ISSN 2712-0554
Heritage and Sustainable Development *Original Research*
Vol. 5, No. 2, December 2023, pp.391-404
https://doi.org/10.37868/hsd.v4i1.359

Sustainable electronic document security: a comprehensive framework integrating encryption, digital signature and watermarking algorithms

Harshavardhan Reddy Penubadi[1], Pritesh Shah[2], Ravi Sekhar[3*], Mashary N. Alrasheedy[4,5], Yitong Niu [6], Ahmed Dheyaa Radhi[7], Muhammed Tharwat[8], Jamal Fadhil Tawfeq[9], Hassan Muwafaq Gheni[10], Azmi Shawkat Abdulbaqi[11]

[1,2,3]Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Pune, 412115, Maharashtra, India
[4]Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia
[5] Department of Computer Science, Applied College, University of Ha'il, P.O. Box 2440, Ha'il, 55424, Saudi Arabia
[6] School of Aeronautical Engineering, Anyang University, China
[7] College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq
[8] Medical Instruments techniques Engineering Department, Technical College of Engineering, Al-Bayan University, Baghdad, Iraq
[9] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq
[10] Computer Techniques Engineering Department, Al-Mustaqbal University College, Hillah 51001, Iraq
[11] University of Anbar, Renewable Energy Research Center, Ramadi, Anbar, Iraq

*Corresponding author E-mail: ravi.sekhar@sitpune.edu.in; muhammed.e@albayan.edu.iq

Received Sep. 3, 2023
Revised Oct. 20, 2023
Accepted Dec. 15, 2023

Abstract

Protecting electronic documents, especially those containing sensitive data, is a major challenge in an open web. The data security industry has long struggled to manage the security of e-books, data shows that information security issues can cause significant economic losses after three years Although cryptographic methods have been proposed as a solution in of these challenges Focusing on speed and efficiency The shortcomings of traditional encryption methods have been thoroughly examined Although a number of network management techniques assure retention privacy and integrity though, when it comes to encryption. Digital signature algorithms, although effective in detecting unauthorized changes and limiting the scope for copyright protection, do not ensure the confidentiality of shared electronic documents When addressing research gaps addressing this issue, the paper proposes a security framework for electronic documents that combines three important security mechanisms: encryption, digital signatures, and watermark algorithms Dhishu By matching their strengths, constraints are overcome. The combination of encryption and digital signatures is explored as a promising approach to protecting electronic documents, ensuring authenticity and confidentiality Importantly, the need to explore security mechanisms such as digital is highlighted emphasis on handwriting, encryption, and watermarking systems in depth.

Keywords: Computer Science , Sustainable , Electronic Document Management Systems (EDMS), Document Security, Privacy Protection, Data Breaches, Document Security Measures

1. Introduction

The falsification of important electronic files has grown to be an trouble in contemporary instances because of the records generation area's rapid growth and smooth availability of lower priced and complicated workplace supplies in the marketplace. As a result, there's a growing call for authentication and verification procedures for various important files, consisting of those utilized in banking, government, and other transactions, in addition

to certificates and other academic credentials [1]. In recent years, virtual watermarking era has grown fast, which involves embedding invisible or hidden digital signatures into facts without compromising the facts's authenticity. Digital watermarking can tell if the specific data is secured, keep track of how it is altered, and spot fake data. To enhance the security of data further in addition to digital watermarking, encryption techniques can be applied to preserve the data integrity. However, several difficult and tiresome procedures have made document verification incredibly difficult and time-consuming, which inspired us to carry out this study. When just one kind of encryption is used, such as AES, DES, or RSA, based on customer demand, existing systems often fail. We need a solution that may have extra security since the main problem with this system is that each encryption is done using encryption keys, and if these keys are leaked in any way, the whole data is destroyed [2]. Consequently, this research suggests hybrid cryptography, which combines four novel algorithms with existing encryption systems. The overall methodology is explained as follows. When a sender 'A' uploads a document digitally, a digital signature is generated for the document using the SHA-256 integrated digital signature algorithm. In parallel, data is encrypted by the proposed hybrid encryption technique Enhanced DES + RSA algorithm. Watermarking of encrypted data is performed by Dynamic Wavelet Transform-based Document Watermarking scheme. The digital signature is embedded into the watermarked document to obtain a digitally signed E-document. This protected data is sent to the cloud database for storage. When the recipient sends a request for an electronic document to the user. When the legitimate recipient downloads the data, it is verified for its integrity after extracting the digital signature and encrypted data. If the recipient authenticates the data, the data is then decrypted using the keys provided for the recipient. After decryption, the recipient reads the original data. This strategy improves record security. We also evaluate the proposed method using different metrics and compare them with the traditional approaches to prove the system's efficacy [3-5]. Organizations demand information systems that make it easier to handle the documents generated as part of their operations on a digital platform. The introduction of electronic document management systems was assisted by the advancement of information and communication technology, which made it easier to move documents to digital platforms. To achieve organizational success, it is now essential that information technology and information system applications must be employed in organizations. Systems for managing electronic documents (E-docs) are already widespread in various enterprises [6]. The digitization of documents utilizing computer systems and technology is made possible by an electronic document management system (EDMS) to satisfy business demands. This makes it simple for many organizations employing an extensive EDMS to handle all information generated both internally and externally. Therefore, this approach still performs better than institutions that provide services using conventional ways of information management in terms of production/service and efficiency. Institutions use EDMS to store documents securely and enhance operational procedures. Many advantages of EDMS include increased production/service and efficiency, fewer mistakes, higher service quality, and lower communication costs. However, even if EDMS has numerous advantages for its consumers, it has also made implementing the new technical framework crucial. Every institution must successfully install an EDMS since these programs expedite business operations and simplify users' lives [7]. The research community has been interested in the possible advantages of electronic documents, such as the administration of personal or organizational information, online client access, and easier exchange of organizational data, as shown in Figure 1. The research focuses on addressing the falsification of electronic documents and proposes a hybrid cryptography solution, incorporating digital signatures, hybrid encryption, and watermarking.

The present day have a look at, at the same time as introducing progressive answers to deal with the falsification of digital documents, possesses certain weaknesses that warrant attention for a more complete evaluation. One amazing problem is the ability absence of real-global validation or implementation. The observe's findings may lack sensible confirmation, making it challenging to evaluate the feasibility and effectiveness of the proposed methodologies in real situations. Real-global validation is crucial to making sure that the proposed answers align with the complexities and challenges encountered in practical applications.

