KJMS 2026 VOL.8 (1): 195-208

KDU Journal of Multidisciplinary Studies (KJMS)
Volume 8. Issue 1 July 2026
DOI: https://doi.org/10.4038/kjms.v8i1.263

VERIFICATION OF LEGAL DOCUMENTS IN JUDICIAL SERVICES USING BLOCKCHAIN TECHNOLOGY

D.S.M. Jayasooriya[1], N.M.A.P.B. Nilwakka[2] and K.M.D. Prashadika[2]

Department of Physical Sciences, Faculty of Applied Sciences, Rajarata University of Sri Lanka, Mihintale, Sri Lanka[1].
Department of Computer Sciences, Faculty of Applied Sciences, Rajarata University of Sri Lanka, Mihintale, Sri Lanka[2]

ABSTRACT

A safe and effective way to validate legal documents is becoming more important, as document forgery appears to be an increasing problem within Sri Lanka's legal system. Conventional procedures that rely on manual verification are challenging, prone to corruption, and susceptible to human error. This paper proposes a blockchain-based method for verifying legal documents to address these challenges. In the proposed approach, a SHA-512 hash value is generated for the entire content of the uploaded document, as discussed in the research methodology, and stored on the blockchain. Additionally, a QR code that serves as a digital signature is created containing the verifiers *and verification details. This method also utilizes Ethereum smart contracts for storing the hash values, ensuring decentralization and immutability. The system demonstrates 91% accuracy for documents written in Sinhala script, due to difficulties in recognizing some Sinhala characters, and 100% accuracy for documents written in English script. The overall accuracy for both Sinhala and English scripted documents is 95%. This study aims to enhance document integrity using advanced cryptographic hashing techniques. It also identifies challenges specific to the judicial sector when exploring blockchain applications in real-world legal contexts. The proposed system is well-suited for high-security applications in Sri Lankan court services and It would make them perfect. However, limitations exist in terms of document types and classifications, particularly for documents written in Sinhala and English. Future work will focus on improving Sinhala document verification, incorporating user authentication methods such as passkeys and OTP, and developing the system as a mobile application*

KEYWORDS: Legal Document Verification, Blockchain, Sha-512 Hashing, Smart Contract, QR Digital Signature

Corresponding Author: D.S.M. Jayasooriya email: shiharajayasooriya@gmail.com

https://orcid.org/0009-0001-8229-2283

1. INTRODUCTION

Document verification has become a crucial task in this era of digital technology. However, digital documents carry a great risk of forgery and misrepresentation. This has prompted researchers to discover new methods of document verification, and one such solution is the application of blockchain technology (Marella and Vijayan, 2020). Blockchain has been receiving considerable interest in recent years due to its potential in enabling digital transactions to become more secure and trustworthy. Decentralized and tamper-proof are a few of its features that qualify it as an excellent platform for document verification. By putting data on a blockchain, institutions can render documents tamper-proof and genuine, thereby establishing greater confidence and accountability (Marella and Vijayan, 2020).

Document authentication has gained prominence in many sectors, particularly in court services, banking sector and education and recruitment. It is necessary for employers, organizations, and governments to ensure the authenticity of important documents, and other certificates. This guarantees trust and avoids forgery. The traditional methods of verification, however, involve manual processes, which are prone to mistakes, time-consuming, and vulnerable to manipulation. There is one solution that has been created to address these problems, though -- blockchain technology. Through blockchain, one can significantly enhance the security and authenticity of document verification (Ghazali and Saleh, 2018).

The legal industry relies heavily on accurate document verification to maintain integrity. Traditional methods like manual inspection and relying on trusted third parties are vulnerable to forgery and inefficiency. Blockchain technology offers numerous benefits, including immutability, which ensures trustworthiness, and decentralization, which eliminates intermediaries, making processes more economical and efficient (Jitesh Choudhary, 2024). The authors suggest that blockchain technology can revolutionize court proceedings by providing a secure and efficient system for document verification. They argue that blockchain immutability can make court documents tamper-proof, ensuring the integrity of the judiciary. However, challenges like legal uncertainties and data privacy remain (Kumar et al., 2023).

Even with the advancement of blockchain technology for document verification in education, healthcare, construction and employment, these limited researches have engaged on the verification of legal documents within judicial services. The existing studies has focused on certificates (Saleh et al., 2020, Kumar et al., 2020, Ghazali and Saleh, 2018, A. Gayathiri, 2020), curriculum vitae (Marella and Vijayan, 2020), academic records (Shakan et al., 2021), and academic documents (Yashchyk et al., 2023, Chaniago et al., 2021), while the specific requirements of legal documents including, writes, contracts, deeds and court records remain uninvestigated. Furthermore, the most existing systems use SHA-256 hashing and not provide a user-friendly platform for identifying document verifiers (Kumar et al., 2020, Ghazali and Saleh, 2018). Therefore, there is a need for a secure blockchain-based legal document verification system specifically designed for Sri Lankan judicial services.

