The Investigation of Industry Application Scenarios in Digital Signature

Yuchen Liu
Computer science and technology, Chengdu University of Technology, Erxianqiao Dongsan Rd, Chengdu, Sichuan, China

Keywords: Digital Signature, Security and Trust, Blockchain Technology, Industry Applications, Legal Compliance.

Abstract: The rapid development of the digital era has brought about significant changes in how corporations operate, presenting numerous opportunities along with the challenge of maintaining security and trust in the digital realm. Digital signatures have emerged as a crucial aspect of verifying the authenticity of digital files and providing legally binding signatures. This paper explores the development, applications, and challenges associated with digital signatures in various industries such as digital finance, medical, legal, and government agencies. The discussion includes the use of encryption algorithms and hash functions to ensure secure, verifiable, and tamper-proof signatures. Additionally, the potential of emerging technologies like blockchain, artificial intelligence, and the Internet of Things in shaping the future of digital signatures is delved into. Compliance with laws and regulations and the need for robust private key management systems are identified as key challenges. The integration of blockchain technology is proposed to enhance the security and trust of digital signatures, while artificial intelligence can improve verification processes. Looking ahead, a promising future for digital signatures with increased adoption, global interoperability, and continued advancements in technology and legal frameworks is anticipated.

1 INTRODUCTION

The arrival of digital era completely changed the way that corporation operate, brought mass of opportunities, but also need to face the challenges on maintaining the security and trust, one of them is the verify of the digital file and how to equip legally binding signature. In today's world, where paper-based files are becoming obsolete, the importance and relevance of digital signatures have surged, marking a significant shift in how businesses handle documentation and authentication.

Digital signature can manage to use encrypted algorism to encrypt digital file in order to provide secure, verifiable, and tamper-proof signatures, and it comes with a series of pros, include enhanced security, ease to use, increased efficiency and cost effectiveness. And because of these traits, the digital signature can be trending between big corporations. With new trends such as blockchain, artificial intelligence and the Internet of Things (IoT) continuing development, foresee how these newly trending technologies affect the future picture of digital signatures. Knowing more about these new born technology, deeper connection between the digital signature can be found, which is vital for corporations and organizations to maintain a leading position in this digitalized era. Understanding the nuances of emerging technologies reveals the deeper significance of digital signatures, which is crucial for corporations and organizations striving to stay at the forefront in this digital era.

In terms of the finance industry, digital signature can be important during deal transactions, it can make sure the deal’s security and integrity, prevent tampering and fraud (Weldon 2023). Digital signature can also be used during signing contracts electronically, making them legally binding. For medical industry, it can be used in ensure the security and reliability of electronic medical records. Doctors can use digital signatures to sign diagnostic reports, prescriptions, and medical documents, preventing tampering and protecting patient privacy (Insight Editor 2021). And for legal industry, digital signature plays an important role in signing legal documents and contracts, lawyers and legal agencies can use digital signatures to verify contracts, legal documents and other important documents to ensure their integrity and legal binding. Last is for government agency, government agencies will often go through

Liu, Y.
The Investigation of Industry Application Scenarios in Digital Signature.
DOI: 10.5220/0012837200004547

In *Proceedings of the 1st International Conference on Data Science and Engineering (ICDSE 2024)*, pages 542-546
ISBN: 978-989-758-690-3

large number of documents and transactions, and digital signatures can improve the efficiency and security (Kruhliakova & Sushko 2020). Government departments can use the digital signature to sign and verify the submitted documents, licenses and government purchase contracts, etc., to make sure their authenticity and legitimacy. The digital signature was first introduced by Diffie et al in 1976, they described the idea of a digital signature scheme, but they only theorized that such schemes existed, then in 1977, Rivest et. al. The inventor of the RSA algorithm created a method that could generate a basic form of digital signature., the foundational technology 'hash algorism' was introduced by Merkle et al in 1979. Finally in 1988 (Stevens 2018), Lotus Notes 1.0, which used the RSA algorithm, became the first widely marketed software package to offer digital signatures, Prior to 2008, the digital signature utilized in PDF file formatting was not an open standard and was not recognized by the International Organization for Standardization (ISO). However, in that year, it became ISO 32000 and was established as an integral component of the file format (SIGNiX 2014).