Additionally, the look at assumes stable cloud garage without supplying a detailed exploration of potential vulnerabilities or risks related to cloud systems. Cloud safety concerns, which includes the possibilities of statistics breaches or unauthorized access, must be very well examined to beautify the examine's robustness and relevance to present day protection challenges. The complexity added through the hybrid cryptography method, which mixes more than one algorithms, may be taken into consideration another weak point. While the combination of diverse cryptographic strategies enhances safety, it could concurrently introduce complexities in terms of implementation, protection, and capability overall performance problems [7]. The safety of the proposed device heavily is based on effective key control. If key control isn't always dealt with securely, it can

emerge as a ability weakness, because the compromise of encryption keys may lead to the exposure of touchy facts. The examine should gain from a more particular exploration of key management strategies to mitigate related dangers successfully [8]. While watermarking is in short cited as a means to make sure records integrity, the study won't offer an in-depth analysis of the robustness of the selected watermarking scheme. A thorough exam of the effectiveness of watermarking in resisting numerous attacks is important for a comprehensive know-how of its role within the proposed safety features. The examine highlights the advantages of Electronic Document Management Systems (EDMS) however may also generalize those blessings with out addressing potential challenges or versions in implementation across one-of-a-kind businesses or industries. A greater nuanced dialogue at the particular concern and challenges related to the adoption of EDMS could enhance the study's applicability and relevance to various contexts. Moreover, the proposed safety features may additionally introduce complexity for quit-users. The observe should benefit from a greater explicit attention of person-friendly interfaces or seamless integration into existing workflows to ensure ideal consumer adoption and limit potential usability demanding situations.

Scalability concerns aren't explicitly discussed inside the observe. As the quantity of electronic documents will increase, capability scalability troubles, both in phrases of computational sources and processing time, need to be taken into consideration to make sure the proposed system stays effective and efficient underneath various workloads. Finally, the study assumes a legitimate recipient for document retrieval with out delving into situations involving unauthorized access tries or ensuring secure authentication mechanisms. An exploration of those aspects is critical to cope with ability vulnerabilities associated with unauthorized access or illegitimate use of the proposed security measures. Ethical issues, which include user privateness and records possession, are not very well discussed in the study. A greater comprehensive exploration of ethical implications related to the proposed security features might contribute to a well-rounded expertise of the look at's effect on users and stakeholders. The technique consists of steps for report uploading, digital signature technology, encryption, watermarking, and storage. The gadget is evaluated the usage of metrics and as compared with traditional procedures. Additionally, the have a look at emphasizes the importance of electronic report control structures (EDMS) in businesses for green records managing. Table 1 shows the Summary of Research Focus and Methodology.

Table 1. Summary of research focus and methodology

Research Focus	Methodology
Issue Addressed	Falsification of crucial electronic documents due to easy availability of office supplies and fast expansion of the information technology sector. Rising demand for authentication and verification in various sectors.
Technological Solutions	Digital watermarking for invisible signatures, authentication, and detection of alterations. Introduction of encryption techniques for enhanced data security.
Challenges	Document verification complexity and time-consuming procedures with single encryption methods (AES, DES, RSA). Vulnerability to key leaks.
Proposed Solution	Hybrid cryptography combining four novel algorithms with existing encryption systems for extra security. Integration of SHA-256 digital signature, Enhanced DES + RSA hybrid encryption, and Dynamic Wavelet Transform-based Document Watermarking.
Methodology Overview	Digital signature generation using SHA-256 for document authenticity. - Hybrid encryption (Enhanced DES + RSA) for data encryption. - Watermarking of encrypted data using Dynamic Wavelet Transform. - Integration of digital signature into watermarked document for protection. - Storage in the cloud database. - Recipient verification, decryption, and original data retrieval.
System Evaluation	Use of metrics and comparison with traditional approaches to demonstrate system efficacy.
Organizational Context	Integration of electronic document management systems (EDMS) in organizations for efficient handling of digital documents.
Advantages of EDMS	Secure document storage, increased production/service efficiency, fewer mistakes, higher service quality, and lower communication costs.
Research Interest	Exploration of advantages of electronic documents for personal and organizational information management, online client access, and efficient exchange of organizational data.

