Research on Data Protection Scheme for Road Maintenance System Based on Hybrid Encryption

Jiawang Cui[1, a], Junwei Xiao[1, b], Qingfang Wang[1, c]

2995945180@qq.com[a], 1151884096@qq.com[b], 842371649@qq.com[c]

Wuhan Polytechnic University, Hubei, Wuhan, 430048[1]

Abstract: Blockchain technology is now being used in a wide range of industries, the most recent of which being the financial sector. These industries include healthcare, city planning, and supply chain management. This article proposes a security and privacy solution that makes use of blockchain technology in order to reduce the likelihood that private data may be used in an unauthorized manner. The proposed design for the road maintenance system encrypts sensitive information using AES symmetric encryption and RSA digital signatures, and then utilizes blockchain technology to make the whole process more reliable and secure. When people share information with one another, the aim of this piece is to allay the concerns of data collectors and consumers with respect to the danger of data manipulation. In order for the adversary to see the data in its original form, they will need to decipher the ciphertext. The RSA method is effective in scenarios such as these, as well as for sending keys across insecure networks.

Key words： Block chain technology, security, privacy, data sharing, and encryption

1 Introduction

The technology known as blockchain is still in its infancy but has made significant strides in recent years. The data that is stored in the block is described as being "unfalsified," having "full trail," being "traceable," being "open and transparent," having "collective endorsement," and so on; in essence, it is a shared database. There are three subcategories of blockchains: public blockchains, private blockchains, and alliance blockchains. These subcategories are distinguished from one another by the service groups they support and the authentication procedures they implement. Not only was the public chain the very first blockchain ever developed, but it is also the one that has garnered the most attention and been adopted by the most people. Everyone in the world is able to see and make use of the transactions that have been recorded on the public blockchain since its users come from all over the world. Private blockchains, on the other hand, only make use of the blockchain ledger technology and are restricted to a certain number of users. Moreover, all of the nodes that make up a private blockchain are owned by the same organization. The execution speed of a private blockchain is substantially closer to that of a traditional database than it is in a public blockchain due to the fact that there are fewer nodes in a private blockchain. Because of the high level of trust that exists between them, not all of the nodes are required to reach consensus in order to validate a transaction. Alliance chains are a special sort of private blockchain that allow only authorized nodes to join the network and only let participating nodes to read and change information in line with their own permission settings. This prevents unauthorized users from

EMIS 2023, February 24-26, Chengdu, People's Republic of China

DOI 10.4108/eai.24-2-2023.2330677

tampering with the data. It is assumed that the nodes are connected to one another by means of a robust network connection. The Alliance chain is still a private chain, despite the fact that it has some of the qualities of a completely decentralized system. Since it does not need as much confidence in its nodes as private blockchain does, alliance chain offers a greater degree of flexibility.

The traditional method of human inspection, which is laborious, time-consuming, and prone to mistake, is being phased out in favor of cutting-edge information technology in the intelligent inspection of road issues. Traditional centralized databases are having a hard time keeping up with the ever-changing requirements of society (Saxena R, 2021); this is largely attributable to the difficulties that come along with sharing data and preventing the inadvertent disclosure of sensitive information. Traditional databases are also finding it difficult to adapt to new technologies. Because of the way the intelligent system is now set up, the problems that have been identified inside it are not amenable to being fixed via the traditional approach of sharing information. It is essential to use a variety of encryption methods to encrypt the data that is stored inside private information systems and their respective databases. After conducting an in-depth study of privacy data protection issues related to areas such as financial transaction processing, the Internet of Things (IoT), intelligent systems, and the sharing of personal information, Ji (Ji, Haoyu,2019) provided a summary of blockchain-based privacy protection technologies. The fact that the ledger is distributed and cannot be altered provides an additional layer of security for the data. The authors of this research (McGhin, T, 2019) suggest a patient-centered healthcare information platform that is both private and secure by making use of blockchain technology. It is essential to one's anonymity that sensitive data be encrypted in order to prevent unauthorized access. Arora et al. conducted research to see how successful various security strategies are when used to cloud networks (Priyanka Arora, 2012). This study will investigate the potential benefits of utilizing cloud resources to implement popular encryption algorithms (such as the symmetric encryption algorithm AES, the asymmetric encryption algorithm RSA, and the hashing algorithm MD5) that are used to protect sensitive information. These algorithms include AES, which is used to encrypt data using symmetric keys, and RSA, which is used to encrypt data using public keys. When Seth et al. (Shashi Mehrotra Seth, 2011) compared the three algorithms RSA, DES, and AES, they took into consideration several parameters like as computation time, memory utilization, and output byte. The results of the tests indicate that the DES and AES algorithms are the ones that use the least amount of memory and encrypt data in the shortest period of time, respectively. As compared to other methods, the RSA one encrypting a message takes the most time, uses the most memory, and generates the least amount of data possible.