This paper aiming to discuss the application scenario of the digital signature, and demonstrate different digital signature can be used differently in many application scenarios, research will be carry out between financial, medical, legal, government and other industries, research about how the digital signature change the file management and transaction process, besides, research will also discuss challenge or potential risks of digital signature, like the need for a solid digital key management system and compliance with laws and regulations.

2 METHOD

2.1 PKCS #1: RSA Cryptography Standard

Public-Key Cryptography Standards (PKCS), is a series of standards, and #1 is the most basic standard, it provides standards for implementing. Public key cryptographic encryption schemes and digital signatures based on the RSA algorithm are defined in terms of the basic format of the RSA public key function.

This includes the calculation of the digital signature, encompassing both the signature data and its format. An RSA key pair consists of a public key and a private key. The public key contains the modulus (n) and the public exponent (e), besides the private key includes the modulus (n) and the private exponent (d) (Cobb 2021). Mathematically speaking, these values are related, are all allowed to encryption with public key and decryption with the private key.

For PKCS#1_PADDING and the RSA algorithm, the length of RSA encrypted data is related to the number of key bits. Common key lengths include 1024bits and 2048bits. Theoretically, the maximum length of data that can be encrypted with a 1024bits key is 1024bits (1024/8 = 128bytes). The padding pattern is provided in Table 1.

PKCS#1padding V1.5 is the default padding method for RSA encryption and decryption. When performing RSA operations, you need to convert source data D to Encryption block (EB). The padding mode of pkcs1padding V1.5 works as follows (Wang 2012).

$$EB = 00 + BT + PS + 00 + D \qquad (1)$$

EB： Is the filled hexadecimal encrypted data block, the length is 1024/8 = 128 bytes (if the key length is 1024 bits)

00：It starts with 00 and is a reserved bit

BT：In the current version, there are three values 00, 01, 02, BT is 02 (encryption) if operated with the public key, and may be 00 or 01 (signature) if operated with the private key.

PS：Fill bit, PS = K-3D bytes, k represents the byte length of the key, if using 1024bit RSA key, k=1024/8=128 bytes, D represents the byte length of plaintext data D, if BT is 00, PS is 00, if BT is 01, PS is FF, If BT is 02, PS is a randomly generated byte of data other than 0x00.

00：The last byte before the source data D is represented by 00

D：Actual source data

As can be observed from the method, when the RSA_PKCS1_PADDING is used, BT=2, and PS filled before plaintext is a random value, so the ciphertext was caught by the same plaintext and the same public key encryption is different, which improves the security of RSA algorithm. Since the PKCS#1 specification advises that the minimum length of PS is 8, the maximum plaintext length which can be encrypted is the key length (-3) + (-8), which is less than or equal to length -11.

Table 1: Padding Pattern In & Output.

Padding pattern	Input	Output
RSA_PKCS1_ PADDING	It must be at least 11 bytes shorter than the RSA key, which is RSA_size(rsa) -11	As long as the private key
RSA_PKCS1_OAEP_ PADDING	RSA_size(rsa) – 41	As long as the private key
RSA_NO_PADDING	It can be as long as the RSA key. If the plaintext input is too long, it must be cut and then filled	As long as the private key

2.2 Hash Algorithm

Commonly, it's thought that hashing is merely a security feature in digital signatures, yet technically, hashing is not a cryptographic algorithm in the traditional sense. This distinction arises because encryption will always relate to decryption, but actually hash algorithm is a one-way cryptosystem, it is an irreversible mapping from plaintext to ciphertext, only the encryption process, no decryption process. A fixed-size result obtained by applying a one-way mathematical function to any amount of data. If there is a change in the input data, the hash will also change. So, it can easily be used in ID verify and digital signature.

In recent times, the hash algorithms MD5 and SHA-1 have gained significant popularity and are extensively used. It is worth noting that these algorithms are developed on the foundation of MD4, serving as their basis. The details are outlined as follows.

(1) MD4

Message Digest, or MD4 (RFC 1320), was created in 1990 by Ronald L. Rivest of MIT. It is based on 32-bit operand operations and is implemented using fast software on 32-bit word processors (Ronald 1990).

