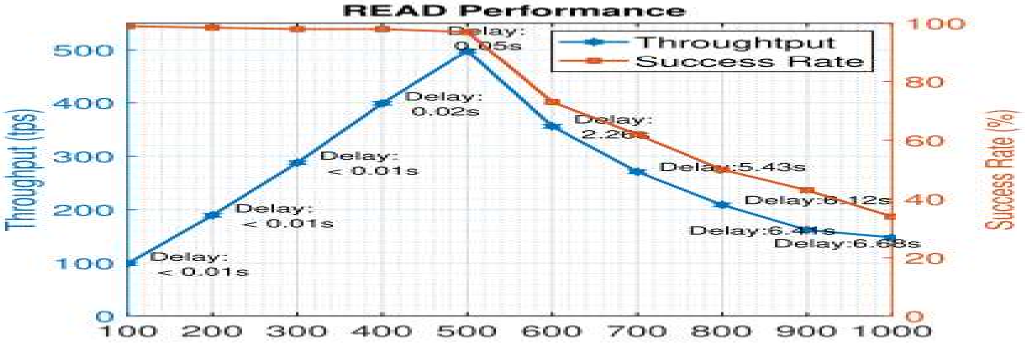


Figure 15. Read performance using the different workloads.

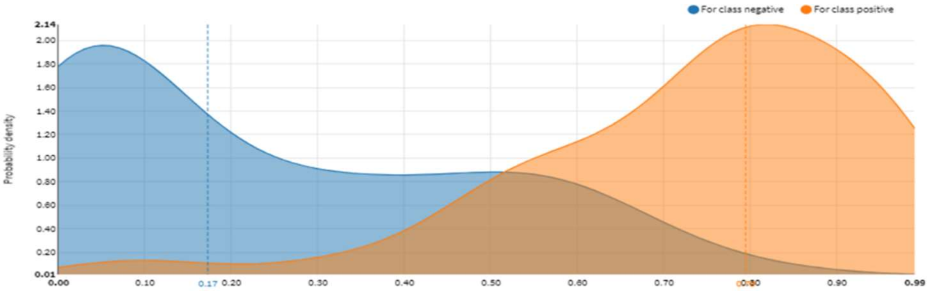


Figure 16. Density chart for SVM.

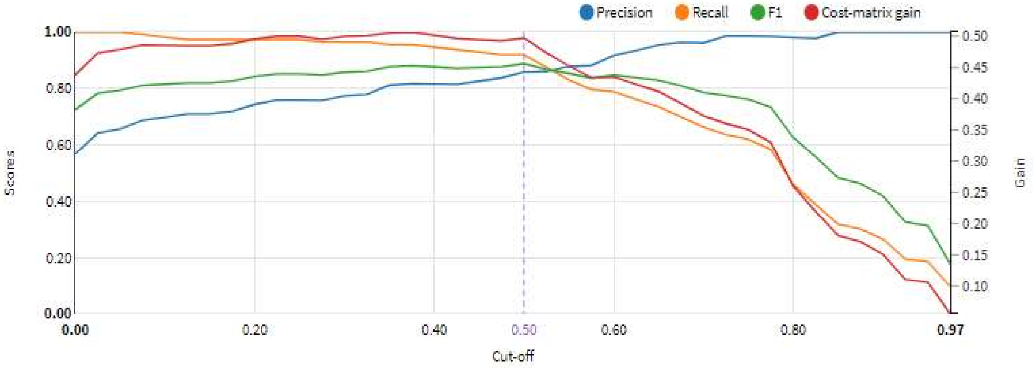


Figure 17. Cut-off chart for SVM model.

5.5 Discussion

Because our data needs a high level of security, high availability, and fast storage system, we used our proposed model to ensure data is securely available anywhere and at any time. An appropriate data compression method was also used to keep transactions fast and easy to store. The quick response code was also used to link the secured electronic system (Full digitalization) with the traditional paper system (partial digitalization) to obtain the advantages of the two systems. We have done many experiments and identified some test cases. Test files were uploaded to evaluate the accuracy, including Egypt's governmental stamp seal imprints in different sizes. For example, we compared different test cases with a fixed compression threshold value of 64.

In test case I, we found that when a file with a size of 62960 bits was used, the resulting hash size (64 digits) needed to complete this hash is 115 cycles with an execution time is 0.918 seconds, as shown in Table IV. However, in test case II, when we used a file with a size of 77630 bits, the resulting hash size (63 digits) needed to complete this hash is 93 cycles with an execution time is 1.003 seconds, as shown in Table V. In this case, we found that the time was increased, and the hash size was reduced slightly compared with the previous test case according to the file size.