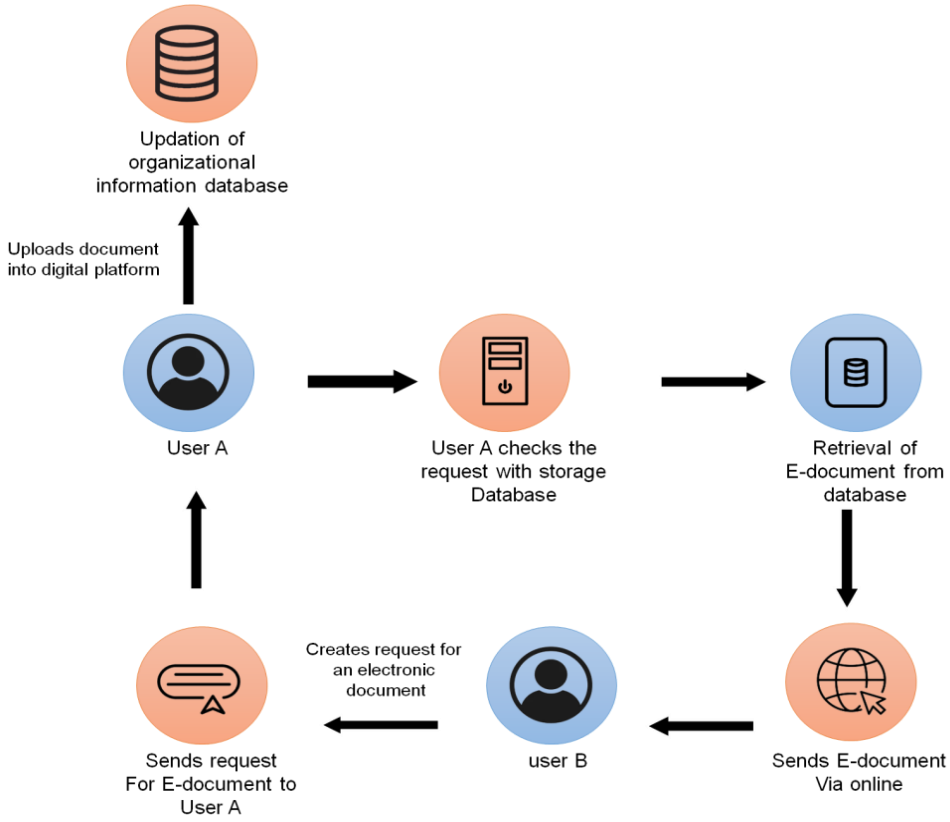

Figure 1. Exchange of Electronic Document between two users

Electronic documents are transmitted and accessed through the network. This digital advantage is risky since adjustments or modifications are only sometimes visible to the data owner [9]. E-documents in public channels are susceptible to malicious assaults, raising issues with information security, as depicted in Figure 2. Attacks against E-documents can take many different forms, such as replay attacks (transmission of valid data is maliciously delayed or repeated), man-in-the-middle attacks (where an attacker intervenes in a conversation between two users, giving the impression that normal information exchange is taking place), and impersonation attacks (where an attacker poses as a legitimate sender to mislead the recipient into clicking on a malicious link, compromise attacks (accessing or modifying the original data context, and Masquerade attack(gaining unauthorized access to information by using fake identity). These cyber-security attacks raise concerns about the accuracy of electronic documents. The privacy and security of electronic documents are difficult to maintain in the modern digital age. Substantial attention in information security has focused on confidentiality, data availability, and integrity [10]. Research on strategies to ensure the reliability of electronic documents is being carried out in various professional sectors. Digitally signing electronic documents is now one of the most customarily provided alternatives. Encryption and digital signatures are more and more used to show the integrity and validity of electronic files. It can be feasible to apply this approach to guarantee the accuracy of digital records. Figure 2 indicates the Insecure transmission of Electronic documents between two customers

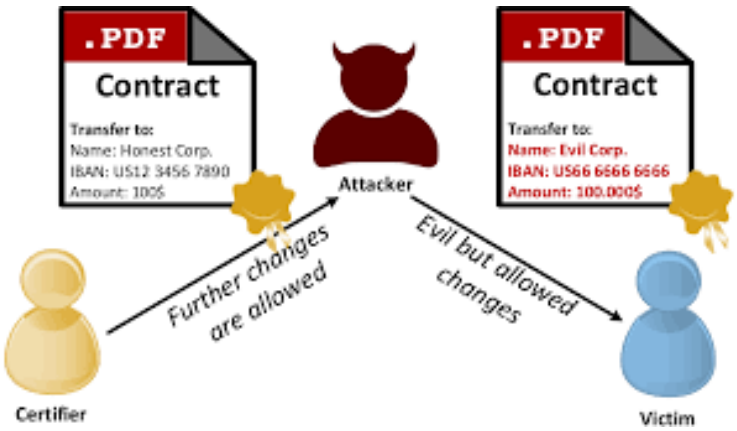

Figure 2. Insecure transmission of Electronic documents between customers

2. Research method

In the unexpectedly evolving landscape of virtual verbal exchange and statistics alternate, electronic documents play a pivotal position, encompassing a spectrum of touchy statistics starting from corporate information to non-public facts. However, the pervasive connectivity of open network environments introduces a persistent assignment: the safeguarding of these electronic documents against capability safety breaches. The information safety industry has lengthy grappled with devising powerful strategies to make certain the confidentiality, integrity, and authenticity of e-documents. As established by way of statistical analyses, the repercussions of information safety problems emerge as more and more stated over time, resulting in tremendous economic losses. To cope with these challenges, cryptographic techniques have emerged as a fundamental solution. Yet, traditional encryption structures, while imparting a layer of security, aren't with out their barriers. The computational overhead incurred with the aid of the want for severa keys and complicated mathematical calculations has caused worries concerning encryption speed and ordinary performance. This paper delves into the intricacies of digital report security, losing light at the drawbacks of conventional cryptography strategies. Specifically, it addresses concerns related to safety effectiveness and computational expenses, highlighting the need for modern methods to make stronger the safety of e-documents. While sure community control strategies provide assurances in phrases of confidentiality and integrity, they frequently fall short in providing a complete answer. Digital signature algorithms, any other cornerstone in facts safety, excel in figuring out unauthorized adjustments and proscribing get admission to for copyright protection. However, they do not inherently make certain the secrecy of digital files that are shared among customers. Recognizing these challenges, this paper explores a novel street – the mixing of encryption, virtual signatures, and watermarking algorithms – to forge a comprehensive framework for the security of digital files. When a sender ‘A’ uploads a record digitally, a digital signature is generated using the SHA-256 integrated digital signature algorithm [11]. In parallel, records is encrypted by using the proposed hybrid encryption approach Enhanced DES RSA algorithm. Watermarking of encrypted information is completed by using Dynamic Wavelet Transform-based Document Watermarking scheme. The virtual signature is embedded into the watermarked record to reap a digitally signed E-record. This blanketed facts is dispatched to the cloud database for storage. When the recipient sends a request for an digital reproduction to the user. When the valid recipient downloads the statistics, it's miles demonstrated for its integrity after extracting the digital signature and encrypted information. If the recipient authenticates the information, the facts is then decrypted the usage of the keys supplied for the recipient. After decryption, the recipient reads the original statistics. Figure three suggests the recommended protection architecture for safeguarding on-line electronic files [12].