To address this research gap, this work guided the objectives as follows: (1) To ensure document integrity using hashing technology. (2) To integrate blockchain technology as a replacement for traditional databases in order to prevent operational disruptions such as decentralization challenges, data integrity issues, and smart contract failures. (3) To develop a system that ensures high accuracy. (4) To create user-friendly interfaces for accessing the developed system. (5) To explore how blockchain can streamline the verification process, reduce human error, and minimize delays compared to traditional methods.

To bridge this gap, this study is guided by the following core research questions: (1) How can blockchain technology be effectively utilized to address the challenges associated with document integrity verification? (2) What specific features of blockchain contribute to achieving the highest accuracy and speed in the verification process? (3) How does the use of a suitable hashing algorithm enhance the security and reliability of the document verification process within the proposed blockchain-based system? (4) How can hashing algorithms be

utilized in a blockchain-based solution to ensure the accuracy, authenticity, and trustworthiness of legal documents, considering that not all hashing algorithms are suitable for this purpose? (5) What mechanisms can be implemented within the blockchain system to identify the identity of the document verifier? The significance of this work is to provide a highly secure system that strictly reduces manual verification backlogs and enhances the integrity of judicial administrations.

1.1 Parameter Identification

The literature review has found a few key parameters commonly used in blockchain based document verification applications across educational, legal, construction, medical and other document domains. These parameters include authenticity, integrity, privacy, transparency, security, traceability, scalability, interoperability, accessibility confidentially and non-Jitesh Choudhary, 2024; Sharma and Khanna, 2023; S. Mthethwa, 2018; Prathmesh Sinkar, 2024; Moumita Das, 2022; Marella and Vijayan, 2020; Kumar et al., 2023; Ghazali and Saleh, 2018; Ghani et al., 2022; and A. Gayathri, 2020)

Further, the technologies such as digital signatures, stamps, cryptography hashing and self-sovereign identity mechanisms have been identified as most important components that would ensure the stoppage of authorizing modifications and document authenticity Wrong bracketing. Rectify them as done in the earlier instance.

From these parameters, authenticity, transparency, security and traceability were mainly identified as the most critical aspects for legal document verification. These parameters ensure that the documents remain verifiable, tamper-proof, traceable and secured from unauthorized modifications through their proceedings (Zhuk, 2023; S. Mthethwa, 2018; Kumar et al., 2023; and Jitesh Choudhary, 2024). Therefore, these parameters were chosen as the primary considerations for the proposed blockchain based legal document verification system.

1.2 Blockchain and traditional verification methods

Blockchain-based verification methods with traditional techniques had been compared. Traditional practices are typically human checks, such as physical checking, signature checks, and checks against official documentation. The processes are labour-intensive, wasteful of resources, and prone to human error (Ghazali and Saleh, 2018). Blockchain technology offers a decentralized, automated process for certificate validation, ensuring data integrity through cryptographic hashing. This process, combined with smart contracts, improves efficiency by reducing manual checks and enhancing data integrity, thereby reducing administrative demands (A. Gayathiri, 2020).

Blockchain technology offers a distributed, immutable bookkeeping system that enhances security and transparency. The decentralized nature of Blockchain eliminates the need for middlemen by presenting a peer-to-peer network where transactions are retained (Ghani et al., 2022). Blockchain technology offers significant advantages over traditional document verification processes, reducing time and cost by eliminating intermediaries, ensuring unique identification and timestamped documents (Prathamesh Sinkar, 2024).

Traditional methods tend to utilize central systems and intermediaries such as government organizations or third-party service providers in authenticating documents. SSI technology makes it possible for people to be in charge of their own identities and documents, reducing the requirement of centralized authorities. All documents are assigned a unique hash and linked to the user's self-sovereign identity, ensuring authenticity and integrity (Satybaldy et al., 2022).

The traditional verification of documents as time-consuming and prone to errors had been described. The process typically involves physical verification of the documents, comparison against records with issuing authorities in possession, and manual entry of data into central systems (S. Mthethwa, 2018).

Blockchain technology with traditional verification methods used to process legal documents are contrasted (Jitesh Choudhary, 2024). Traditional methods include manual processes, centralized data bases, and reliance on third parties such as notaries,

court clerks, or third-party verification service providers. The methods are linked with manual processes, paper records, and reduced transparency (Kumar et al., 2023).

It describes the typical document verification techniques in the judiciary, the usual document verification entailed several procedures, such as submission of the documents, their examination by officials, and verification using physical books (Zhuk, 2023). Automation and digital frameworks enhance productivity and cost reduction in educational institutions, while traditional methods like postal mail and emails are costly, time-consuming, and unreliable. (Dhyani et al., 2022).

Traditional methods of verifying university student and graduate data include manual checks, calling institutions, and third-party verification agencies. These are time-consuming, costly, and susceptible to error and fraud (Shakan et al., 2021).

When contrasted with traditional verification procedures, which necessitates direct contact between employers or institutions and the awarding organization--a resource and time-consuming task, Blockchain-based systems utilize immutable ledgers and hash functions to ensure data confidentiality and integrity, significantly reducing the need for incessant verification inquiries (Rasool et al., 2020).