(2) MD5

Rivest created MD5 (RFC 1321) as an enhanced version of MD4 in 1991. Similar to the MD4, it still groups the input into 512-bit words and outputs a cascade of four 32-bit words. Although MD5 is slower and more difficult than MD4, it is more secure and excels in anti-analysis and anti-differential (Rivest 1992).

(3) SHA-1 and others

SHA1, formulated by NIST and NSA, was specifically created to complement DSA, offering a 160-bit hash value for inputs shorter than 264 in size. As a result, it offers enhanced resilience against brute-force attacks. Similar to MD4, SHA-1 was developed following the same foundational principles and imitates its algorithmic approach (NIST 2022).

Furthermore, the three most widely utilized hashing techniques are:

(1) The direct addressing method involves utilizing the keyword itself or a linear function value derived from the keyword as a hash address. Thus, H(key) can be represented as key or H(key) = a * key + b, where a and b are fixed constants. This hash function is commonly referred to as the self-function.

(2) Random number method: Select a random function, take the random value of the keyword as the hash address, usually used for occasions with different keyword lengths.

(3) The residual method involves determining the hash address by taking the remainder of dividing the keyword by a value p, where p is less than or equal to the length of the hash table, denoted as m. In other words, H(key) is calculated as key MOD p, where p is chosen to be a prime number or m. This method allows for direct modulation of the keyword or modulation after performing folding and squaring operations. It is crucial to carefully select the value of p, as poorly chosen values can result in synonymous hash addresses (Zhang & Chum 2010).

3 DISCUSSION

The development of digital signature has completely changed many industries, including finance, medical, law enforcement and government agency. However, there are some digital signature-related challenges and potential risks that are still required to be solved.

3.1 Private Key Management System

One of the challenges of realizing digital signature is to build a safe private key management system. Digital signatures are heavily dependent on RSA and similar encryption algorithms, making the security of private keys crucial. Organizations must ensure the secure storage of these keys, guarding against unauthorized access or data breaches. Additionally, it's important to implement key revocation and update procedures to mitigate the risks associated with key loss (Tomkevičiūtė 2023).

3.2 Complying with Laws and Regulations

The other aspect which also need to consider is to identify if the digital signature is comply with laws and regulations. Different country or jurisdiction has its own legal framework governing the use of digital signatures, such as the Global and National Commercial Electronic Signatures Act (ESIGN) in the United States (Aswathy 2023). Organizations must ensure that their digital signature solutions comply with these regulations to ensure the legal validity of digitally signed documents.

3.3 Potential Risks

Although there are plenty advantages for using the digital signature, but it still necessary to solve potential risks. One of the risks is the possibility of cryptographic vulnerabilities in the algorithms used for digital signatures. As computer's computing power increases, older algorithms may become more vulnerable to attack (Hart 2022). Continuous monitoring and updating of encryption algorithms are essential to solve such risks.

3.4 Blockchain and Emerging Technologies

The appearance of blockchain technology has the potential to further improve the security and trust of digital signatures. By taking advantage of blockchain's decentralized and immutable features, digital signatures can be securely stored and verified, providing an additional layer of trust. In addition, emerging technologies such as artificial intelligence and the Internet of Things (IoT) are also likely to have a significant impact on the future of digital signatures, enabling more seamless integration and automation across industries (Shin 2019).

3.5 Future Prospects

Looking ahead, the prospects for digital signatures are very promising. With advancements in blockchain technology, a more secure and trustworthy environment for digital signatures can be established. Blockchain-based digital signature solutions can provide an immutable signature record, ensuring the integrity and authenticity of documents. In addition, the mix of artificial intelligence and machine learning algorithms can improve the efficiency and accuracy of the digital signature verification process (Sahana et al. 2023) due to their excellent performance in many tasks (Qiu et al. 2022). These techniques can analyze patterns and identify errors to detect any potentially fraudulent activity or tampering attempts. Besides, the continued development of international standards for digital signatures and cross-border identification can promote global adoption and interoperability (Pourhabibi 2020). Efforts to harmonize legal frameworks and establish mutual recognition agreements can further promote the acceptance of digital signatures in different countries and industries.