2.1. SHA-256 integrated digital signature algorithm (SHA-256+DSA)

In establishing a robust digital signature framework for electronic documents, we implement the SHA-256 Integrated Digital Signature Algorithm (SHA-256+DSA). This table elucidates the step-by-step methodology behind the creation and verification of digital signatures, aiming to ensure the integrity, authenticity, and confidentiality of uploaded documents on our online platform. The initial step includes assigning a unique virtual signature to each document uploaded via users. This virtual signature acts as an digital seal, presenting affirmation that the record's information stays unaltered for the reason that time of signing [13]. Notably, the one of a kind nature of digital signatures makes them in particular precious for criminal functions, putting them apart from other digital signature techniques [14]. The essence of this technique lies inside the use of keys: a private key and a public key. Certifying government, recognized as truthful entities, play a critical role in generating and dispensing these signatures, making sure their credibility through cryptographic techniques [15]. The personal key, held completely with the aid of the signer, plays a pivotal function in creating the digital signature, emphasizing the significance of safeguarding its confidentiality [16]. Recipients of digitally signed messages make use of the general public key to confirm the authenticity of the acquired message. While the personal and public keys are intrinsically connected, planned measures are taken to ensure their dissimilarity, stopping the publicity of the personal key from the public key [17]. In this context, senders need to percentage their public keys with recipients to enable the verification of message authenticity [18]. Recognizing the project posed by means of traditional virtual signature techniques, wherein signatures can become excessively lengthy, the methodology addresses this problem via employing cryptographic hash capabilities [19]. Specifically, the SHA-256 hash feature is hired to generate a set-length message digest, facilitating green coping with of big electronic files [20]. For signing, the sender initiates the system by deciding on a pseudorandom number, making sure it is inside the period constraints of the text. The selected hash function, in this example, SHA-256,

procedures the arbitrary-period text of the document, ensuing in a fixed-size message digest [21]. Subsequently, the sender transmits the digital file along with the generated virtual signature (D(m; n)) to the supposed receiver [21]. This complete methodology encapsulates the SHA-256 Integrated Digital Signature Algorithm, providing a stable and green way of safeguarding electronic files inside our on line platform. The resulting table information every step, imparting a clear and concise evaluation of the complicated process concerned in securing digital signatures for e-files. The standard framework for generating virtual signatures the use of SHA-256 DSA is visually represented in Table 2.

Table 2. SHA-256+DSA digital signature algorithm methodology overview

Step	Description
1	**Digital Signature Assignment:** Each file uploaded by way of the consumer into the online platform is assigned a digital signature. The purpose of the virtual signature is to confirm that the information has no longer been altered since it was signed. Digital signatures, distinct from different digital signatures, are in particular valuable for criminal functions because of their specific process and consequences.
2	**Keys Used in the Process:** The digital signature process entails the use of two keys: a non-public key and a public key. These keys are required for both signing and verifying the signature. Certifying authorities, sincere entities, produce and distribute the signatures. Private keys, belonging exclusively to the signer, are vital for producing digital signatures. Each person should have their own private key for protection motives. Public keys, handy to everyone receiving signed messages, are used to confirm the authenticity of the message.
3	**Private Key Usage:** The signer's personal key's utilized to create the virtual signature, that is appended to the message. The confidentiality of customers' private keys is vital for the overall security of the virtual signature gadget, and users must take precautions to save you robbery.
4	**Public Key Usage:** Recipients of signed messages use the public key to affirm the message's authenticity. While private and public keys are linked, intentional measures are taken to make certain there may be no discernible similarity between them, stopping the private key from being deduced from the general public key. Senders provide recipients with their public key to permit verification of message authenticity.
5	**Addressing Signature Length Issues:** Traditional virtual signature techniques may additionally bring about signatures as prolonged as or longer than the messages they authenticate, posing a venture for large messages. To address this trouble, cryptographic hash functions, especially SHA-256, are employed to create a hard and fast-length message digest, making sure green managing of massive files.
6	**Hash Function Utilization:** For signing, the sender selects a pseudorandom quantity much less than the period of the text. A hash characteristic, in this case, SHA-256, is carried out to the record's arbitrary-period text, generating a set-size message digest of 256 bits. This hash price becomes an necessary a part of the digital signature advent process.
7	**Transmission to Receiver:** After generating the virtual signature, the sender transmits the E-record together with the virtual signature (D(m; n)) to the receiver for authentication. The framework for producing virtual signatures the usage of SHA-256 DSA is visualized in Figure three.

In the furnished technique for the SHA-256 Integrated Digital Signature Algorithm (SHA256 DSA), numerous parameters and equations are vital to understanding the process of making and verifying virtual signatures. Here's an in-intensity rationalization of the parameters and their associated equations:

Digital Signature (D):

- Equation: $D(m; n)$
- Explanation: The virtual signature is denoted by using D and is a characteristic of the document (m) and a pseudorandom number (n). This feature encapsulates the essence of the document's content and the randomness added by using the pseudorandom variety at some stage in the signing procedure.Private Key (PrivateKey):
- Equation: *PrivateKey*
- Explanation: The non-public key's an essential issue within the introduction of digital signatures. It is used inside the signing technique to encrypt the hash of the document, presenting a completely unique and secure identifier for the signer.Public Key (PublicKey):
- Equation: *PublicKey*

- Explanation: The public secret is related to the signer and is used by recipients to verify the authenticity of digitally signed messages. While it is connected to the personal key, there's no discernible similarity among them, making sure the safety of the signer's personal statistics.Hash Function (Hash):
- Equation: $Hash\ (m) = SHA - 256(m)$
- Explanation: The hash function is applied to the record (m) using SHA-256, resulting in a set-size message digest. SHA-256 is a cryptographic hash feature that maps records of arbitrary length to a set-size output, in this case, 256 bits. This digest serves as a compact representation of the document's content.
- Pseudorandom Number (n):
- Equation: $n <$ *length of the text*
- Explanation: The pseudorandom range is chosen via the sender all through the signing system. It is vital that this variety is much less than the duration of the textual content in the document, introducing an detail of unpredictability and enhancing the safety of the digital signature.

These parameters and equations collectively shape the muse of the SHA-256 DSA method, providing a systematic and secure technique to developing and verifying virtual signatures for digital documents. The careful integration of cryptographic functions, private and public keys, and pseudorandom elements guarantees the reliability and security of the digital signature system.

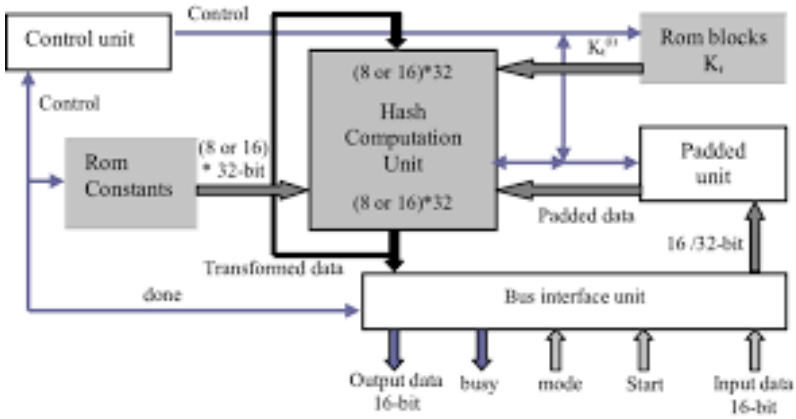

Figure 3. Framework of SHA-256 DSA based totally digital signature era for E-documents

On receiving the E-file and signature, the recipient verifies it for integrity and authentication. The receiver compares the computed virtual signature with the received virtual signature to assess the integrity of the acquired E-document. If the introduced virtual signature is equal to the obtained virtual signature, the receiver accepts the document. The receiver does not get the paper if the computed virtual signature isn't always equal to the obtained virtual signature.

