ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 10 (2023) No. 4, pp.174-188
DOI:10.33168/JLISS.2023.0412

Strengthening the Security and Privacy of National Identity Numbers (NINs) in Smart Contract Mechanisms through AES Encryption

Irwan Sembiring , Danny Manongga , Septovan Dwi Suputra Saian

Faculty of Information Technology, Satya Wacana Christian University 50711, Indonesia

irwan@uksw.edu (Corresponding author), dmanongga@uksw.edu, septovan.ovan@gmail.com

Abstract. National Identity Numbers (NINs) or Similar identification numbers issued by the government are considered sensitive personal information that needs to be protected from theft or unauthorized access. In 2022, the Ministry of Communications and Informatics in Indonesia reported 33 incidents related to violations of personal data protection. Data breaches of national identity information are serious cases that can have detrimental consequences for individuals and society. If the security of such systems is inadequate, NIN data can be hacked or stolen by unauthorized parties. The current storage applications for personal data still rely on centralized systems. In a centralized system, all control, decision-making, and data are concentrated within a central authority or entity. This central authority has full control over the system and can make decisions on behalf of the entire system. Centralized systems have drawbacks in terms of privacy and data security because they are fully controlled by a central entity or server. NIN smart contracts on the blockchain provide a solution due to their decentralized and immutable nature. Smart contracts offer a higher level of protection, enhancing security and privacy. In a decentralized system, decision-making and control are distributed among multiple participants or nodes, eliminating the need for a central authority. Participants in the system work together to achieve consensus and maintain system operations. Data is typically distributed and stored across multiple nodes, and participants have more autonomy and control over their data. The popular encryption technique AES offers essential security for sensitive data. Smart contract mechanisms automatically encrypt all transactions and data and validate the stored data on the blockchain to prevent unauthorized access. This is achieved by integrating AES 256 and SHA-256 encryption. This research aims to develop a dApps population management system using blockchain and proof-of-stake consensus. The goals include enhancing privacy, data security, user autonomy, and transparency by eliminating central authorities and enabling peer-to-peer interactions. The impact of this research is to reduce incidents of personal data breaches.

Keywords: National Identity Numbers (NINs), Smart contract, Blockchain

1. Introduction

Hackers employ various techniques to steal national identification numbers. Phishing is a common tactic where individuals are tricked into revealing their NINs through fraudulent emails, text messages, or phone calls. Phishing scams are difficult to recognize as they often utilize authentic-looking designs and strategies. (Atanassov & Chowdhury, 2021). Social engineering strategies are often used by hackers to obtain personal data, such as NINs. Hackers impersonate reputable authorities to gain the trust of their victims, allowing them to disclose their identities. (Al-Essa, 2019)(Alqaralleh et al., 2021),(Antal et al., 2021) Data breaches that grant hackers access to a large amount of personal data, including NINs, can occur in organizations that store NINs or other sensitive personal information. When a business does not have strong security procedures in place to protect sensitive data, it becomes vulnerable to such data breaches. (Seh et al., 2020).

Hackers can physically steal documents or items containing NINs. This can occur through theft or unauthorized access to physical documents or electronic devices that store personal information. It is important to securely store and handle physical documents or items that contain sensitive information to prevent unauthorized access or theft. This can occur as a result of theft or unauthorized access to physical documents or technological devices that contain personal data(Singh, 2021). In 2022, the Ministry of Communications and Informatics of Indonesia reported 33 incidents related to violations of personal data protection (Arum Titah, 2022).

Account takeover is a serious issue where an attacker can exploit a victim's online account using a stolen NIN, especially if the NIN is used as a login credential. The attacker can use the stolen NIN to change passwords, gain access to the victim's emails or phone numbers, or engage in financial fraud. Stolen NINs can be used to apply for loans or other financial products, open bank accounts or credit cards without the victim's permission, and leave the victim in debt. Attackers can also use social engineering strategies, posing as legitimate businesses or government representatives, to gain the victim's trust and extract more personal information or money from them. Identity theft using a stolen NIN can enable impersonation of the victim, granting illegal access to personal information, bank accounts, and other sensitive data.

A decentralized system, where one of its characteristics is immutability, provides a high level of security. AES encryption can be used to enhance the security and privacy of blockchain technology. AES, also known as the Advanced Encryption Standard, is a widely recognized encryption method that offers strong security for sensitive data. By integrating AES encryption into the blockchain system, all transactions and data stored on the blockchain can be secured using a secure key. This ensures that unauthorized access to data can be prevented, even if the blockchain is compromised (X. Chen, 2020)(Al-Essa, 2019).

AES encryption is also important to ensure anonymity in the blockchain process. In a blockchain system, transactions are typically tracked in a public ledger that is accessible to everyone. However, by encrypting the information using AES, only individuals with the appropriate encryption key are allowed to access and decrypt it. This greatly enhances the privacy and confidentiality of the blockchain system. With its decentralized and secure nature, the use of blockchain technology continues to strengthen its appeal (Benil & Jasper, 2020). Individuals' personal information is better protected by enhancing the security and privacy of NINs in smart contract blockchain, resulting in increased transparency, trust, and efficiency in NIN administration (Khan et al., 2021).

The study focuses on improving the security and privacy of NINs in smart contract mechanisms through the implementation of AES encryption. This research proposes a prototype privacy data protection system for NIN in Indonesia using blockchain technology, transitioning from a centralized data protection system to a decentralized one. The research aims to minimize the issue of data breaches.

2. Literature Review

2.1. Secure and Efficient Privacy-Preserving Authentication Scheme in Blockchain.

Fathiyana (Fathiyana et al., 2020) claims that the duplication and redundancy of population data are caused by a lack of coordination in integrating information systems across government entities issuing identification numbers. Blockchain can facilitate data integration between organizations and is a secure and reliable mechanism for maintaining the identification details of individuals. The strength of this research lies in conducting duplicate checks, but it does not discuss security resilience.