Besides, in test case IV, when we used a file with a size of 84947 bits, the resulting hash size (64 digits) needed to complete this hash is 173 cycles with an execution time is 1.188 seconds, as shown in Table VII. The proposed robust model uses one-way encryption to generate a secure QR code and ensure data integrity. Various nodes or peers were used in this manuscript. Practically, we use transaction throughput as an evaluation metric.

We found that the transaction throughput approximated three hundred per second, as shown in Fig. 12. Also, the creation time of a block was compared with Bitcoin, which Bitcoin gets an average of seven transactions per second, as demonstrated in Fig. 13. However, the query range and several query statements were used to calculate the average query time. Fig.14 shows the system's efficiency by calculating the query's performance using 300 transactions. In the verification phase, we achieve accuracy 98%, TPR 96%, FPR 3%. Fig.16 and fig. 17 represent the density and cut-off charts of SVM model respectively. In Fig.18, the final representation of the secured document is represented as an output on the printed document.

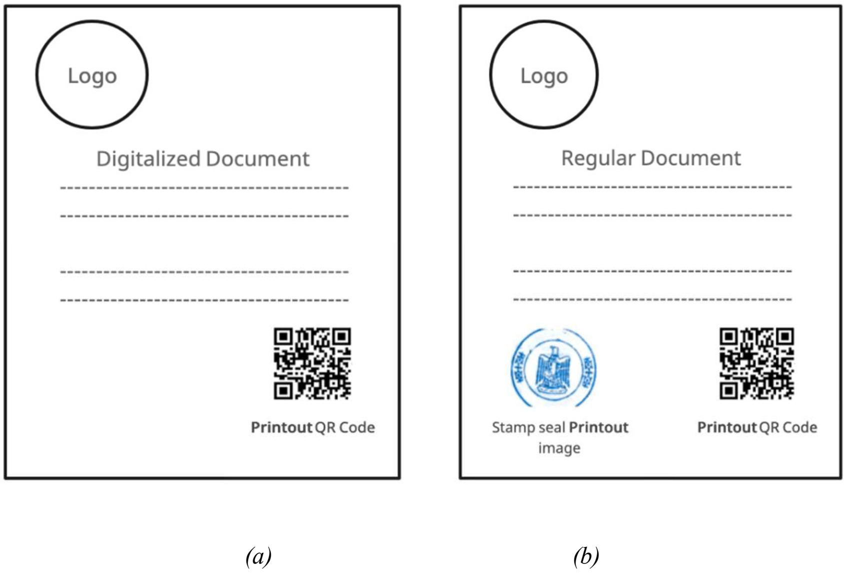


Figure 18. The final representation of the secured document. (a) Full digitalization for securing digital document. (b) Partial digitalization for securing physical document.

As shown in Fig.18, we follow in full digitalization all the securing process as in parital digitalization including document data creation, document hashing, blockchain integrity, generating QR code, verification process, QR code decoding and blockchain check. The only difference between full and partial digitalization is in full digitalization no need to have physical document in our hand (paper less environment), but in partial digitalization we have a physical document in our hand. Partial digitalization is a step towards full digitalization.

The gravity of the issue: We have provided comprehensive data and real-world examples illustrating the increasing incidence of document forgery and its implications for personal, corporate, and national security. This highlights the urgency of developing more secure verification systems.

Theoretical foundations: We have strengthened our discussion of the theoretical principles that guide our approach, including the principles of cryptography, decentralized storage, and data integrity. We have also referenced key studies that have identified the vulnerabilities of current document verification systems and the potential of blockchain technology in addressing these challenges.

Justification for attention: The manuscript now clearly articulates why the problem of document forgery necessitates immediate academic and practical intervention. We underscore the technological lag in current systems and the societal costs of inaction, thereby framing our research as a response to a critical vulnerability in data security.

Impact and implications: We have elaborated on the potential impact of our proposed solution on various stakeholders, including governments, businesses, educational institutions, and individuals. By doing so, we have connected the conceptual basis of our work with tangible outcomes that resonate with a broad audience.