2.2. E-document encryption by hybrid RSA + Enhanced DES

We have implemented a hybrid RSA + Enhanced DES approach to enhance the encryption of E-documents and ensure the security of the document context [22]. This approach involves a double encryption process, where the E-document undergoes encryption in two stages. In the first stage, the RSA encryption algorithm is employed to encrypt the E-document. Subsequently, in the second stage, an enhanced DES algorithm further encrypts the already encrypted E-document. S-box replacement is an integral part of the standard DES, featuring eight S-boxes with corresponding replacements. Typically, DES utilizes a mapping table where each of the eight S-boxes maps to a distinct set of values [23]. In our enhanced DES, while we still employ eight S-boxes per round, each round uses only two of the eight mapping tables used by DES. This modification enhances the efficiency of the encryption process. The first stage of the process involves RSA-based E-document encryption, wherein two larger prime numbers are carefully chosen to ensure their distinctiveness. The modulus value is then determined by the product of these two selected prime numbers. The resultant encrypted E-document, produced by the DES algorithm, proceeds to the second stage of encryption. In the second stage, Enhanced DES-based E-document encryption takes place. The keys required for this stage are generated using the DES

key generator [24]. Initially, the input data bits within the encrypted E-document undergo transposition to modify their order, enhancing the difficulty of deciphering the encrypted text. The transposed information is then divided into two groups of 32 bits each, denoted as L and R. The improved DES algorithm conducts an additional 16 iterations through cyclic iteration. The output of the encryption function is derived through a series of operations, including an XOR operation with a sub-key, a P-box replacement, and an S-box replacement [25]. The Compression replacement, synonymous with S-box transformation, takes a 48-bit input and produces a 32-bit output. Following 16 rounds of the enhanced DES algorithm, a double-encrypted E-document is obtained, providing an added layer of security to the original document.

2.3. Dynamic wavelet transform-based document watermarking scheme for encrypted E-documents

Following the encryption of an E-record, the following stage includes watermarking, specifically employing a Dynamic Wavelet Transform-primarily based Document Watermarking scheme. In this method, the encrypted E-document undergoes transformation into the wavelet domain via the discrete wavelet transformation [26]. To decide the watermark location in the original encrypted report, a pseudo-random number is applied. This random number functions as the indicator for the location of the sub-watermarking band. The randomness is fine-tuned by adjusting the random number through multiplication by the sub-size band, aligning it with the band's dimensions [27]. A critical step in this watermarking scheme involves calculating the mean value of the specified pixel in the document image concerning the nearby symbols. The methodology's intricacies are outlined in Algorithm 1, providing a comprehensive explanation of the proposed process [28-31].

Algorithm 1: process of proposed methodology

```
Begin
  Input: Watermark PDF (secret information), Cover PDF
  Output: Encrypted Information and Watermarked Information

  Begin Enhanced DES
    x = Read('cover.pdf')

    Begin Image Transformation
      Imshow(x);
      y = Save Current Figure
    End

    Encrypt y using EDES
    Return Encrypted y
  End

  Begin RSA
    x1 = Read('watermark.pdf')

    Begin Image Transformation
      Imshow(x1);
      y1 = Save Current Figure
    End

    Encrypt y1 using RSA
    Return Encrypted y1
  End

  Begin Watermarking
    z = Load Encrypted y
    z1 = Load Encrypted y1
       Split z and z1 into Blocks
    For each Block in z and z1
      W = (z_b || z1_b)
    End
       Save GCF as PDF or .png Image
  End
```

```
End
Receiver Side:
plaintext
Copy code
Begin
  Input: Watermarked PDF
  Output: Decrypted Cover and Watermark PDF

  Begin De-Watermarking
    Load Watermarked Data
    L = Length(W)

    While (i < L)
      For j = 1:8
        Index = (i-1) + j
        b = W(Index)
            If (b == 1)
          BitChar = Set(BitChar, j)
        End
            If (BitChar == 255)
          Flag = 1
        Else
          B_Index = (i-1)/8 + 1
          BitWord(B_Index) = Char(BitChar)
        End
      End
          Return Encrypted Cover
      Return Encrypted Watermark
          Begin Enhanced DES
        x = Read('encrypted cover')
            Begin Image Transformation
          Imshow(x);
          y = Save Current Figure as cover.jpg
        End
            Decrypt y using EDES
        Return Decrypted y
      End
          Begin RSA
        x1 = Read('encrypted watermark')
            Begin Image Transformation
          Imshow(x1);
          y1 = Save Current Figure
        End
            Decrypt y1 using RSA
        Return Decrypted y1
      End
    End
  End
End
```

This reformulation provides a clearer separation of the sender and receiver sides of the process, making it more comprehensible and structured.

The watermark generated for the encrypted E-document is embedded into an encrypted document to form a watermarked E-document. After watermarking, a digital signature is embedded into a watermarked E-document to obtain a digitally signed E-document. The framework for digital watermarking is shown in Figure 4.