Antal (Antal et al., 2021) claim that the duplication and redundancy of population data in population information is due to a lack of coordination in integrating information systems across government departments issuing identification numbers. Blockchain is considered a reliable and secure mechanism for storing the identification records of individuals and can also facilitate data integration across organizations. The strength of this research lies in the integration of data between organizations through a decentralized network, but it does not address the data integrity and validation processes used.

Akhter et al. (Suaib Akhter et al., 2021) on the Internet of Vehicles (IoV), a secure and private blockchain authentication system, has been designed. Blockchain, created on the Ethereum platform and utilizing digital signature methods to ensure confidentiality, non-repudiation, integrity, and privacy of IoV, is used to store and manage authentication information in a distributed and decentralized environment. Numerical analysis is used to validate the proposed cooperative protocol and shows that the protocol successfully improves system throughput while reducing the Packet Dropping Rate (PDR). The strength of the research lies in data integrity and communication speed, while the weakness is the lack of discussion on validation techniques in this system.

Guerrero-Sanchez (Guerrero-Sanchez et al., 2020) suggests a solution based on the security benefits offered by blockchain and the use of cryptographic tools to help maintain data availability and integrity. The accuracy of the proposed methodology is evaluated using a Wireless Sensor Network (WSN) supported by the Internet of Things to sense temperature and humidity. The collected findings indicate that the idea meets the main criteria for an IoT system. It is independent, secure for the exchange and transmission of information between devices and users, ensures the transmission of personal data, is reliable, and the information can be accessed within the infrastructure. The results of this research demonstrate that this technique is more resilient to common attacks on IoT systems, including connection attacks, man-in-the-middle attacks, and distributed denial of service (DDoS) attacks.

Arunkumar (Arunkumar & Kousalya, 2020) states that to address privacy and security concerns when sharing patient healthcare data among various medical institutions; there is a need for a secure, decentralized cloud-based Medical Blockchain (CMBC) development. To enhance the performance of healthcare services, data from Electronic Health Records (EHRs) are encrypted using lightweight encryption techniques authenticated with AES_256_GCM before being uploaded to the cloud-based blockchain. Atanassov & Chowdhury, 2021 focuses on (1) network communication and smart contract attack methods and defenses for blockchain security issues, such as distributed denial of service (DDoS) attacks, Sybil attacks, eclipsing attacks, and reentrancy attacks in medium protocol attacks; and (3) privacy theft attack methods and defenses for blockchain security issues, such as block withholding, 51% attacks, pool hopping, selfish mining, and fork after withholding attacks in consensus-based attacks (Y. Chen et al., 2022)(Azeez et al., 2020).

Azeez et al . (Azeez et al., 2020) researched to protect internet users from phishing attacks, and many anti-phishing models have been proposed. The methods currently used to address this issue are inadequate and not entirely successful. By examining the conceptual and literal coherence between the unified resource locator (URL) and online content, they hope to identify phishing websites and protect internet users from falling victim to various types of phishing attacks. The proposed PhishDetect approach has been implemented and achieved an accuracy rate of 99.1%, demonstrating its effectiveness in identifying various phishing attacks.

2.2. The Encryption Techniques Used in Blockchain

Internet users can now be protected from phishing attacks using various anti-phishing models. The methods currently used to address this issue are inadequate and not entirely successful. By examining the conceptual and literal coherence between the unified resource locator (URL) and online content, we hope to identify phishing websites to prevent internet users from falling victim to various types of phishing attacks. The adopted phishing detection approach achieves an accuracy rate of 99.1%, demonstrating its effectiveness in identifying different phishing attempts (Krishnapriya & Sarath, 2020)(Fotohi & Shams Aliee, 2021)(Ranjith Kumar & Bhalaji, 2021).

A single key is used in symmetric encryption to encrypt and decrypt data. This method is commonly used to encrypt recorded information in the blockchain, such as user information and transactions (Guo et al., 2020)(Ma et al., 2021)(Acquah et al., 2020).

Data is encrypted and decrypted using a pair of keys called the public key and private key in asymmetric encryption, sometimes referred to as public-key cryptography. This technique is often used in blockchain to encrypt communication exchanged between users or to digitally sign transactions (Chowdhary et al., 2020; Dubovitskaya et al., 2020; Dutta et al., 2020; Ge et al., 2021; Gong et al., 2022; Hasan et al., 2021; Mansouri & Wang, 2021; Mousavi et al., 2021; Thirumalai et al., 2020; Ye et al., 2020).

Public key cryptography, known as elliptic curve cryptography (ECC), is widely used in blockchain to ensure the accuracy of transactions and data. Zero-knowledge proofs (ZKPs) are a technique used to prove the validity of a claim without revealing any additional information. ZKPs are often used in blockchain to protect the privacy of transaction participants or to verify the accuracy of data (Alqaralleh et al., 2021; Benil & Jasper, 2020; Chandel et al., 2020; Christo et al., 2021; Ghayvat et al., 2022; Ghimire et al., 2020; Kaur et al., 2021; Kim et al., 2020; Neelakandan et al., 2022; Ngabo et al., 2021; Saini et al., 2021; Suhail et al., 2021; Wang et al., 2021; Yu et al., 2020). Lee (Lee et al., 2022).

Blockchain typically employs elliptic curve cryptography (ECC), a type of public key encryption, to ensure the accuracy of transactions and data. Zero-knowledge proofs (ZKPs) are a method to prove something is true without revealing further details. In blockchain, ZKPs are often used to protect the privacy of transaction participants or to verify the accuracy of data (Krishnapriya & Sarath, 2020). Using blockchain for land registration has significantly reduced security issues.