2 Proposed model

In-field inspections and automated device monitoring both generate data, which is then either automatically or manually entered into a database management system. For the highest level of protection, the information collected by the different sensors is processed and saved in a manner that utilizes mixed encryption. RSA and AES are compared here with regard to the key length used in hybrid encryption, key management, encryption speed, and decryption time. It proposes a new form of encryption algorithm that incorporates the most beneficial aspects of the two that are now in use. Continue reading to find out how the sensitive data gathered by

employees on roads is encrypted. The AES method is employed in symmetric encryption even though it has a poor reputation for the level of key security it provides. This is because the same key is used for both the encryption and decryption procedures in symmetric encryption. It is for this reason that an asymmetric kind of encryption based on the RSA algorithm is used. The RSA method is used to encrypt the key once again after it has first been encrypted using the AES method. Asymmetric encryption employs a combination of cryptographic procedures, known as encryption and decryption, that each make use of their own unique key in order to guarantee the confidentiality of data transmissions. When it comes to the process of encrypting data, the AES technique is superior in terms of speed, whilst the RSA algorithm is superior in terms of both security and the management of keys. The obtained raw data is encrypted in a manner that makes optimal use of both of the aforementioned methods.

2.1 AES

The Rijndael encryption algorithm is a common name for the symmetric key encryption technique that was accepted by the National Institute of Standards and Technology (NIST) in 2001 (Kumar T M,2022). This method is part of the Advanced Encryption Standard (AES). The AES method performs the conversion from plaintext to ciphertext by first splitting the input into 128-bit data blocks using a fixed-length key that is either 128, 192, or 256 bits in length. This is done by a series of permutations and transformations. Encryption and decryption are the two phases that make up the AES algorithm. Encryption is the first step. After determining the length of the key that is required for encryption, the key is then lengthened in order to provide a set of symmetrical keys that may be put to use in the process. At the first step of the process, the plaintext and the key are XORed together. The output is what is utilized as input for the subsequent round. With each transformation and permutation that takes place throughout the procedure, a new round key is used for the XOR operation. It is possible to obtain plaintext by applying the same key to the encryption process in the opposite sequence, starting with the key for the last round of encryption and working your way back to the key for the first round.

2.2 RSA

RSA is a factorization-based asymmetric encryption technique. It is based on the idea of public and private keys, with the former used to encrypt data and the latter to decode it (Anand Dohare,2020). With the recipient's public key, the sender of an RSA encrypted message may encrypt their plaintext, and the recipient can use their own private key to decode the message. Thus, the plaintext can only be read by the intended recipient. This prevents the private key from being deduced by an attacker who only has access to the public key. The RSA algorithm encrypts plaintext using the product of two big prime integers, p and q, as the public key, then decrypts the ciphertext using the private key.

2.3 Hybrid encryption

The data is encrypted using a mix of the RSA and AES algorithms in this implementation. The AES method is chosen because of the great encryption efficiency it offers in addition to the rapid encryption speed it has. The RSA algorithm is well-known for its excellent security, but it is a time-consuming method that is used to encrypt large amounts of data. Encryption of the AES key is done using the RSA method in order to go around this limitation (Himani

Agrawal,2020). The encryption method is made both quicker and more secure when RSA and AES are used together as a consequence of their combination.