1.3 Document verification processes

The blockchain system verifies the CV of candidates automatically by generating a unique cryptographic hash, validating digital signatures using private and public keys, and cross-verifying information with other documents. The system also communicates with existing HR systems, provides automatic alert to employers, and stores verified CVs permanently on the blockchain for future reference (Kumar et al., 2023).

The document verification processes proposed by Ghazali and Saleh using blockchain technology involve several steps. Candidates submit their graduation certificates digitally, which are recorded on the blockchain. A unique cryptographic hash of each certificate is generated and stored on the blockchain, ensuring data integrity and immutability. Digital signatures from both the candidate and the issuing institution are used for authentication (Jitesh Choudhary, 2024).

The document verification processes using blockchain technology outlined in detail: Each certificate is assigned a unique cryptographic hash, ensuring its integrity and immutability. Digital signatures from the issuing institutions and authorized personnel are used to authenticate the certificates. Smart contracts automate the verification process by cross-referencing the certificate data with other blockchain records or integrated databases, ensuring that the information is accurate and up-to-date. The verified certificates are stored permanently on the blockchain (Sharma and Khanna, 2023).

Documents are first digitized and hashed in the findings which, creating a unique digital fingerprint for each document. This hash is then recorded on the blockchain, where it can be securely and transparently accessed by authorized parties. When a document needs to be verified, the system checks the document's hash against the hash stored on the blockchain. If they match, the document is verified as authentic (Prathamesh Sinkar, 2024).

The system proposes and leverages blockchain technology to secure the verification process. When verification is required, the system compares the current document hash with the hash stored on the blockchain (A. Gayathiri, 2020). The presentation offers a blockchain-based approach to document verification processes that involves document digitization, hashing, and storage on a blockchain ledger. This secures the process, and it becomes accessible and compatible with future verification systems (Ghazali and Saleh, 2018).

Blockchain and cloud computing facilitate procedures for document verification. Hashes are included with soul bound tokens, unique identifiers of individual patients. Tokens are encrypted on the blockchain and are readable by authorized personnel for purposes of verification. The process identifies unauthorized alteration and prevents misuse or misrepresentation (Rasool et al., 2020).

The proposed blockchain-based document verification process involves digitizing educational documents, hashing them using cryptographic algorithms, and recording the hash along with metadata like issuance date and institution's identity (Yashchyk et al., 2023). Blockchain technology has also been applied in document verification in construction applications, starting with digitization of documents and hashing them using cryptographic algorithms. This allows authorized parties to access the blockchain ledger to confirm (Saleh et al., 2020).

The proposed framework ensures the authenticity of certificates by using cryptographic techniques to secure the data on the blockchain. Each certificate is linked to a unique cryptographic hash, that is nearly impossible to alter once it has been recorded on the blockchain. Educational institutions, employers, and other stakeholders can access and verify the authenticity of certificates in real-time, without the need for intermediaries. This reduces the time and cost associated with traditional verification methods, which often involve multiple steps and coordination between various parties (Moumita Das, 2022).

This process employs blockchain technology, 2D barcodes, OCR, and cryptographic hashing to provide document integrity. It requires documents to be scanned, a cryptographic hash to be generated, and the latter to be registered in the blockchain. An OCR scan verifies the authenticity of the document, leveraging smart contracts for effective verification (Chavan et al.). Document verification process using blockchain technology for the management of legal documents had discussed. The process begins with the digitization and hashing of legal documents, converting them into digital formats suitable for blockchain integration. Each document is hashed using cryptographic algorithms, creating a unique and immutable digital signature. This hash is recorded on the blockchain, along with metadata such as the issuer's identity (Zhuk, 2023), (Ghani et al., 2022).

The Ethereum blockchain secures electronic diploma and transcript documents by creating cryptographic hash values based on uniqueness, preventing hackers from accessing them. PDF files are used to ensure validity, and the SHA-256 method generates hash values and addresses. The technology automatically extracts and saves smart contract addresses (Imam et al., 2021). New dynamic document generation approach using an open-source platform which involves a web portal for document verification, where students upload their documents. A trusted third party authenticates the documents, storing the data securely on the blockchain. Once verified, the unique document ID or QR code is generated, which can be submitted to organizations for validation. The system uses a smart contract mechanism and can be executed in vulnerable environments to eliminate network attacks like DOS and MiM (Chavan et al.).

Ethereum smart contract is a blockchain scalable technique formed with Solidity programming language assistance. Remix IDE is used for solidity syntactic and linting checks, and document verification system for data definition. Web interface module provides blockchain integration to Web3.js framework (Satybaldy et al., 2022). The intended model uses techniques like hashing, digital signatures, peer-to-peer networking, cryptography, security for online storage, and proof of work for easy verification of uploaded files. It uses SHA-256 encryption and Ethereum Blockchain for securing data, with a user-friendly frontend (Shakan et al., 2021).