The computed hash value for each block will be different because it is linked to the hash of the previous block. The SHA256 algorithm is commonly used for hashing. In addition to SHA256, the Proof of Work (PoW) method is also employed, enhancing the security of transaction-related data. Each hash in the message digest generated for a specific block reflects the entire sequence of transactions included in that block and has a fixed size. A network of 12 nodes is planned for the land registration blockchain. These nodes perform tasks such as verifying transactions, mining new blocks, and uploading them to the blockchain. With the blockchain approach, which offers tamper-proof evidence and the latest version of land registration, nearly 200 land transactions have been recorded. Elliptic curve cryptography is used to create signatures that can be used to confirm that transactions are signed by the appropriate parties. Hash links between transactions are created using a Merkle tree, which requires less storage space. By proposing the use of blockchain for land registration, manual record-keeping work can be reduced by up to 99%.

2.3. The MixColumns Function

The MixColumns function is an operation performed in the AES (Advanced Encryption Standard) encryption algorithm. It operates on the columns of the state matrix during the encryption process. The newly converted columns are generated by the MixColumns function, which multiplies each column with a preset matrix. This transformation helps in the dispersion and mixing of data, thereby strengthening the cryptographic capabilities of the AES algorithm. (Huy et al., 2019). The constant values used in Equation 1.

$$\begin{bmatrix} S'0 \\ S'1 \\ S'2 \\ S'3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 \\ 01 & 02 & 01 \\ 01 & 01 & 03 \\ 03 & 01 & 02 \end{bmatrix} X \begin{bmatrix} S0 \\ S1 \\ S2 \\ S3 \end{bmatrix} \quad (1)$$

Equation 2 represents matrix multiplication (Huy et al., 2019).

$$S'_0 = (02 \cdot S_0)\ XOR\ (03 \cdot S_1)\ XOR\ (01 \cdot S_2)\ XOR\ (01 \cdot S_3) \quad (2)$$

Similar to MixColumn(), InvMixColumn() uses constants defined in Equation 3 (Lee et al., 2022)(Huy et al., 2019). The values described in the decimal form need to be converted to bytes before operating.

$$\begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \quad (3)$$

3. Methodology

The privacy data security system for NINs dApps is developed using the Remix editor and the Solidity programming language. This application is called "population management dApps," where all data communication is hashed and encrypted using the Ether.js and Crypto.js libraries. Every query for NINs data and validation process for gas fees is done using Metamask.

3.1. Flow Client Library and Key Expansion Development.

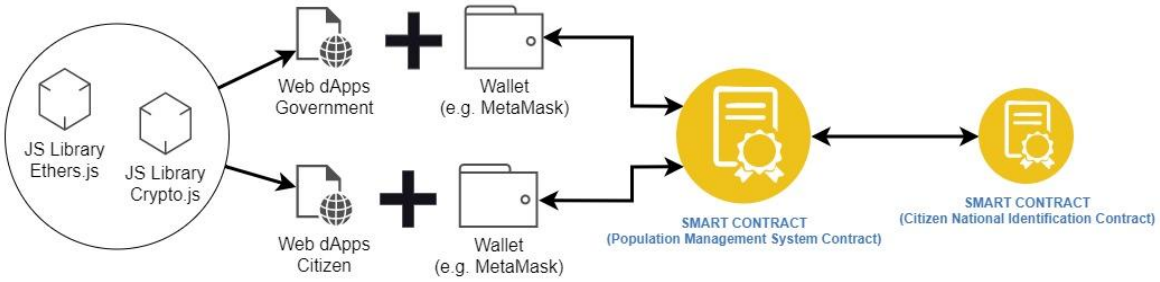


Fig.1: Flow Client Library and Key Expansion Development

Figure 1 illustrates an example of this procedure where ether.js and crypto.js are used in the client library channel when creating dApps. Before the smart contract consensus phase, the procedure involves transforming input data and keys into byte arrays and generating key expansion.

3.2. The Architecture of a Population Management DApps's Smart Contract.

The functionality of the dApps is centered around the smart contract layer. These are self-executing contracts stored on the blockchain that automatically enforce predefined rules and conditions. User registration, identity verification, data storage, and access control are all handled through smart contracts. The infrastructure for the dApps is provided by the blockchain layer, offering a secure and decentralized setup to manage and store population control data. All transactions and interactions within the dApps are recorded in an immutable ledger maintained by the blockchain. The data required for the population management system needs to be stored and managed by the data storage layer. Depending on the dApps's requirements and architecture, it may involve a standard database or a decentralized storage system. The dApps can communicate with external systems and services thanks to the integration layer. This facilitates integration and data sharing with other platforms or applications, such as public databases, identity verification services, or external APIs. These components can be visualized

as illustrated in Figure 2.

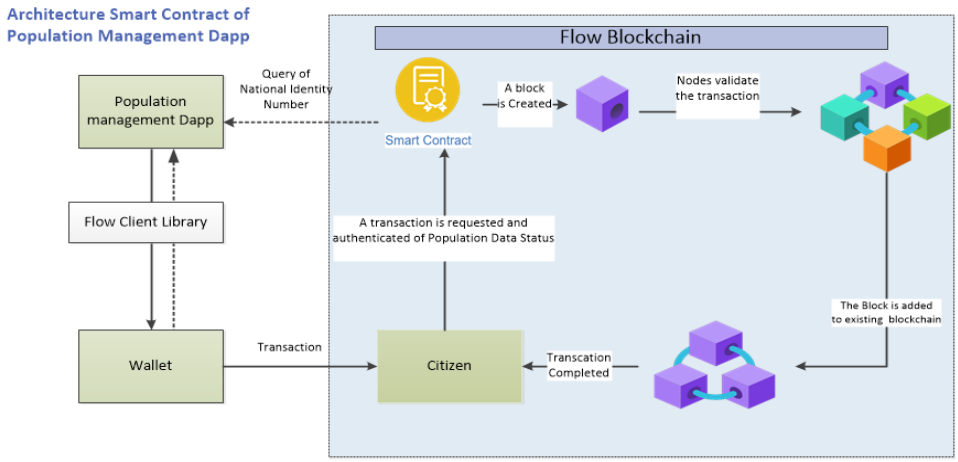


Fig.2: Smart Contract Architecture for Population Management dApps

4. Result and Analysis

This experiment was conducted on hardware with the following specifications: Intel Core i3-4030U CPU, 8 GB RAM, and an average bandwidth of 64 Mbps. 4.1 Transforming a 128-bit key into an array of bytes. The key data is influenced by the value of Nk. The influence lies in the size of the array, which is 4xNk. Therefore, the array size for a 128-bit key is 4x4, 192-bit is 4x6, and 256-bit is 4x8. This process can be seen in Figure 3, which illustrates the transformation of a 128-bit key into an array of bytes with a size of 4x4.