6. CONCLUSION

The proliferation of counterfeit documents featuring forged stamp seal imprints has emerged as a formidable challenge with considerable security and societal implications. Governments' reliance on centralized systems globally has been fraught with issues concerning data protection and the integrity of stamp seal imprints. These systems are plagued by vulnerabilities, including susceptibility to single points of failure, data inaccessibility due to systemic failures, and susceptibility to Denial of Service (DoS) attacks. This research has created an innovative strategy for bridging the gap between traditional paper-based systems and a fully digitized environment. Our approach facilitates the verification of documents and their contents and reinforces their authenticity through a comprehensive integration of multiple indicators, such as stamp seal images, signatures, watermarks, and unique textual patterns, all underpinned by a robust feature extraction and analysis protocol. At the core of our model lies the strategic employment of data encryption and a decentralized blockchain network, which collectively ensure the security of stamp seal imprints and intelligent documents. Additionally, the generation of QR codes offers expedited and fortified access to the blockchain record, further solidifying the model's reliability through the use of one-way encryption to preserve data integrity. An empirical assessment of our model underscores its efficacy, as evidenced by a remarkable 98% accuracy and security rate in verifying stamp seal imprints and documents while significantly outpacing current systems in retrieval speeds. Looking to the horizon, the current model's dual-faceted design for securing physical and fully digital documents presents an avenue for expanding a broader spectrum of documents, including but not limited to digital certificates, legal contracts, and government-issued licenses.

Future research should delve into integrating diverse datasets, such as those emanating from the Internet of Things (IoT). The confluence of our model with IoT devices promises to unlock the potential for real-time verification and validation of documents and their seals. Moreover, as we chart the course forward, enhancing the system's scalability and efficiency is imperative, particularly in the wake of expanding document quantities and user bases.

DECLARATIONS

- Ethics approval and consent to participate: Not applicable.
- Consent for publication: Not applicable.
- Competing Interests: Authors have no competing interests.
- Funding: Not applicable. This research received no specific grant from any funding agency.
- Authors' Contributions: Conceptualization, M.W., M.M.E., A.A.E., and M.E.; methodology, M.W. and M.M.E.; database search, data curation, assessment of bias; writing—original draft preparation, M.W. and M.M.E..; writing—review and editing, M.M.E., A.A.E., and M.E.; supervision, M.M.E., A.A.E., and M.E.. All authors have read and agreed to the published version of the manuscript. All authors read and approved the final manuscript.
- Acknowledgments: Not applicable.
- Availability of data and material: on request.

REFERENCES

[1] Lin SY, Zhang L, Li J, Ji L li, Sun Y. A survey of application research based on blockchain smart contract. Wirel Networks, Springer; 2022, 28:635–90.

[2] Haveri P, Rashmi UB, Narayan DG, Nagaratna K, Shivaraj K. EduBlock: Securing Educational Documents using Blockchain Technology. 2020 11th Int Conf Comput Commun Netw Technol ICCCNT 2020. Institute of Electrical and Electronics Engineers Inc.; 2020.

[3] Zheng W, Zheng Z, Chen X, Dai K, Li P, Chen R. NutBaaS: A Blockchain-As-A-Service Platform. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2019,7:134422–33.

[4] Wang M, Xu C, Chen X, Zhong L, Wu Z, Wu DO. BC-Mobile Device Cloud: A Blockchain-Based Decentralized Truthful Framework for Mobile Device Cloud. IEEE Trans Ind Informatics. IEEE Computer Society; 2021,17:1208–19.

[5] Alhazmi HE, Eassa FE, Arabia S. BCSM: A BlockChain-based Security Manager for Big Data. IJACSA) Int J Adv Comput Sci Appl, 13:2022.

[6] Sayeed S, Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Appl Sci 2019, Vol 9, Page 1788, 9:1788.

[7] Agung AAG, Handayani R. Blockchain for smart grid. J King Saud Univ - Comput Inf Sci. Elsevier; 2020.

[8] Alghamdi TA, Ali I, Javaid N, Shafiq M. Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism Based on Blockchain. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020,8.

[9] Singhal A, S. Pavithr R. Degree Certificate Authentication using QR Code and Smartphone. Int J Comput Appl. Foundation of Computer Science; 2015,120:38–43.

[10] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. Smart Contract-Based Access Control for the Internet of Things. ArXiv. 2018, 1802.04410.

[11] Mengelkamp, E., Notheisen, B., Beer, C. et al. A blockchain-based smart grid: towards sustainable local energy markets. Comput Sci Res Dev, 2018, 33, 207–214.

[12] *Hawlitschek, F., Teubner, T., Adam, M.T., Borchers, N.S., Moehlmann, M., & Weinhardt, C. Trust in the Sharing Economy: An Experimental Framework. I*nternational Conference on Interaction Sciences, 2016.