The authors propose a blockchain-based verification mechanism that simplifies document verification processes, such as certificate issuance, transmission, and verification. The system leverages decentralized storage and smart contracts, with additional certificate information and cryptographic hashes for purposes of validation, reducing human interaction and enhancing efficiency (Kumar et al., 2020). The proposed blockchain-based verification of university students' and graduates' data is achieved by creating a unique identifier using cryptographic techniques. The data is rehashed compared to the stored hash, and upon matching the two hashes, the record is verified as authentic and untampered (Shakan et al., 2021).

1.4 Current challenges in judicial document verification

The current judicial document verification process is plagued by critical issues, including reliance on manual steps, human factors, fraudulent behaviour,

and inefficiencies. Manual verification passes through multiple intermediaries, which means high cost and inconsistency. Discrepancy across jurisdictions complicates the process, and authenticity and integrity issues persist (Zhuk, 2023).

Blockchain technology's potential to improve court proceedings is faced with the handicaps of manual processes, variations, and inconsistencies, as well as the decentralized character of legal systems, which can lead to disparities and intricacies in cross-border legal proceedings (Ghani et al., 2022). The conventional legal systems are challenged to verify judicial documents because of complexities and inefficiencies such as manual processes, long errors, and susceptibility to forgery. A lack of solid security measures adds to the problem of ensuring documents' authenticity and integrity (Dhyani et al., 2022).

1.5 Benefits of blockchain for legal document verification

Blockchain technology can be used to improve verification of legal documents by eliminating middlemen and reducing risks of fraud. Its decentralized nature offers a tamper-proof record with unique hashes for each document. Cryptographic algorithms help identify forgery and enhance reliability. The immutable ledger allows approved stakeholders to follow a document's history, reducing conflicts and optimizing judicial efficiency (Zhuk, 2023), (Ghani et al., 2022).

Furthermore, blockchain facilitates the automation of document verification through the use of smart contracts, which execute predefined rules and conditions embedded within the blockchain network. This automation not only reduces the reliance on manual intervention but also streamlines the verification process, thereby expediting court operations and enhancing overall efficiency (Ghani et al., 2022).

2. METHODOLOGY

2.1 Data Collection and Analysing

2.1.1 Major Document Categories

- Writs
- Plaints and Complaints
- Affidavits
- Petitions
- Bills
- Summons
- Bail Bonds
- Deeds
- Contracts and Agreements
- Power of Attorney
- Notarial Acts
- Proxy
- Probate Documents
- Legal Notices
- Case Files
- Appeals
- Power of Attorney
- Notarial Acts

Category ‘Other’ was added because there are small documents which are submitted to the courts. For instance, in some cases, lawyers submit to the courts photocopies of original documents certified as true copies.

1.2 Identification of Verifier (Lawyer)

There are two ways to identify a lawyer.

- SC Enrolment No.

Supreme court enrolment number is given to a new lawyer after he/she is sworn in to the Supreme Court of Sri Lanka as Attorney-at-Law. This consists of six characters with five digits along with the capital letter A of the English alphabet.
Example: A00000

- Membership No.

Membership number which a lawyer receives after becoming a member of the Bar Association of Sri Lanka. This consists of five characters with four digits along the first capital letter of the surname of the concerned person.
Example: If the surname is Perera, the number will be P0000.

2.1.3 Identification of Verifier (Lawyer)

- Attorney-at-Law
- Commissioner for Oaths
- Company Secretary
- Notary Public
- Sworn Translator
- Proxy Lawyer
- Judge
- Barristers
- Paralegals

2.2 Flow Diagram

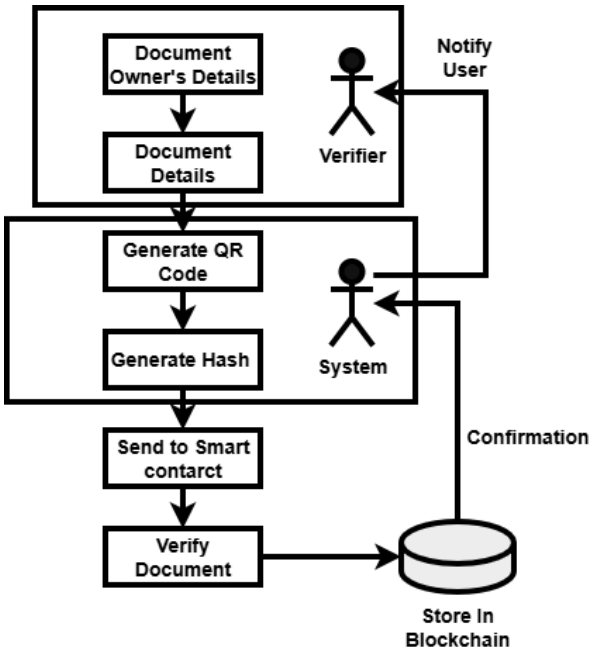

Figure 1: Flow diagram for methodology.

2.2.1 Digital Signature

A particular kind of signature that serves as identification evidence and is supported by a digital certificate is called as a digital signature. Once digital signatures can be confirmed and are cryptographically connected to the signed document, they are acknowledged as a more secured kind of electronic signature. For the suitable digital signature mechanism, a QR code is chosen here. This QR code is used to identify the verifier, the owner and the document uniquely.