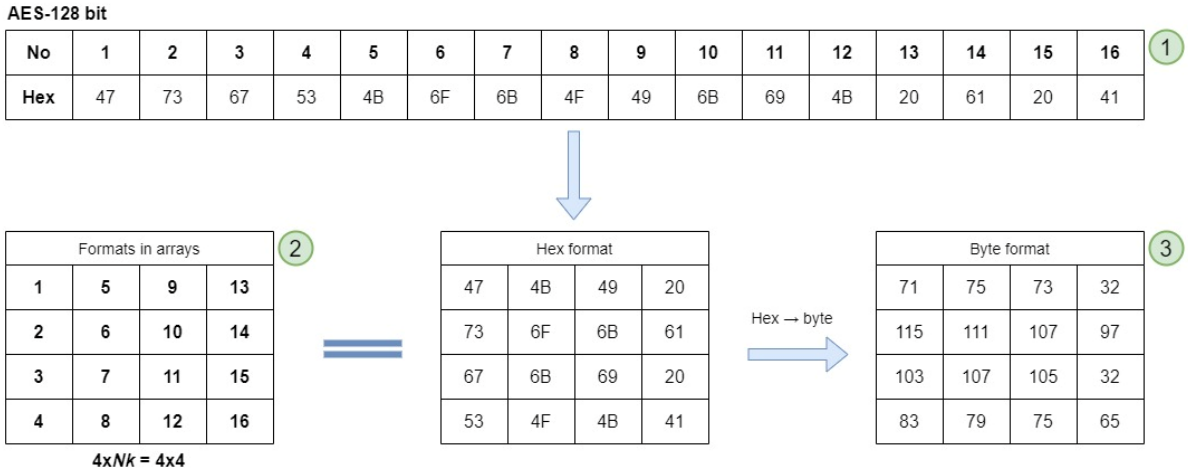


Fig.3: Transforming a 128-bit key into a byte array.

The key is transformed into a 4xNk byte array to create the input data at this stage. Figure 3 shows that each column in the array is referred to as a word. Depending on the key being used, the key expansion is generated by creating Nb (Nr + 1) words.

4.1. Key Expansion Generation

The input data at this stage is the result of transforming the key into a 4xNk byte array. Figure 4 depicts that each column in the array is referred to as a word. Key expansion generation involves generating Nb (Nr + 1) words, depending on the key being used. This generation is done through a function called

g. Function g involves manipulations such as SubWord (), RotWord (), and Rcon (). The pseudocode for the function g can be seen in Figure 8. The result of this function is to create a collection of 4xNb or 4x4, or 128-bit byte arrays with a total count of Nr + 1. This is referred to as the expansion key round. Therefore, if a 128-bit key is used, it results in 11 expansion key rounds, a 192-bit key results in 13 expansion key rounds, and a 256-bit key results in 15 expansion key rounds—an illustration of the expansion key round.

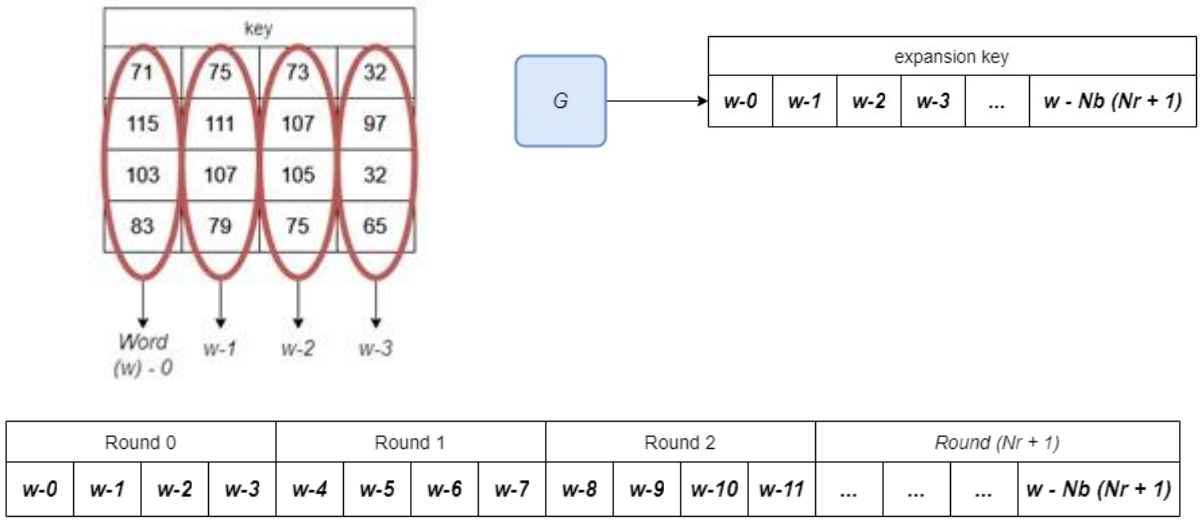


Fig.4: Key expansion generation

Figure 4 shows the derivation of this procedure, and the function g (generate) involves manipulations that include operations like SubWord(), RotWord(), and Rcon(). The pseudocode for the function g can be seen in Figure 5.