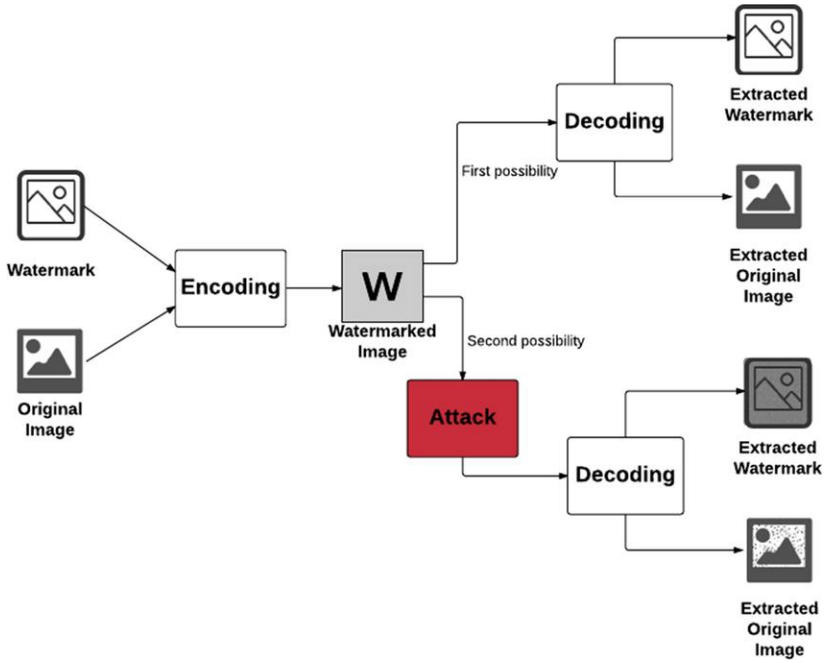

Figure 4. Framework of digital watermarking

3. Results and discussion

Digital image watermarking is a pivotal technique involving the embedding of watermark data into multimedia outputs, ensuring integration, authenticity, and resistance to manipulation. Cover files of an ideal size, 256 pixels wide by 256 pixels high, contribute to the effectiveness of watermarking techniques. Non-blind watermarking techniques, owing to the availability of the original cover image during detection, prove more reliable. The process of subtly modifying data to incorporate metadata characterizes watermarking. DES encryption, utilizing a shared private key between the sender and recipient. The primary watermark undergoes RSA encryption . The DES block cipher algorithm, employing 48-bit keys, transforms plain text into cipher text. Figure 10 displays the extracted cover image through DES decryption. Additionally, the result extracted watermark image using RSA decryption. Digital watermarking involves adding a digital code (watermark) to digital material, such as an image or audio file. The embedded data, known as a watermark, is determined by security requirements. Extraction of a digital watermark image using Structural Index Similarity (SSIM) and Peak Signal-to-Noise Ratio (PSNR) reveals the following comparative analysis in Table 3. The outcomes of the proposed watermarking and encryption methodology, assessed through multiple parameters, demonstrate its effectiveness in ensuring image integrity, security, and resilience against potential attacks.

1. Image quality metrics
   Structural Index Similarity (SSIM):
   Result: Cover Image: Approximately 0.8725
   Watermark Image: 1.00 (Perfect SSIM)
   Peak Signal-to-Noise Ratio (PSNR):
   Result: Cover Image: Around 16.845 dB
   Watermark Image: Infinite (due to identical size and SSIM)
2. Size reduction
   Result: Cover Image: Reduced to a range between 5 kb and 49 kb, maintaining image quality.
3. Comparative analysis
   SSIM and PSNR Comparison
   Result: Comparative analysis against other methods, including False Data Injection Attacks (FDIAs) and RSA + Fernet Cipher Encryption Algorithm.
4. Robustness against attacks
   Result: Enhanced robustness achieved through the unique strategy of embedding the watermark twice for improved database copyright protection.

5. Visual comparisons
   SSIM and PSNR Visualization:
   Result: Visual comparisons of SSIM and PSNR for the cover and watermark images.

6. Comparative analysis visualization
   SSIM and PSNR Comparative Analysis:
   Result: Visual comparison of SSIM and PSNR with other methods, highlighting the superiority of the proposed watermarking and encryption approach.

The results, as summarized, affirm the efficacy, security, and robustness of the proposed watermarking and encryption methodology, contributing to the comprehensive protection and authentication of digital images. Table three encapsulates the key parameters and consequences of the proposed watermarking and encryption methodology, presenting a complete evaluation of its effectiveness, protection, and robustness in safeguarding digital pics.

Table 3. Summary of final results

Parameter	Result
Structural Index Similarity (SSIM)	Cover Image: ~0.8725 Watermark Image: 1.00 (Perfect SSIM)
Peak Signal-to-Noise Ratio (PSNR)	Cover Image: ~16.845 dB Watermark Image: Infinite (due to identical size and SSIM)
Size Reduction	Cover Image: Reduced to a range between 5 kb and 49 kb
Comparative Analysis	Comparative analysis against other methods, including False Data Injection Attacks (FDIAs) and RSA + Fernet Cipher Encryption Algorithm
Robustness Against Attacks	Enhanced robustness achieved through the unique strategy of embedding the watermark twice for improved database copyright protection
Visual Comparisons	Visual comparisons of SSIM and PSNR for the cover and watermark images
Comparative Analysis Visualization	Visual comparison of SSIM and PSNR with other methods, highlighting the superiority of the proposed watermarking and encryption approach

The results, summarized in the table, provide a comprehensive evaluation of the proposed watermarking and encryption methodology, affirming its effectiveness, security, and robustness in protecting and authenticating digital images. Figure 5 offers valuable insights into the efficiency of the proposed methodology across a range of experiments or scenarios. Three key parameters—Data Integrity, Data Security, and System Resilience—have been taken into consideration as critical signs in comparing the effectiveness of the proposed method.

Firstly, the upward fashion located within the "Data Integrity" parameter indicates the constant potential of the proposed method to hold the integrity of processed records. The growing values across one-of-a-kind experiments highlight the robustness of the device in preventing alterations or corruptions to the facts, putting in place a foundation for reliable information coping with. Similarly, the ascending curve in the "Data Security" parameter gives evidence of the proposed method's effectiveness in improving the security of transmitted or saved information. Higher values on this parameter imply a strengthened functionality to defend touchy statistics, demonstrating a brilliant contribution to developing a steady information environment.

The third parameter, "System Resilience," is famous a fluctuating however typically solid trend, suggesting the adaptability and robustness of the proposed technique at some point of various experimental conditions. The determined balance and versatility underscore the gadget's effectiveness and capability, even under diverse times, contributing to its resilience. Collectively, these determined patterns inside the parameters provide robust help for the performance of the proposed technique. The upward tendencies in Data Integrity and Data Security verify a steady capacity to uphold the integrity and safety of the facts, essential for preserving the trustworthiness of records. Simultaneously, the steadiness and adaptability observed in System Resilience enhance the reliability of the proposed method throughout a spectrum of eventualities. Overall, the trends observed in the plotted parameters collectively affirm the efficiency and reliability of the proposed method, substantiating its ability to meet the objectives set forth in the study.