2.2.2 Best Hashing Algorithm

The original data is summarized by the hash value, where the function known as hashing algorithms take an input and outputs a fixed-length result, called the hash or hash value. During the literature review phase, four hashing algorithms from SHA family could be found such as SHA-1, SHA-256, SHA-384 and SHA-512. The proposed system must be a high-secured one because it is proposed for legal services in judicial systems. Therefore, under the requirement of the highest level of security of the document, SHA-512 is an excellent choice. (Compared specifications are mentioned under Section 2.3).

2.2.3 Verifier

The verifier of the legal document must be a qualified lawyer engaged in judicial services within Sri Lanka, who has been sworn as an Attorney-at-Law at the Supreme Court of Sri Lanka and is registered with the Bar Association of Sri Lanka. This ensures that the verifier is not only legally qualified but also recognized by the highest judicial authority in the country and affiliated with the professional body that regulates legal practice in Sri Lanka. The verifier must fill and enter all the relevant details obtained from the client?for the verification process. He must also scan and make a pdf of the client's document to upload to the system.

2.2.4 Document Owner's Details

The document owner is the person (client) who wants to get a document verified by a lawyer. The document owner must meet the verifier (lawyer) with the correct details and produce the document to the lawyer to complete the verification process. For the document owner's details, he/she must provide his/her details such as NIC Number, Full Name, Contact, Address and Date of Birth to the verifier.

2.2.5 Generate Hash

This is the main function of the legal document verification system. After entering the correct and relevant details by the verifier, the system generates the hash value for the uploaded document. With the hardcoded SHA-512 algorithm, Verifier's Enrolment Number, Owner's NIC Number and Document ID is used to generate the hash value. At the end of the process, it merges into the last page of the document, and it is sent to blockchain using smart contract.

2.2.6 Generate QR Code

Document ID, Verifier's Details (Enrolment Number, Membership Number, First Name, Last Name, Position, Workplace, Email) and Document Owner's Details (NIC Number, Full Name, Contact) are details combined into a single string for the generating the QR code. At the end of the process the generated QR

code is displayed on the user interface and merged into the last page of the uploaded document.

2.2.7 Send to Smart Contract

Digital contracts known as "smart contracts" are kept on a blockchain and are programmed to activate automatically in response to specific events. After deploying the smart contract, the generated hash value is added to the smart contract to the first phase of the verification.

2.2.8 Verify Document

After adding the hash value into the smart contract, the verifier can store the document with the hash value in the blockchain. After the verification of the document, it can be identified whether the document is a forged one or not.

2.2.9 Blockchain

Here the Ethereum platform is used as the blockchain to maintain a distributed and immutable database for legal documents that can be trusted by courts, legal professionals and regulatory bodies. Ethereum's blockchain allows for the deployment of smart contracts which are self-executing contracts.

2.3 Compared the Specifications for Selecting Best Hash Algorithm

Table 1: Specifications for hash algorithms

	SHA-1	**SHA-256**	**SHA-384**	**SHA-512**
Hash Length	160-bit	256-bit	384-bit	512-bit
Speed	Faster than other algorithms due to shorter hash length	Offers a good balance	Offers a good balance.	Slower than SHA-256 due to increased complexity and longer hash length
Security	Less	Good	Average	Higher
Efficient	Efficient but not secure.	Efficient for most applications	Suitable for high-security requirements where performance is less critical	
Implement Ease	Easy	Widely supported	Supported in most cryptographic libraries	
Adaptability	Limited	High		Highest
Standardization	Deprecated in most standards, including NIST and PCI DSS	Standardized by NIST under FIPS PUB 180-4		
Data Integrity	Historically used but now replaced due to security vulnerabilities	Widely used in blockchain, digital signatures, and certificate authorities	Used in scenarios requiring higher security than SHA-256	deal for high-security environments, such as government or financial institutions
Regulatory Requirements	Not compliant with most modern security regulations	Compliant with most regulatory frameworks and recommended for new implementations	Compliant and recommended for high-security environments	
Digital Signatures	Deprecated	Commonly used	Preferred in high-security digital signatures, especially for long-term validation	
Password Hashing	Not recommended	Commonly used (crypts or Argon2)	Suitable for scenarios requiring high security, though still often paired with salts and key-stretching techniques	
Community and Tool Support	Legacy support remains but diminishing rapidly	Extensive support across all major platforms and cryptographic libraries	Supported but less commonly used than SHA-256	
Industry Adoption	Largely abandoned	Widely adopted	Gaining adoption in sectors requiring higher security	
Framework and Tool Support	-	-	Widely supported by blockchain development	Supported in advanced blockchain platforms or custom implementations where

			platforms like Ethereum, and Hyperledger	higher security is needed
Integration with Hash Algorithms	Used in blockchain-related projects	Commonly used in blockchain technology (e.g., Bitcoin)	Less commonly used in public blockchains	
Memory Requirements	Requires minimal memory for storage (20 bytes per hash)	Requires 32 bytes per hash	Requires 48 bytes per hash	Requires 64 bytes per hash
Practical Usage	Due to its short hash length, it is easy to store but not recommended for new applications	The most common in blockchain	More secure but less commonly used	More secure but less commonly used, and the longer hash size could lead to slightly increased storage demands

After analyze above mentioned facts,

- SHA-1 is No longer suitable due to significant security vulnerabilities.
- SHA-1 is not recommended due to security issues and low storage requirements. SHA-256 is provide a strong balance of security and performance. As well as making it the most widely used.
- SHA-256 is ideal for most blockchain applications due to its strong security and adoption in blockchain frameworks.
- SHA-384 is offer higher security than SHA-256.
- SHA-512 provides the highest level of security and it suitable for applications where the security is most important.