Figure 1 is a flowchart that illustrates the encryption process that was implemented into this design.

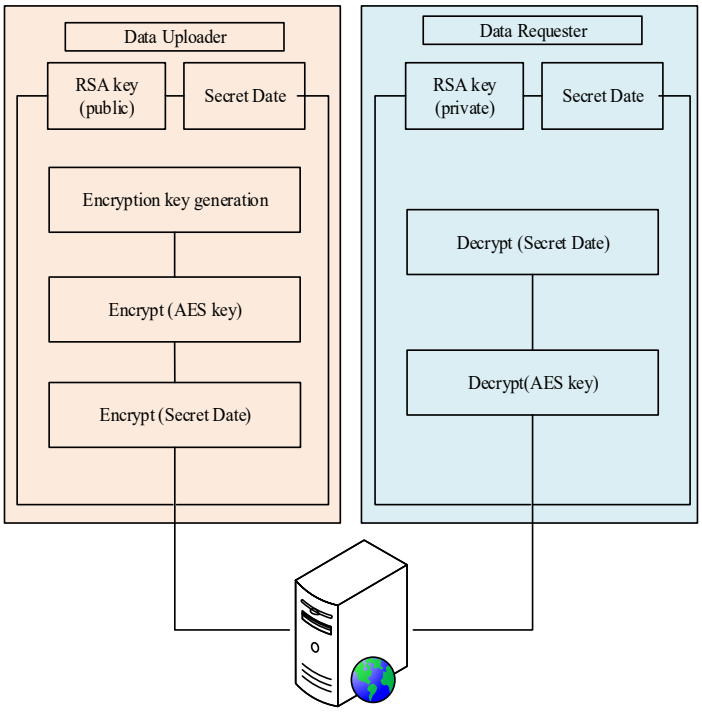

Figure 1. Hybrid Encryption Process

3 An Encryption Model with Three Parts

To protect the privacy of data while it is being kept, this encryption method calls for the involvement of not one, not two, but all three persons involved: the person uploading the data, the person requesting the data, and the server.

3.1 Data Uploader

Before being transferred to the road maintenance business system, the data from the road condition monitoring system is encrypted using a hybrid technique. This is done regardless of whether the data was determined manually by field staff or identified automatically by equipment. The fact that the original data is transported via an unprotected network, where it is at risk of being lost or altered, is the root cause of the mistrust that surrounds the data. The Advanced Encryption Standard (AES) with a 256-bit key is the principal method of encryption that is implemented. The act of encrypting data is accomplished by a multi-stage procedure, which includes the following steps:

1)A data administrator is required to generate a 256-bit AES key while also ensuring that the operation is both secure and random. They are also required to generate an RSA key pair, which consists of a public key that may be shared with the general public and a private key that must be kept a secret at all times. It is necessary to have a key length of 4096 bits in order to generate an RSA key pair.

2) Encrypt the data using an arbitrary AES key that you have produced using the AES algorithm. The technique known as the advanced encryption standard (AES) is used to independently encrypt each block of data that is sent. The message is encrypted using a succession of random round keys when you use the AES technique. The generation of round keys is necessary since all future round keys are derived from the initial key. The data is protected adequately to be sent over a public network.

3) Encrypt the AES key. Due to the fact that AES employs a symmetric key, it is absolutely necessary for the key to be encrypted before it is sent. Encryption may be accomplished by using the RSA public key in conjunction with the AES key. Provide the data that has been encrypted as well as the AES key to the server at the same time.