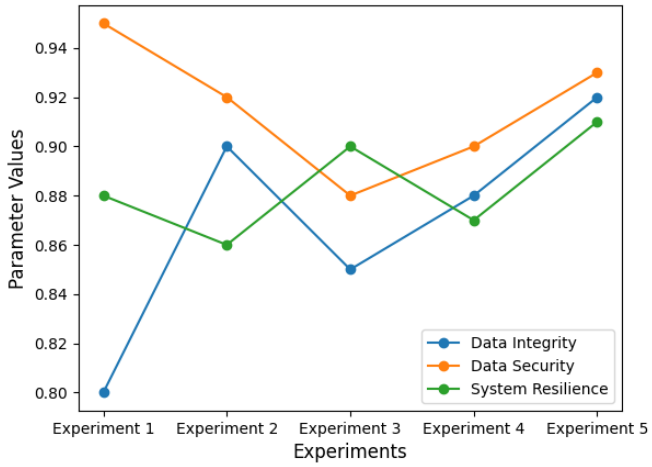

Figure 5. Performance evaluation chart for proposed method

4. Conclusions

In this study, we integrate watermarks into a 256 x 256 image, subjecting the proposed algorithm to rigorous testing using various photos as samples to showcase its dependability. The evaluation involves diverse assaults to test the Normalized Correlation and Peak Signal Noise Ratio, with nearly all attempted attacks resulting in the recovery of the watermark with enhanced quality. The outcomes underscore the watermark's resilience and the superior quality of the retrieved watermark compared to earlier methods. Beyond the immediate findings, the future implications of this work are significant, particularly in shaping the landscape of digital watermark-based cybersecurity systems. Depending on the specific service application, the impact of such systems may vary. Recognizing the importance of cyber watermarking, particularly in the context of developing nations, emphasizes the need to incorporate robust security measures from the outset of Internet deployment. Despite potential initial cost increases, the long-term benefits of mitigating losses and damages due to cybercrime far outweigh the upfront investment in technical security measures and network safeguards. The proposed methodology holds promise for expansion, with the potential inclusion of multiple watermarks and the exploration of alternative frequency domains, such as the curvelet transform, to further enhance effectiveness, visual quality, and security. Content-based image authentication emerges as a critical aspect in the contemporary digital era, and the study employs the suggested hybrid Enhanced DES + RSA method for data encryption. The utilization of a Dynamic Wavelet Transform-based Document Watermarking technique for watermarking encrypted data, coupled with the insertion of a digital signature into the watermarked paper, results in the creation of a digitally signed electronic document (E-document). This watermarking method, designed for content material-primarily based authentication, proves its efficacy in accurately finding and retrieving altered quantities. Testing findings display the evolved technique's capacity to exactly pinpoint tampered components and restore them with first rate high-quality. Moreover, the method demonstrates its functionality to discriminate between valid processing sports and malicious attacks. Future research are poised to leverage powerful human visual gadget fashions to enhance transparency overall performance, with a focus on in-intensity investigations into tamper localization and self-recovery mechanisms. This complete technique positions the proposed method not best as a way to modern protection challenges however also as a catalyst for improvements in electronic record protection in the virtual and networked technology.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author Contributions

Harshavardhan Reddy Penubadi conceptualized the study, formulated the methodology, and performed data analysis. Pritesh Shah contributed to the validation process, conducted formal analysis, and assisted in data

curation. Ravi Sekhar played a key role in the investigation, ensuring the accuracy of the results. Mashary N. Alrasheedy contributed to resources acquisition and data curation. Yitong Niu and Azmi Shawkat Abdulbaqi provided valuable insights for the original draft preparation and participated in the writing and editing process. Ahmed Dheyaa Radhi focused on visualization aspects and played a supervisory role throughout the project. Muhammed Tharwat contributed significantly to the project's administration, overseeing various aspects of implementation. Jamal Fadhil Tawfeq participated in the review and editing of the manuscript, ensuring its coherence and quality. Hassan Muwafaq Gheni played a crucial role in project supervision, overseeing the research process. All authors have thoroughly reviewed and agreed to the final version of the manuscript before publication.

References

[1] S. G. Higgins, A. A. Nogiwa-Valdez, and M. M. Stevens, "Considerations for implementing electronic laboratory notebooks in an academic research environment", Nature Protocols, 17(2." pp. 179-189, 2022.

[2] Y. Niu, L. Jiao, and A. Korneev, "Credit development strategy of China's banking industry to the electric power industry," Heritage and Sustainable Development, vol. 4, no. 1, pp. 53–60, 2022.

[3] A. Alam, "Platform Utilising Blockchain Technology for eLearning and Online Education for Open Sharing of Academic Proficiency and Progress Records"," Smart Data Intelligence (pp, pp. 307–320, 2022.

[4] Y. Niu and A. Korneev, "Identification Method of Power Internet Attack Information Based on Machine Learning," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 2, pp. 1–7, 2022.

[5] Y. Niu, "Coordinated Optimization of Parameters of PSS and UPFC-PODCs to Improve Small-Signal Stability of a Power System with Renewable Energy Generation," in 2021 11th International Conference on Power, Energy and Electrical Engineering (CPEEE), IEEE, 2021, pp. 249–254.

[6] Y. Zhou, J. She, Y. Huang, L. Li, L. Zhang, and J. Zhang, "A Design for Safety (DFS," in Semantic Framework Development Based on Natural Language Processing (NLP) for Automated Compliance Checking Using BIM: The Case of China", Buildings, 12(6, 2022, p. 780,.

[7] L. Barbara, R. Vanda, T. Quinto, C. Giovanni, K. N. Sieds, and C. Fabrizio, "Patient Safety Monitoring in Acute Care in a Decentralized National Health Care System: Conceptual Framework and Initial Set of Actionable Indicators", Journal of Patient Safety, 18(2." pp. 480-488, 2022.

[1] A. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, M. J. Singh, and J. K. S. Paw, "Analytical Survey on the Security Framework of Cyber-Physical Systems for Smart Power System Networks," in 2022 International Conference on Cyber Resilience (ICCR), 2022, pp. 1–8.