According to the methodology,

First take SHA-256 hash algorithm. Here trimmed hash for SHA-256 is stored. SHA-256 hash has 32 bytes (256 bits) and 64 hexadecimal characters. According to this, 32 trimmed characters and the hash are stored?

- Secondly, take SHA-256 hash algorithm. Here, the full hash for SHA-256 is stored. According to the generated hash, it is successfully stored.
- Thirdly, take SHA-512 hash algorithm. Here the full hash for SHA-512 is stored. SHA-512 hash has 64 bytes (512 bits) and 128 hexadecimal characters. According to the generated hash, it is successfully stored

Therefore, the document verification in judicial services application requires enhanced security, and understanding that this will involve more complex implantation and higher memory allocation, it can be finalized as,

- The best Hash Algorithm is SHA-512

2.4 Generating QR Code

QR codes are a secure and scannable method for verifying user data authenticity and integrity. They encode all verifier's data, including Enrolment ID, Membership ID, Email, and contact, making them resistant to tampering and easily detectable. QR codes are highly accessible, as they can be scanned with common devices like smartphones, enabling verification even offline.

The process involves extracting the first two letters of each word in a tile, converting them to uppercase, splitting the title into words, mapping each word to its first two letters, and joining the resulting parts into a single string with 'DOC'. The last three digits of the verifier's Enrolment ID are then retrieved, along with the last four digits of the document owner's NIC number. The autogenerated document ID is with the last two digits hidden. The document owner's NIC number is also hidden, along with the verifier's full name and contact.

2.5 Backend Design

The research project consists of three tables: Signup_Details, Owner_Details, and Verification_Details. The Signup_Details table contains information about the verifier's registration, while the Owner_Details table contains information about the document owner. The primary key is Enrolment_ID, and the Owner_Details table has five attributes. The Verification_Details table contains information about the document verification process, with seven attributes. The primary key is Document_ID, and the foreign keys are Verifier_ID and Owner_ID. A well-designed database is essential for developing scalable, maintainable, and high-performance systems that meet application requirements.

3. RESULTS AND DISCUSSION

3.1 Results

According to the used 59 test cases and their results,

$$\text{Average} = \frac{\text{Total Result (Succesfull)}}{\text{Total Count of Test Cases}}$$

$$= \frac{59}{59}$$

$$= 1$$

Therefore, the percentage of system testing is 100%.

According to the tested 24 English documents,

$$\text{Average} = \frac{\text{Total Result (Succesfull)}}{\text{Total Count of Documents}}$$

$$= \frac{24}{24}$$

$$= 1$$

Therefore, the percentage of performance testing of English documents is 100%.

According to the tested 36 Sinhala documents,

$$\text{Average} = \frac{\text{Total Result (Succesfull)}}{\text{Total Count of Documents}}$$

$$= \frac{33}{36}$$

$$= 0.9167$$

Therefore, the percentage of performance testing of English documents is 91%.

According to the overall inserted all documents,

$$\text{Average} = \frac{\text{Total Average}}{\text{Total Count}}$$

$$= \frac{1.9167}{2}$$

$$= 0.9584$$

Therefore, the percentage of performance testing of overall inserted documents is 95%. So, this system performs all its functionalities with 95% accuracy.

The proposed system has achieved an overall verification accuracy of 95%, including 100% accuracy for English documents and 91% accuracy for Sinhala documents. The lower accuracy found in Sinhala documents can be attributed to optical character recognition (OCR) limitations associated with Sinhala character identifications. Compared with traditional manual verification processes such as oversight, susceptible to human errors and inconsistencies, the proposed automated system offers a more reliable verification mechanism. The results indicate that blockchain based verification can improve document authenticity assessment while preventing opportunities for forgery.

$$\text{Average time} = \frac{\text{Total time (Seconds)}}{\text{number of times}}$$

$$= \frac{2789}{07} \text{ secs}$$

$$= 398.3 \text{ secs}$$

$$\approx 07 \text{ minutes}$$

The system provides results for all users at once, with some users requiring extra assistance. The majority of users find it easy to navigate, generate QR codes, and verify legal documents. The system is accessible and user satisfaction is high. Some users suggest future enhancements, which are addressed in the future recommendations section. Document templates for usability are attached. The system takes nearly 07 minutes for first-time users to receive results.