[13] Alnahari, M.S.; Ariaratnam, S.T. The Application of Blockchain Technology to Smart City Infrastructure. *Smart Cities* 2022, *5*, 979-993.

[14] Guo, X.; Zhang, G.; Zhang, Y. A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing: A Framework, Challenges and Future Research Directions. *Sensors* 2023, *23*, 155.

[15] Kshetri, Nir. Blockchain’s roles in meeting key supply chain management objectives. International Journal of Information Management, 2018, 39, 4, 80-89.

[16] Casino, F., Dasaklis, T. K., & Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 2019, 36, 55-81.

[17] Zhu, P.; Hu, J. ; Zhang, Y. & Li, X. A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability. *IEEE Access*, 2020, 8, 184256-184272.

[18] Grech, A., & Camilleri, A. F. Blockchain in education. In Joint Research Centre, 2017.

[19] Al-Saqaf, W., & Seidler, N. J. Blockchain technology for social impact: opportunities and challenges ahead. Journal of Cyber Policy, 2017, 2, 3, 338-354 .

[20] Yermack D. Corporate Governance and Blockchains. Rev Financ. Oxford Academic; 2017, 21:7–31.

[21] Sullivan C, Burger E. E-residency and blockchain. Comput Law Secur Rev. Elsevier Advanced Technology, 2017;33:470–81.

[22] Pongnumkul S, Siripanpornchana C, Thajchayapong S. Performance analysis of private blockchain platforms in varying workloads. 2017 26th Int Conf Comput Commun Networks, ICCCN 2017. Institute of Electrical and Electronics Engineers Inc.; 2017.

[23] Xu Y, Zhao S, Kong L, Zheng Y, Zhang S, Li Q. ECBC: A High Performance Educational Certificate Blockchain with Efficient Query. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics), Springer, Cham; 2017, 10580 LNCS:288–304.

[24] Saha G. DSign digital signature system for paperless operation. Proc 2017 IEEE Int Conf Commun Signal Process ICCSP 2017. Institute of Electrical and Electronics Engineers Inc.; 2018;2018-January:324–8.

[25] Nguyen DH, Nguyen-Duc DN, Huynh-Tuong N, Pham HA. CVSS: A blockchainized certificate verifying support

system. ACM Int Conf Proceeding Ser. Association for Computing Machinery; 2018;436–42.

[26] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate. Proc 4th IEEE Int Conf Appl Syst Innov 2018, ICASI 2018. Institute of Electrical and Electronics Engineers Inc.; 2018;1046–51.

[27] Khan SN, Shael M, Majdalawieh M. Blockchain technology as a support infrastructure in E-Government evolution at Dubai economic department. PervasiveHealth Pervasive Comput Technol Healthc. ICST; 2019;124–30.

[28] Xu C, Yang H, Yu Q, Li Z. Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain. 2019 IEEE 5th Int Conf Comput Commun ICCC 2019. Institute of Electrical and Electronics Engineers Inc.; 2019,1237–42.

[29] V S. SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN. J Ubiquitous Comput Commun Technol. Inventive Research Organization; 2019,01:45–54.

[30] Geneiatakis D, Soupionis Y, Steri G, Kounelis I, Neisse R, Nai-Fovino I. Blockchain Performance Analysis for Supporting Cross-Border E-Government Services. IEEE Trans Eng Manag. Institute of Electrical and Electronics Engineers Inc.; 2020,67:1310–22.

[31] Bharadi VA, Ghag PP, Chavan SR, Gawas SS, Kazi A. Integrating Blockchain with Local Public Service System. Springer, Singapore; 2020, 93–103.

[32] Xie R, Wang Y, Tan M, Zhu W, Yang Z, Wu J, et al. Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System. IEEE Internet Things Mag. Institute of Electrical and Electronics Engineers (IEEE); 2020,3:44–50.

[33] He H, Zheng L han, Li P, Deng L, Huang L, Chen X. An efficient attribute-based hierarchical data access control scheme in cloud computing. Human-centric Comput Inf Sci [Internet]. Springer Science and Business Media Deutschland GmbH; 2020, 10:1–19.

[34] Sun J, Yao X, Wang S, Wu Y. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020;8:59389–401.

[35] Gao Y, Pan Q, Liu Y, Lin H, Chen Y, Wen Q. The Notarial Office in E-government: A Blockchain-Based Solution. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2021, 9:44411–25.