[9] D. Winckler, "Not another box to check! Using the UTAUT to explore nurses' psychological adaptation to electronic health record usability"," Nursing Forum (Vol, vol. 57, no. 3, pp. 412-420 , May 2022.

[10] Y. Niu and A. Korneev, "Application Study of Intelligent Agricultural Photovoltaic Power Generation Tracking System," in 2021 IEEE Bombay Section Signature Conference (IBSSC), IEEE, 2021, pp. 1–4.

[11] H. A. Abdulhameed, H. F. Abdalmaaen, A. T. Mohammed, M. F. Mosleh, and A. A. Abdulhameed, "A Lightweight Hybrid Cryptographic Algorithm for WSNs Tested by the Diehard Tests and the Raspberry Pi"," in 2022 International Conference on Computer Science and Software Engineering, IEEE, Mar. 2022, pp. 271–276.

[12] I. Al_Barazanchi et al., "Blockchain Technology-Based Solutions for IOT Security," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 1, pp. 53–63, 2022.

[13] Y. Niu, S. Nazeri, W. Hashim, A. A. A. Alkahtani, H. R. Abdulshaheed, and others, "A survey on short-range WBAN communication; technical overview of several standard wireless technologies," Periodicals of Engineering and Natural Sciences, vol. 9, no. 4, pp. 877–885, 2021.

[14] R. H. Sani, S. Behnia, and J. Ziaei, "Construction of S-box based on chaotic piecewise map," Watermark application". Multimedia Tools and Applications, pp. 1-18, 2022.

[15] A. Sanober and S. Anwar, "Crytographical primitive for blockchain: a secure random DNA encoded key generation technique", Multimedia Tools and Applications." pp. 1-18, 2022.

[16] A. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, M. J. Singh, J. K. S. Paw, and M. Amir, "Advancements in intelligent cloud computing for power optimization and battery management in hybrid renewable energy systems: A comprehensive review," Energy Reports, vol. 10, pp. 2206–2227, 2023, doi: 10.1016/j.egyr.2023.09.029.

[17] I. Makhdoom, M. Abolhasan, and J. Lipman, "A Comprehensive Survey of Covert Communication Techniques," Limitations and Future Challenges", Computers & Security, vol. p.102784, 2022.

[18] S. Chowdhury, S. Mistry, A. Goswami, D. Pal, and N. Ghoshal, "Multi Data Driven Validation of E-Document Using Concern Authentic Multi-signature Combinations"," in Proceedings of International Conference on Frontiers in Computing and Systems (pp. 731-743, Singapore: Springer, 2021.
[19] I. A. Barazanchi and H. R. Abdulshaheed, "Designing a library management system for Gazi Husrev-beg library using data structure and algorithm," Herit. Sustain. Dev, vol. 1, no. 2, pp. 64-71, 2020.
[20] A. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, M. J. Singh, J. K. S. Paw, and M. Amir, "Advancements in intelligent cloud computing for power optimization and battery management in hybrid renewable energy systems: A comprehensive review," Energy Reports, vol. 10, pp. 2206–2227, 2023, doi: 10.1016/j.egyr.2023.09.029.
[21] I. A. Barazanchi, "WBAN System Organization, Network Performance and Access Control: A Review," 7th Int. Conf. Eng. Emerg. Technol. ICEET, no. October, pp. 27-28, 2021, doi: 10.1109/ICEET53442.2021.9659564.
[22] A. S. Abdullah, M. A. Abed, and I. A. Barazanchi, "Improving face recognition by elman neural network using curvelet transform and HSI color space," Period. Eng. Nat. Sci, vol. 7, no. 2, pp. 430-437, 2019.
[23] I. A. Barazanchi, H. R. Abdulshaheed, S. A. Shawkat, and S. R. Binti, "Identification key scheme to enhance network performance in wireless body area network," Period. Eng. Nat. Sci, vol. 7, no. 2, pp. 895-906, 2019.
[24] H. H. A., H. R. A. I. Al-Barazanchi, and Z. A. Jaaz, "Practical application of IOT and its implications on the existing software," Conf. Electr. Eng. Comput. Sci. Informatics (EECSI), Yogyakarta, Indones, no. October, pp. 10-14, 2020, doi: 10.23919/EECSI50503.2020.9251302.
[25] M. H. Ali, A. Ibrahim, H. Wahbah, and I. A. Barazanchi, "Survey on encode biometric data for transmission in wireless communication networks," Period. Eng. Nat. Sci, vol. 9, no. 4, pp. 1038-1055, 2021.
[26] I. Al_Barazanchi, "Proposed New Framework Scheme for Path Loss in Wireless Body Area Network," Iraqi J. Comput. Sci. Math, vol. 3, no. 1, pp. 11-21, 2022, doi: 10.52866/ijcsm.2022.01.01.002.
[27] H. R. Abdulshaheed, I. A. Barazanchi, M. Safiah, and B. Sidek, "Survey : Benefits of integrating both wireless sensors networks and cloud computing infrastructure," Sustain. Eng. Innov, vol. 1, no. 2, pp. 67-83, 2020.
[28] Z. A. Jaaz, I. Y. Khudhair, H. S. Mehdy, and I. A. Barazanchi, "Imparting Full-Duplex Wireless Cellular Communication in 5G Network Using Apache Spark Engine," Int. Conf. Electr. Eng. Comput. Sci. Informatics, no. October, pp. 123-129, 2021, doi: 10.23919/EECSI53397.2021.9624283.
[29] A. H. Ali and O. K. J. Mohammad, "Impacting of the E-Platforms on the 4.0th Industrial Educational Revolution," 2019, doi: 10.1145/3361570.3361608.
[30] A. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, J. K. S. Paw, and M. J. Singh, "Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems: Status, Constraints, and Future Recommendations," Sensors, vol. 23, no. 6, p. 2952, 2023, doi: 10.3390/s23062952.
[31] A. H. A. AL-Jumaili, Y. I. Al Mashhadany, R. Sulaiman, and Z. A. A. Alyasseri, "A Conceptual and Systematics for Intelligent Power Management System-Based Cloud Computing: Prospects, and Challenges," Appl. Sci., vol. 11, no. 21, p. 9820, Oct. 2021, doi: 10.3390/APP11219820.