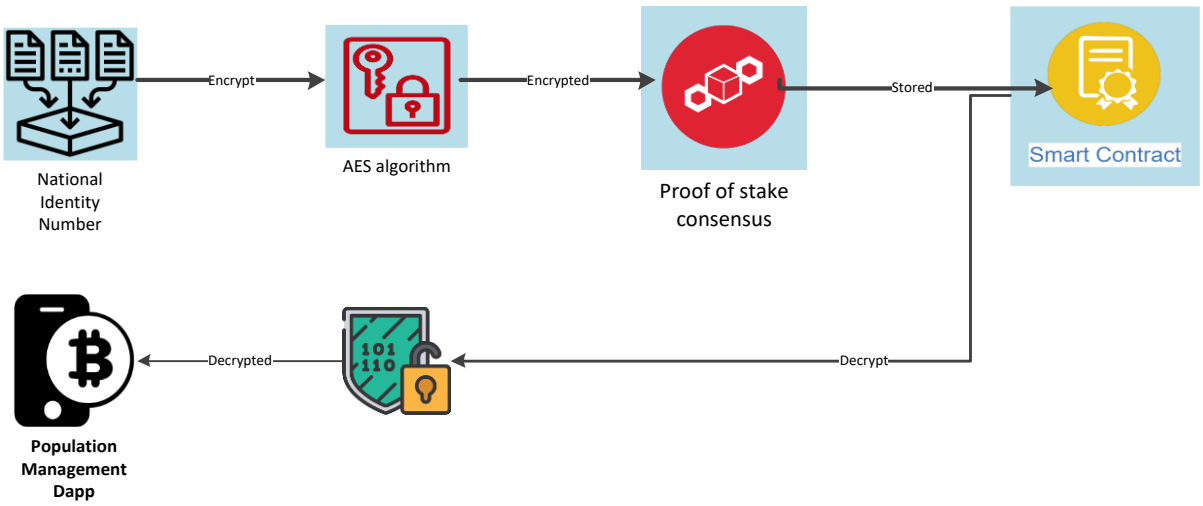
```
KeyEpansion (byte key[Nb, Nk], int Nb, int Nr, int Nk)
begin
  result_keys, result_keys_block

  for(i=0, i < Nk, i++)
  begin
    byte word

    for(iRow=0, iRow < Nb, iRow++)
    begin
      word[iRow, 0] = key[iRow, i]
    end

    result_keys.push(word)
  end

  for(i = Nk, i < Nb * (Nr+1), i++)
  begin
    byte[] word = result_keys[i-1]

    if (i mod Nk)
    begin
      for(iRow=0, iRow < Nb, iRow++)
      begin
        byte selectedItem = word[iRow, 0]
        SubWord(RotWord(selectedItem))
      end

      word[0, 0] = word[0, 0] XOR Rcon[i/Nk]
    end
    else if (Nk > 6 AND i mod Nb = 4)
    begin
      for(iRow=0, iRow < Nb, iRow++)
      begin
        SubWord(word[iRow, 0])
      end
    end

    byte[] temp
    for(iRow=0, iRow < Nb, iRow++)
    begin
      temp[iRow, 0] = result_keys[i-1][iRow, 0] XOR word[iRow, 0]
    end

    result_keys.push(temp)
  end

 result_keys_block = SplitToBlock(result_keys, Nb)
 return result_keys_block
end
```

```
SplitToBlock(byte result_keys[], Nb)
begin
  result_keys_block
  int indexResult = 0
  int columnIndex = 0
  byte[] expandedKey

  foreach(item in result_keys)
  begin
    for(i=0, i < Nb, i++)
    begin
      expandedKey[i, columnIndex] = item[i, 0]

      if(columnIndex != Nb)
      begin
        columnIndex++
      end
      else
      begin
        result_keys_block.push(indexResult, expandedKey)
        columnIndex = 0
        indexResult++
      end
    end
  end

  return result_keys_block
end
```

Fig.5: The Pseudocode for The Function g

4.2. Encryption and Decryption Process.

The data to be encrypted is first translated into a suitable format for encryption, such as a byte array. The symmetric encryption key is then generated or obtained. The data is then encrypted using the generated encryption key using symmetric encryption methods like AES. The encrypted data is securely stored in a variable or storage location within the smart contract. During the decryption process, the encrypted data is retrieved from the smart contract storage. The required decryption key is obtained, which is used during the encryption procedure. The data to be encrypted is first translated into a suitable format, such as a byte array, before initiating the encryption process. Afterward, the symmetric encryption key is generated or obtained. The generated encryption key is then used to encrypt the data using symmetric encryption methods like AES. The smart contract securely stores the encrypted data, typically in a variable or storage location. During the decryption procedure, the encrypted data is retrieved from the smart contract storage. The required decryption key from the encryption procedure is obtained, as illustrated in Figure 6.



Plain Text	Key	Encrypted Text
{“Nins” “001122334455667788”	Ox50239e16…Bd4ab39d26	U2FsdGVkX1+…0HL7Kh3Q==

Fig.6:.Encryption and decryption text

4.3. Consensus Mechanism

Consensus algorithms are crucial in maintaining network uniformity and agreement in blockchain networks. Proof of Stake (PoS) is a well-known consensus algorithm. In a proof-of-stake (PoS) system, validators are selected based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. This selection process ensures that validators have a stake in maintaining the security and integrity of the blockchain. Blockchain networks can achieve consensus on the state of the blockchain and the execution of smart contracts by using consensus algorithms such as PoS. Creating new blocks and validating transactions help protect the network and ensure the accuracy of transaction data. The security of a blockchain includes vital steps like transaction validation. This helps maintain the validity, confidentiality, and integrity of transactions and blockchain data. Validators ensure accurate transactions, prevent fraud or other malicious behavior, and ensure that only valid transactions are recorded on the blockchain. Transaction validation techniques and consensus algorithms like PoS are crucial elements of blockchain security that enhance the reliability and trustworthiness of the overall network.