When sensitive information is encrypted using a hybrid approach, it is shielded throughout the process of file transmission to the server from both indirect and direct attacks, such as eavesdropping. If the RSA method is used to encrypt file data directly in this scheme, the unpredictability of the encryption and decryption durations is caused by the fact that the length of the data varies. The usage of the block cipher technique AES with a predetermined block length is preferred when compared to simply encrypting data using RSA. This is because AES uses a defined block length. The AES algorithm generates ciphertext of a fixed length, which is then passed on to the RSA technique for encryption. This is done with the intention of improving the algorithm's overall efficiency.

Meanwhile, active speech features include speech recognition, automatic speech synthesis and voice conversation services.

1. Speech recognition is a technology that converts a person's speech signals into text messages comprehensible to a computer to help machines better understand and direct human speech input. The technology can be used to implement a range of applications, such as voice command, voice interaction, online speech translation and so on.

Speech recognition technology is based on speech signal processing, machine learning and language modeling. It can identify useful information from speech, including the sentences, words, phrases and so on. It allows computers to interpret the sounds humans make in order to respond. More recently, speech recognition technology has enabled accurate speech-to-text functionality, which can be realized using any device that supports rich speech recognition capabilities.

The essence of speech recognition technology is to identify features from many large volumes of voice data and create an accurate model, or machine learning algorithm, to process future input voice changes. It also requires powerful computing power to process large amounts of data in order to be able to recognize speech more accurately. In the future, speech recognition technology including words, regular expressions and sentiment analysis will overlap to improve the performance of speech processing machines and bring more convenience to people.

2. Automatic speech synthesis function is a kind of technology that simulates human speech by using computer science technology and produces sound by synthesizing or playing the recording. It uses professional software to record and convert words into correct phonemes that can be used to display information, and uses specific algorithms to process morphemes, so that under certain conditions it can realize the conversion of digital sound and language similar to the form of natural language. It can grab text from the network, sometimes requires some special processing to grab text simple application, and for speech synthesis pronunciation. After the function of automatic speech synthesis can convert text into numbers that can be recognized by the machine, there is a certain process of network distribution to form hardware devices that meet the requirements of human speech, and then it is input to the microprocessor through technical algorithms to form speech data, and then output as sound signals, and mapped to the actual sound system.

3. As for voice conversation services.

First of all, the voice dialogue service should use intelligent voice recognition technology to provide accurate and high-quality voice recognition service to ensure the accuracy and reliability of the service.

Secondly, it is necessary to cultivate professional customer service, adopt systematic and systematic customer service standards, improve customer service ability, strengthen customer service knowledge and skills reserve, and improve customer service quality.

In addition, voice recognition service software that is easier to use and more powerful can be developed to improve the speed and quality of service.

3.2 Data Requester

The second step of this encryption procedure involves moving the file from its storage location to the location from where it is being requested. It is the responsibility of the data requester to evaluate the operational condition of the city's roads, which may involve manual evaluation, automatic (semi-automatic) identification by a platform, and subsequent manual or automatic (semi-automatic) reconfirmation based on predictions made by automatic monitoring devices. This assessment may also involve semi-automatic identification by a platform.

3.3 Server

In order to do this, the person requesting the data must first send an access request to the server before the storage system may supply the information that was requested. The data requester now has both the data as well as the AES key that has been encrypted, and both of these items need to be decrypted. Instructions for decryption, which is the exact opposite of encryption and can be seen laid out in a step-by-step format in Figure 2, which may be found here.

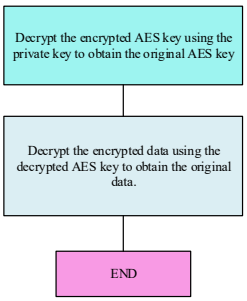

Figure 2. Specific steps in encryption process

Users have the ability to transmit information to the recipients it is meant for by following the protocol outlined above, with the guarantee that the information will not be intercepted or changed while it is in route. When the AES algorithm is employed for data encryption, efficient data transmission can be assured, and secure key exchange can be achieved when the RSA technique is utilized to encrypt the AES key. Both of these benefits may be reached simultaneously. Because of this, the combination of the AES and RSA algorithms offers a strong method to encryption that can ensure the integrity of the data being sent.