For the testing process in this research, three methods were used as system testing, performance testing and usability testing. During the system testing, all the functionalities of the developed system were tested by using test cases and test plan. The performance testing was done with English and Sinhala documents to identify forged documents. During the usability testing, the developed system was tested with legal professionals, and the average time taken for using the system was calculated. Further, a feedback survey was conducted with them.

Document forging is crucial for the Sri Lankan judicial system, and blockchain technology is a suitable solution for high-security applications. The SHA-512 hash algorithm and smart contracts are used to store hash values, providing an immutable database. The generating QR code is a key factor in identifying the verifier of a document, as it displays the verifier's details and merges with the uploaded document's hash value and verified date and time. This method accurately identifies if a document is forged, as a forged document would generate different hash values.

3.2 Discussion

Traditional legal document verification in Sri Lankan judicial services has been depending on manual inspection and centralized authorities such as legal professionals or notaries. These processes are prone to human errors, fraud and delays. The manual verification process of court documents creates inefficiencies and compromise with accommodation of judicial integrity (Kumar et al., 2023). Similarly existing studies also highlight that traditional legal systems are afflicted by authenticity issues especially in global disputes (Zhuk, 2023).

Independently, blockchain-based solutions offer immutability, transparency and decentralization. In the blockchain-based model for certificate verification, studies have demonstrated how cryptographic hashing and smart contracts can enhance reliability while minimizing administrative cost (Ghazali and Saleh, 2018). There was developed Docschain also known as an IoT-integrated blockchain system, which is to verify degree documents while ensuring authenticity and privacy (Rasool et al., 2020). Such approaches have successfully demonstrated applicability in verification processes in education and employment (Dhyani et al., 2022), and they reveal the adaptability across multiple domains beyond the academic domain.

Compared to these existing works, this research introduces a blockchain based verification application specially for Sri Lankan judicial services. The capability of SHA-512 hashing ensures a stronger cryptographic security than other hashing algorithms. While SHA-256 accepts average performance of security, the judicial domain demands higher opposition to impact, making SHA-512 the better choice.

Another notable improvement of this research is the deployment of QR code as a digital signature. DOC-BLOCK highlights blockchain authentication but does not include a user-friendly method (Imam et al., 2021). By embedding document verifier details including Enrolment ID, Membership ID and document owner details into QR code, this application ensures quick accessible verification without requiring direct blockchain interaction. This is very useful in judicial service where speed and reliability are critical operational requirements.

Furthermore, while existing models basically focused on certificates (Ghazali and Saleh, 2018) (A. Gayathiri, 2020) (Rasool et al., 2020) CVs (Marella and Vijayan, 2020) or educational records (Saleh et al., 2020), this research expands the applications to wide aspects of legal documents including, affidavits, Writs, case files, deeds etc. addressing a gap in the literature review. With an achieved accuracy of 95% overall, as 100% for English documents and 91% for Sinhala documents, the proposed application demonstrates a practical Perspective in multi-language legal document proceedings. From the practical perspective, a 95% accuracy rate indicates a high level of reliability, however, in the legal context, even a small error may have serious consequences as incorrect validations.

Therefore, the present research extends the range of blockchain document verification process in the legal sector, introducing stronger cryptographic security using SHA-512 hashing and enhanced accessibility with QR verification and providing innovation over

existing works. These contributions collectively demonstrate a meaningful advancement over existing systems in terms of security, usability, and practical deployment in judicial services.

4. CONCLUSION

This research demonstrates that blockchain technology when combined with progressive cryptographic hashing and QR digital signatures, provide a scalable and strong solution for verifying legal documents in judicial services in Sri Lanka. The traditional manual verification processes which are subject to fraud, human error and inefficiency can be effectively replaced with a blockchain based solution, and it ensures transparency and efficiency. By adopting SHA-512 hashing algorithm, the proposed solution achieves a better level of cryptographic security compared to other hashing algorithms, making it more suitable for legal documents. The integration of QR code as digital signature provides an additional aspect of user-friendliness, allows quick identification of both the document and the verifier. The results of testing show 100% accuracy for English documents and 91% accuracy for Sinhala documents while overall accuracy shows 95%. This shows that the application is practically operable and can notably strengthen the integrity of the judicial service. However, the limitations carry on the language identification accuracy for Sinhala documents and restriction to PDF format. The future enhancements such as adding biometric user authentication, mobile applications and alternative verifier identification methods such as keywords or OTP could upgrade usability, accessibility and security. The successful deployment can serve as a wider adoption of blockchain in legal services, a practicable transforming of how trust and integrity are maintained in Sri Lankan judicial service and beyond.

5. FUTURE WORKS

In cases where the QR code cannot be scanned, it would be better to have a 'Keyword' as an alternative method for identifying the document verifier. The keyword could be set by each verifier during the signup process. During the verification process, the verifier's keyword, along with the document ID, can be entered into the system to retrieve the verifier's details.

The system could be extended to a mobile application to provide easier access and convenience for end users.

At times, certain lawyers tend to forge the proxy lawyer's signature without their consent, getting the clients to sign another proxy with him/her as their proxy lawyer. So, it would be better to send an 'Authentication Code' to the user's mobile whenever a user uploads a document that embodies his seal and the signature. In this way, a third party cannot upload any document to the system as he/she cannot confirm the authentication code sent to the genuine user's mobile, and without alerting the real owner of the signature.