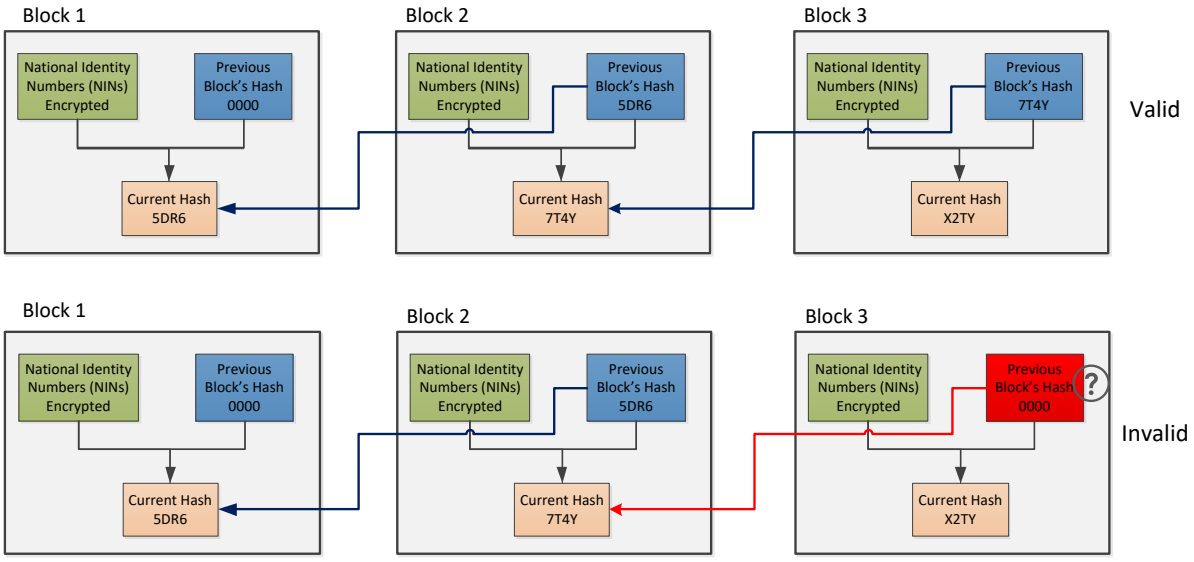


Fig.7:Consensus Proof of Stake (PoS)

The Consensus Mechanism is the validation of the encryption process through the consensus mechanism used in the blockchain network. Consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) ensure agreement among network participants and provide an additional layer of security for encrypted data. The SHA-256 hashing function ensures strong and secure data integrity and security for the encrypted data, As shown in Figure 7.

4.4. Evaluation Criteria.

The evaluation criteria in this research, as shown in Table 1, demonstrate an improvement in security performance by using the AES algorithm in the blockchain system.

Table 1. Evaluation criteria

Criteria	Description	Result
Encryption/decryption time	AES 256	52 MS
Consensus Mechanism	Proof of Stake	Enhanced
Secure Hashing	SHA-256	Enhanced
Access control	Smart Contract-Based Access Control	Enhanced
Storage	AES 256	9 MB

4.5. Discussion

This includes discussing the strengths and weaknesses of the approach, comparing it with existing methods, and highlighting its advantages and novel contributions. The implementation of NINs in a blockchain system using AES is explained as shown in Table 2.

Table 2 The Strengths and Weaknesses of Using AES

Strengths of AES Encryption	Weaknesses of AES Encryption	Comparison with Existing Methods	Advantages and NovelContributions of the Proposed Approach	Challenges, Limitations, and Risks
Strong Security: AES is a widely recognized	Key Management: The security of AES encryption	Compared to traditional centralized systems,	Integration with Smart Contracts: The proposed	Scalability: As the number of transactions and

encryption algorithm that provides robust protection for sensitive data like NINs	heavily relies on the proper management of encryption keys. Weak key management practices can undermine the effectiveness of the encryption.	using AES encryption in smart contracts offers enhanced security through decentralization and immutability.	approach leverages the decentralized nature of blockchain and the automation of smart contracts to ensure the secure storage and validation of NINs	users increases, the scalability of the blockchain network and the efficiency of AES encryption need to be carefully considered.
Standardization: AES has been adopted as a standard encryption algorithm by various organizations, ensuring its compatibility and interoperability.	Quantum Computing Threat: With the emergence of quantum computing, there is a potential future threat to the security of AES encryption. It is important to consider post-quantum encryption algorithms for long-term security.	Compared to other encryption algorithms, AES is widely recognized and has a proven track record of security, making it a reliable choice for protecting sensitive data like NINs	Data Confidentiality: AES encryption ensures that NINs are protected and can only be accessed by authorized parties with the correct encryption key	Regulatory Compliance: Depending on the jurisdiction, there may be legal and regulatory requirements for handling and protecting sensitive personal information, including NINs
Performance: AES encryption is efficient and can be implemented with relatively low computational overhead, making it suitable for use in smart contracts.			Immutable Audit Trail: The use of blockchain provides an immutable and transparent audit trail, allowing for accountability and traceability of NIN-related activities	User Awareness and Adoption: Ensuring user awareness and adoption of the proposed system is crucial for its successful implementation. User education and trust-building efforts may be needed.