[36] Das, M., Tao, X., Liu, Y., & Cheng, J. C. A blockchain-based integrated document management framework for construction applications. Automation in Construction, 133, 104001.

[37] Anwar, Aang Solahudin, Untung Rahardja, Anggy Giri Prawiyogi, Nuke Puji Lestari Santoso, and S. Maulana. "iLearning Model Approach in Creating Blockchain Based Higher Education Trust." Int. J. Artif. Intell. Res 6, no. 1, 2022.

[38] A. K. Sharma, D. M. Sharma, N. Purohit, S. A. Sharma, and A. Khan, "Blockchain Technology," Blockchain Technology, pp. 163–180, Feb. 2022.

[39] A. Pambudi, S. Purnama, T. Ayuninggati, N. P. L. Santoso, and A. Oktariyani, "Legality On Digital Document Using Blockchain Technology: An Exhaustive Study," in 2021 Sixth International Conference on Informatics and Computing (ICIC), 2021, pp. 1–6.

[40] Odeh, S., Samara, A., Rizqallah, R., & Shaheen, L. Digital Identity Using Hyperledger Fabric as a Private Blockchain-Based System. In Blockchain and Applications, 4th International Congress, 2023, pp. 153-161. Cham: Springer International Publishing.

[41] Biswas, A. K., Dasgupta, M., & Ray, S. Secure Management of Digital Academic Certificates Using Blockchain Technology. In Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND, 2023, pp. 805-813. Singapore: Springer Nature Singapore.

[42] Pu, S., & Lam, J. S. L. The benefits of blockchain for digital certificates: A multiple case study analysis. Technology in Society, International Journal of Information Management2023, 72, 102176.

[43] Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J., & Trivedi, M. C. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Information Sciences, 2023, 629, 703-718.

[44] Hikal NA, El-Gayar MM. Enhancing IoT botnets attack detection using machine learning-IDS and ensemble data preprocessing technique. Lect Notes Networks Syst, Springer, 2020, 114:89–102.

[45] Shah, R.; Kotecha, K. Blockchain-based framework for improving government services and citizen experience in a smart city. Wireless Personal Communications, 2021, 118(1), 537-554.

[46] Pažur, I.; Vlahinić, S. Blockchain-based system for digital document verification. Information Systems Frontiers, 2021, 1-17.

[47] Khatoon, A. A secure and efficient digital identity management system for smart cities using blockchain technology. Computers, Materials & Continua, 2021, 67(2), 2189-2203.

[48] Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain for health research: Case study in a genomics and public health registry. Journal of Medical Internet Research, 2021, 23(6), e22740.

[49] Chen, X.; Ji, J.; Luo, Y.; Liao, X. A survey on consensus mechanisms and mining management in blockchain networks. IEEE Access, 9, 2021, 35379-35398.

[50] Chouhan, V.; Singh, S. K. A blockchain-based digital document verification system for education certificates. Procedia Computer Science, 2020, 167, 1191-1200.

[51] Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, 2015.

[52] Khan, S.; Shael, M.; Majdalawieh, M.; Nizamuddin, N.; Nicho, M. Blockchain for Governments: The Case of the Dubai Government. Sustainability 2022, 14, 6576.

[53] Al-Kodmany, K. The New Arab Urbanism in the Middle East and North Africa (MENA). Urban Science, 2018, 2(3), 74.

[54] Cardullo, P.; Kitchin, R. Being a ‘citizen’ in the smart city: Up and down the scaffold of smart citizen participation in Dublin, Ireland. GeoJournal, 2019, 84(1), 1-13.

[55] Mohammed R, Abed E, Elgayar M. Comparative study between metaheuristic algorithms for internet of things wireless nodes localization. International Journal of Electrical and Computer Engineering (IJECE); 2022; 12:660–8.

[56] Fetooh H, El-Gayar M, Aboelfetouh A. Detection Technique and Mitigation Against a Phishing Attack. International Journal of Advanced Computer Science and Applications. 2021;12:177–88.

[57] El-gayar, M.M; Soliman, H; Meky, N. A comparative study of image low level feature extraction algorithms. Egyptian Informatics Journal, 2013, 4,2, 175-181.

[58] Mohammed Ali A, Farhan AK. Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document. IEEE Access. Institute of Electrical and Electronics Engineers Inc.2020, 8:27448–58.

[59] Fan C, Ghaemi S, Khazaei H, Musilek P. Performance Evaluation of Blockchain Systems: A Systematic Survey. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020;8:126927–50.