Since most law firms in Sri Lanka are registered as companies with the Department of the Registrar of Companies, all partners of the law firm are advised to use the same company signature and seal for every legal document. Moreover, in matters such as hire purchase, the plaintiff is usually a bank or a leasing company, and the formats used by lawyers when drafting legal documents are also exactly the same. Sometimes, the figures may also be similar. So, it would be ideal if this system could be improved to identify forged documents in such scenarios as well.

For the better verification of end users, the system could integrate biometric data such as finger prints, facial recognition and iris scanning during the signup process.

6. LIMITATIONS

This system is currently for use only in Sri Lankan judicial operations.

Verification is limited to Sinhala and English documents.

Only PDF formatted documents are accepted.

This has been developed for use only by legal professionals in judicial service in Sri Lanka.

7. REFERENCES

Gayathiri A., J. J. A. S. M. 2020. Certificate validation using blockchain. *2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India*, 1-4.

Chaniago, N., Sukarno, P. & Wardana, A. A. 2021. Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain. *Register,* 7**,** 149-163.

Chavan, D. S., Dayama, R. N., Joshi, P. P., Pawar, P. P. & Londhe, A. DOCUMENT VERIFICATION AND VALIDATION USING BLOCKCHAIN.

Dhyani, K., Mishra, J., Paladhi, S. & Sumaiya Thaseen, I. A blockchain-based document verification system for employers. Proceedings of International Conference on Computational Intelligence and Data Engineering: ICCIDE 2021, 2022. Springer, 123-137.

Ghani, R., Al-Karkhi, A. & Mahdi, S. 2022. Proposed Framework for Official Document Sharing and Verification in E-government Environment Based on Blockchain Technology. *Baghdad Science Journal,* 19**,** 1592.

Ghazali, O. & Saleh, O. S. 2018. A graduation certificate verification model via utilization of the blockchain technology. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* 10**,** 29-34.

Imam, I. T., Arafat, Y., Alam, K. S. & Shahriyar, S. A. DOC-BLOCK: A blockchain based authentication system for digital documents. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021. IEEE, 1262-1267.

JITESH CHOUDHARY, A. S., SAKSHI MALVE, DEEPIKA DAWLE 2024. Application of Blockchain Technology in the

Management of Legal Documents. *IJARSCT,* 4.

Kumar, D., Kumar, S. & Joshi, A. 2023. Assessing the viability of blockchain technology for enhancing court operations. *International Journal of Law and Management,* 65**,** 425-439.

Kumar, K. D., Senthil, P. & Kumar, D. 2020. Educational certificate verification system using blockchain. *international journal of scientific & technology research,* 9**,** 82-85.

Marella, V. & Vijayan, A. Document Verification using Blockchain for Trusted CV Information. AMCIS, 2020.

Moumita Das, X. T., Yuhan Liu, Jack C.P. Cheng 2022. A blockchain-based integrated document management framework for construction applications. 133.

Prathamesh Sinkar, G. S., Sudhir Patil, Mohit Pawar, Prof. Supriya Jagtap 2024. Document Storage and Verification System Using Blockchain Technology. *IJARSCT,* 4.

Rasool, S., Saleem, A., Iqbal, M., Dagiuklas, T., Mumtaz, S. & Ul Qayyum, Z. 2020. Docschain: Blockchain-based IoT solution for verification of degree documents. *IEEE Transactions on Computational Social Systems,* 7**,** 827-837.

S. Mthethwa, N. D. A. G. B. 2018. Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius*, 1-5.

Saleh, O., Ghazali, O. & Rana, M. E. 2020. Blockchain Based Framework for Educational Certificates Verification. *Journal of Critical Reviews,* 7**,** 79-84.

Satybaldy, A., Subedi, A. & Nowostawski, M. 2022. A Framework for Online Document Verification Using Self-Sovereign Identity Technology. *Sensors,* 22**,** 8408.

Shakan, Y., Kumalakov, B., Mutanov, G., Mamykova, Z. & Kistaubayev, Y. 2021. Verification of university student and graduate data using blockchain technology. *International Journal of Computers Communications & Control,* 16.

Sharma & Khanna, D. 2023. Automated Medical Document Verification on Cloud Computing Platform: Blockchain-Based Soulbound Tokens. *Acta Informatica Pragensia*.

Yashchyk, O., Tverdokhlib, I., Franko, Y. & Ozhha, M. 2023. USING BLOCKCHAIN TECHNOLOGY FOR SECURITY AUTOMATION OF MANAGEMENT OF EDUCATIONAL

DOCUMENTS. *The Scientific Issues of Ternopil Volodymyr Hnatiuk National Pedagogical University. Series: pedagogy,* 1**,** 113-120.

Zhuk, A. 2023. Applying blockchain to the modern legal system: Kleros as a decentralised dispute resolution system. *International Cybersecurity Law Review,* 4**,** 351-364.