5. Conclusion and Recommendations

5.1. Conclusion

Smart contracts can ensure that NINs (National Identification Numbers) are stored and transferred in an encrypted manner by adopting security mechanisms such as encryption. This prohibits unauthorized access to NINs and helps maintain the security of sensitive personal information. Blockchain technology offers tamper-proof and immutable storage systems. Storing NINs in the blockchain ensures that data is securely stored and cannot be altered without the consensus of network participants. As a result, NINs become more trustworthy and have greater integrity. Blockchain-based smart contracts can define open access control measures for NINs. Only authorized parties can access and use NINs if access to NINs is controlled by established rules and guidelines. This protects individuals' privacy and

helps prevent unwanted usage. The decentralized operations of blockchain smart contracts do not require a central organization to control NINs. This reduces the likelihood of a single point of failure and decreases the need for reliable intermediaries. It enhances the system's credibility gap and ensures that NINs are handled securely and openly. Blockchain provides transparent and verifiable records of all transactions and operations related to NINs. The ability to track and identify individuals responsible for any changes or access to NINs promotes accountability and prevents criminal activities. Smart contracts streamline the procedures associated with NIN management by automating the enforcement of predefined rules and conditions. This reduces the need for manual intervention, lowers the chances of human errors, and enhances the effectiveness of securely controlling NINs.

5.2. Theoretical and Practical Implications

The theoretically proven impact shows that decentralized systems are capable of enhancing the security of private data. Smart contract mechanisms automatically encrypt all transactions and data and validate the stored data on the blockchain to prevent unauthorized access to data by integrating AES 256 and SHA-256 encryption. This research establishes a population management dApps system using blockchain and proof-of-stake consensus. It improves privacy, data security, user autonomy, and transparency by eliminating central authorities.

5.3. Limitations of Study

Here are some limitations of this research high gas fees. This can impact the cost-effectiveness of the system, especially for frequent or large-scale transactions. Interoperability constraints and Lack of comprehensive attack analysis.

References

Acquah, M. A., Chen, N., Pan, J. S., Yang, H. M., & Yan, B. (2020). Securing fingerprint template using blockchain and distributed storage system. *Symmetry*, *12*(6). https://doi.org/10.3390/SYM12060951

Al-Essa, M. (2019). The Impact of Blockchain Technology on Financial Technology. *FinTech*, *10*(2), 91–107. https://doi.org/10.33168/JLISS.2023.0207

Alqaralleh, B. A. Y., Vaiyapuri, T., Parvathy, V. S., Gupta, D., Khanna, A., & Shankar, K. (2021). Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-021-01543-2

Antal, C., Cioara, T., Antal, M., & Anghel, I. (2021). Blockchain Platform For COVID-19 Vaccine Supply Management. *IEEE Open Journal of the Computer Society*, *2*, 164–178. https://doi.org/10.1109/ojcs.2021.3067450

Arum Titah. (2022). *Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data – Ditjen Aptika*. Aptika.Kominfo.Go.Id. https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data/

Arunkumar, B., & Kousalya, G. (2020). Blockchain-Based Decentralized and Secure Lightweight E-Health System for Electronic Health Records. In *Advances in Intelligent Systems and Computing* (Vol. 1148, pp. 273–289). https://doi.org/10.1007/978-981-15-3914-5_21

Atanassov, N., & Chowdhury, M. M. (2021). Mobile Device Threat: Malware. In *IEEE International Conference on Electro Information Technology* (Vols. 2021-May, pp. 7–13). https://doi.org/10.1109/EIT51626.2021.9491845

Azeez, N. A., Salaudeen, B. B., Misra, S., Damasevicius, R., & Maskeliunas, R. (2020). Identifying phishing attacks in communication networks using URL consistency features. *International Journal of*

Electronic Security and Digital Forensics, *12*(2), 200–213. https://doi.org/10.1504/IJESDF.2020.106318

Benil, T., & Jasper, J. (2020). Cloud-based security on outsourcing using blockchain in E-health systems. *Computer Networks*, *178*. https://doi.org/10.1016/j.comnet.2020.107344

Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., & Ni, T. Y. (2020). A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption. In *Lecture Notes in Networks and Systems* (Vol. 70, pp. 988–1003). https://doi.org/10.1007/978-3-030-12385-7_67

Chen, X. (2020). Implementing AES Encryption on Programmable Switches via Scrambled Lookup Tables. In *Proceedings of the 2020 ACM SIGCOMM Workshop on Secure Programmable Network Infrastructure, SPIN 2020* (pp. 8–14). https://doi.org/10.1145/3405669.3405819

Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confidence Computing*, *2*(2), 100048. https://doi.org/10.1016/j.hcc.2021.100048

Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Kumaresan, P., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. *Sensors (Switzerland)*, *20*(18), 1–19. https://doi.org/10.3390/s20185162

Christo, M. S., Jesi, V. E., Priyadarsini, U., Anbarasu, V., Venugopal, H., & Karuppiah, M. (2021). Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/6966206

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*, *22*(8). https://doi.org/10.2196/13598

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, *142*. https://doi.org/10.1016/j.tre.2020.102067

Fathiyana, R. Z., Hidayat, F., & Rahardjo, B. (2020). An Integration of National Identity towards Single Identity Number with Blockchain. In *Proceedings of the 7th Mathematics, Science, and Computer Science Education International Seminar, MSCEIS 2019*. https://doi.org/10.4108/eai.12-10-2019.2296532

Fotohi, R., & Shams Aliee, F. (2021). Securing communication between things using blockchain technology based on authentication and SHA-256 to improve scalability in large-scale IoT. *Computer Networks*, *197*. https://doi.org/10.1016/j.comnet.2021.108331

Ge, X., Yu, J., Zhang, H., Hu, C., Li, Z., Qin, Z., & Hao, R. (2021). Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification. *IEEE Transactions on Dependable and Secure Computing*, *18*(1), 490–504. https://doi.org/10.1109/TDSC.2019.2896258

Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2022). CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1937–1948. https://doi.org/10.1109/JBHI.2021.3097237

Ghimire, S., Choi, J. Y., & Lee, B. (2020). Using Blockchain for Improved Video Integrity Verification. *IEEE Transactions on Multimedia*, *22*(1), 108–121. https://doi.org/10.1109/TMM.2019.2925961