4 CONCLUSION

In conclusion, this paper provides a comprehensive overview of digital signatures, encompassing their development, application scenarios, and related challenges. The PKCS #1: RSA Cryptography Standard and hash algorithms are discussed as fundamental methods in implementing digital signatures. Nonetheless, the management of private keys and compliance with laws and regulations remain significant challenges. The potential risks associated with cryptographic vulnerabilities and the impact of emerging technologies such as blockchain, artificial intelligence, and the Internet of Things are also highlighted.

In the discussion section, the promising future prospects for digital signatures are explored, including blockchain-based solutions, AI-driven verification, and the development of international standards. The limitations are acknowledged and plans for future research and improvement are outlined. Overall, this research contributes to a deeper understanding of digital signatures and their significance in various industries. It envisions a future where digital signatures are widely adopted globally, ensuring higher levels of security and interoperability through technological advancements and legal frameworks.

REFERENCES

D. Weldon How do digital signatures work? https://www.techtarget.com/searchContentManagement/tip/How-do-digital-signatures-work (2023)

Insight Editor. 6 Reasons E-Signatures Are a Crucial Shift for Healthcare. https://www.insight.com/en_US/content-and-resources/2021/6-reasons-e-signatures-are-a-crucial-shift-for-healthcare.html (2021)

V. Kruhliakova, and V. Sushko, 'Prospects for the Use of Electronic Digital Signature by Government

Authorities and Agencies', Modern Economics, https://www.researchgate.net/publication/342268075_Prospects_for_the_Use_of_Electronic_Digital_Signature_by_Government_Authorities_and_Agencies (2020)

H. Stevens, HANS PETER LUHN AND THE BIRTH OF THE HASHING ALGORITHM. https://spectrum.ieee.org/hans-peter-luhn-and-the-birth-of-the-hashing-algorithm (2018)

SIGNiX. Infographic: The History of Digital Signature Technology. https://www.signix.com/blog/bid/108804/Infographic-The-History-of-Digital-Signature-Technology#:~:text=Here%20are%20some%20of%20the%20milestones%20in%20the,a%20kind%20of%20primitive%20digital%20signature%20More%20items 2014

M. Cobb, RSA algorithm (Rivest-Shamir-Adleman). https://www.techtarget.com/searchsecurity/definition/RSA (2021)

Y. G. Wang, Public-Key Cryptography Standards: PKCS. https://arxiv.org/pdf/1207.5446v1.pdf (2012)

L. Ronald, The MD4 Message Digest Algorithm. https://dspace.mit.edu/bitstream/handle/1721.1/149165/MIT-LCS-TM-434.pdf?sequence=1 (1990)

R. Rivest, The MD5 Message-Digest Algorithm. https://www.rfc-editor.org/rfc/rfc1321 (1992)

NIST. NIST Retires SHA-1 Cryptographic Algorithm. https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm (2022)

X.W. Zhang, and C.S. Chum A New Scheme for Hash Function Construction. https://www.cs.csi.cuny.edu/~zhangx/papers/P_2010_SAM_Chum_Zhang_1.pdf (2010)

A. Tomkevičiūtė, Digital signature: all you need to know. https://cybernews.com/privacy/digital-signature-guide/# (2023)

K. Aswathy, Digital signature vs. electronic signature: What's the difference. https://www.legalzoom.com/articles/digital-signature-vs-electronic-signature-whats-the-difference (2023)

L. Hart, What are the pros and cons of electronic signatures? https://www.techtarget.com/searchcontentmanagement/answer/252523027/What-are-the-pros-and-cons-of-electronic-signatures (2022)

D. D. H. Shin, Blockchain: The emerging technology of digital trust, Telematics and Informatics, Volume 45 (101278), https://www.sciencedirect.com/science/article/abs/pii/S0736585319307701 (2019)

J. M. Sahana, et al. A Study on Digital Signature in Blockchain Technology. https://ieeexplore.ieee.org/document/10073680 (2023)

Y. Qiu, et al. Pose-guided matching based on deep learning for assessing quality of action on rehabilitation training. Biomedical Signal Processing and Control 72 (2022): 103323.

T. Pourhabibi, et al. Fraud detection: A systematic literature review of graph-based anomaly detection approaches, Decision Support Systems (2020)