Gong, L. H., Luo, H. X., Wu, R. Q., & Zhou, N. R. (2022). The new 4D chaotic system with hidden

attractors and self-excited attractors and its application in image encryption based on RNG. *Physica A: Statistical Mechanics and Its Applications*, *591*. https://doi.org/10.1016/j.physa.2021.126793

Guerrero-Sanchez, A. E., Rivas-Araiza, E. A., Gonzalez-Cordoba, J. L., Toledano-Ayala, M., & Takacs, A. (2020). Blockchain mechanism and symmetric encryption in a wireless sensor network. *Sensors (Switzerland)*, *20*(10). https://doi.org/10.3390/s20102798

Guo, Y., Zhang, C., & Jia, X. (2020). Verifiable and Forward-secure Encrypted Search Using Blockchain Techniques. In *IEEE International Conference on Communications* (Vols. 2020-June). https://doi.org/10.1109/ICC40277.2020.9148612

Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., Ciro Rodriguez, R., & Vargas, D. E. (2021). Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications. *Complexity*, *2021*. https://doi.org/10.1155/2021/5540296

Huy, D. Q., Duc, N. M., Khai, L. D., & Lung, V. D. (2019). Hardware implementation of AES with S-Box using composite-field for WLAN systems. *RIVF 2019 - Proceedings: 2019 IEEE-RIVF International Conference on Computing and Communication Technologies*, 1–6. https://doi.org/10.1109/RIVF.2019.8713711

Kaur, K., Kaddoum, G., & Zeadally, S. (2021). Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), 5178–5189. https://doi.org/10.1109/TITS.2021.3068092

Khan, N. A., Altaf, M., & Khan, F. A. (2021). Selective encryption of JPEG images with chaotic-based novel S-box. *Multimedia Tools and Applications*, *80*(6), 9639–9656. https://doi.org/10.1007/s11042-020-10110-5

Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors (Switzerland)*, *20*(10). https://doi.org/10.3390/s20102913

Krishnapriya, S., & Sarath, G. (2020). Securing Land Registration using Blockchain. In *Procedia Computer Science* (Vol. 171, pp. 1708–1715). https://doi.org/10.1016/j.procs.2020.04.183

Lee, Y. L., Lee, H. A., Hsu, C. Y., Kung, H. H., & Chiu, H. W. (2022). SEMRES - A Triple Security Protected Blockchain-Based Medical Record Exchange Structure. *Computer Methods and Programs in Biomedicine*, *215*. https://doi.org/10.1016/j.cmpb.2021.106595

Ma, J., Li, T., Cui, J., Ying, Z., & Cheng, J. (2021). Attribute-Based Secure Announcement Sharing among Vehicles Using Blockchain. *IEEE Internet of Things Journal*, *8*(13), 10873–10883. https://doi.org/10.1109/JIOT.2021.3050802

Mansouri, A., & Wang, X. (2021). A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. *Information Sciences*, *563*, 91–110. https://doi.org/10.1016/j.ins.2021.02.022

Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of Internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*(2), 1515–1555. https://doi.org/10.1007/s11276-020-02535-5

Neelakandan, S., Rene Beulah, J., Prathiba, L., Murthy, G. L. N., Fantin Irudaya Raj, E., & Arulkumar, N. (2022). Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. *International Journal of Modeling, Simulation, and Scientific Computing*, *13*(4). https://doi.org/10.1142/S1793962322410069

Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). The blockchain-based security mechanism for the medical data at fog computing architecture of the Internet of things.

Electronics (Switzerland), *10*(17). https://doi.org/10.3390/electronics10172110

Ranjith Kumar, M. V., & Bhalaji, N. (2021). Blockchain-Based Chameleon Hashing Technique for Privacy Preservation in E-Governance System. *Wireless Personal Communications*, *117*(2), 987–1006. https://doi.org/10.1007/s11277-020-07907-w

Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2021). A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, *8*(7), 5914–5925. https://doi.org/10.1109/JIOT.2020.3032997

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. In *Healthcare (Switzerland)* (Vol. 8, Issue 2). https://doi.org/10.3390/healthcare8020133

Singh, A. K. (2021). Data Hiding: Current Trends, Innovation, and Potential Challenges. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *16*(3s). https://doi.org/10.1145/3382772

Suaib Akhter, A. F. M., Ahmed, M., Shahen Shah, A. F. M., Anwar, A., Kayes, A. S. M., & Zengin, A. (2021). A blockchain-based authentication protocol for cooperative vehicular ad hoc networks. *Sensors (Switzerland)*, *21*(4), 1–21. https://doi.org/10.3390/s21041273

Suhail, S., Hussain, R., Khan, A., & Hong, C. S. (2021). On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions. *IEEE Internet of Things Journal*, *8*(1), 1–17. https://doi.org/10.1109/JIOT.2020.3013019

Thirumalai, C., Mohan, S., & Srivastava, G. (2020). An efficient public key secure scheme for cloud and IoT security. *Computer Communications*, *150*, 634–643. https://doi.org/10.1016/j.comcom.2019.12.015

Wang, W., Huang, H., Zhang, L., & Su, C. (2021). Secure and efficient mutual authentication protocol for smart grid under the blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 2681–2693. https://doi.org/10.1007/s12083-020-01020-2

Ye, G., Jiao, K., Wu, H., Pan, C., & Huang, X. (2020). An Asymmetric Image Encryption Algorithm Based on a Fractional-Order Chaotic System and the RSA Public-Key Cryptosystem. *International Journal of Bifurcation and Chaos*, *30*(15). https://doi.org/10.1142/S0218127420502338

Yu, H., Chen, B., Xu, D., Yang, X., & Sun, C. (2020). Modeling of Rice Supply Chain Traceability Information Protection Based on Block Chain. *Nongye Jixie Xuebao/Transactions of the Chinese Society for Agricultural Machinery*, *51*(8), 328–335. https://doi.org/10.6041/j.issn.1000-1298.2020.08.036