4 Results

When utilizing RSA encryption, it is obvious that the length of the ciphertext will remain the same even if there is a large difference between the lengths of the pieces of data that need to be encrypted. In addition, the length of the ciphertext determines the level of security provided by an RSA encryption. It is clear from looking at Figures 3 and 4 that when encryption is used for longer periods of time, it becomes more challenging to decipher the data.

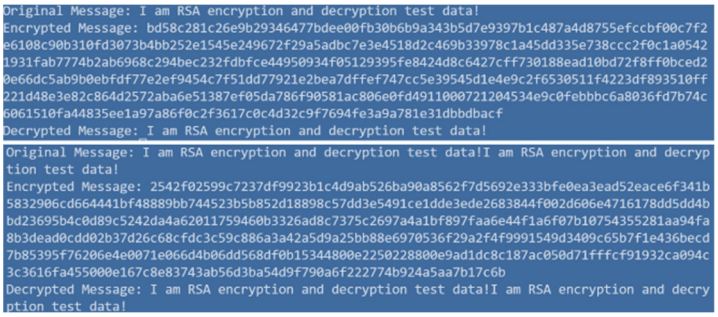

Figure 3. RSA Encryption Ciphertext comparison

The Advanced Encryption Standard (AES) algorithm is an excellent choice for quickly encrypting large amounts of data because of its ease of use and the fact that it is a symmetric encryption technique (which means that it makes use of the same key for both encryption and decryption). Despite this, it is obvious that the length of the ciphertext will grow

proportionately with the size of the data that has to be encrypted using the AES technique. It is likely that the pace at which data is encrypted will slow down as a result of the increased amount of calculations that must be performed.

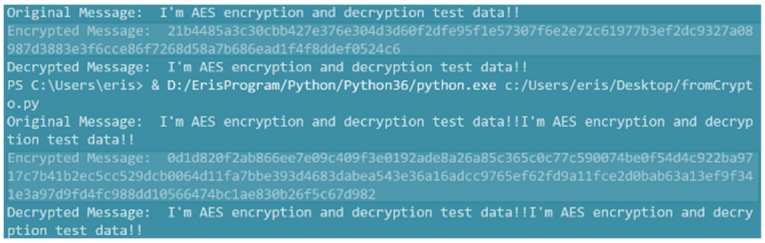

Figure 4. Hybrid Encryption Ciphertext comparison

As the information is being sent to the database, it is protected by not one but two levels of protection. A larger amount of data may be encrypted using the AES method, whereas the RSA encryption standard ensures the security of symmetric encryption. Before developing a hybrid encryption technique, it is necessary to first separately implement the AES symmetric encryption algorithm and the RSA asymmetric encryption algorithm. This is required in order to establish a hybrid encryption method.

Throughout this experiment, the same set of data was encrypted and decoded using three distinct approaches each time. The results were strengthened by taking the average of multiple iterations and excluding the outliers from the analysis. The data made it possible to investigate how RSA, AES, and hybrid algorithms differed in the amount of time required for encryption and decryption. The amount of time needed by each method to encrypt a file of varied sizes is outlined in Table 1, which may be found here.

Table 1. RSA, AES, and hybrid algorithm encryption

Serial number	File size/MB	AES encryption/s	RSA encryption/s	Hybrid algorithm encryption/s
1	1.12	0.005	4.468	0.005
2	6.76	0.029	26.503	0.033
3	13.5	0.052	72.426	0.068
4	19.1	0.071	82.067	0.085
5	26.1	0.109	111.868	0.137
6	28.1	0.117	147.825	0.145
7	31.5	0.119	167.653	0.148

An examination of the aforementioned table results in the production of the plots of encryption times shown in Figure 5 for the three different encryption strategies. The results of the tests show that the amount of time needed to encrypt data using the RSA algorithm increases at a rate that is proportional to the size of the data being encrypted, whereas the amount of time needed to encrypt data using the AES algorithm grows only slightly, and the amount of time needed to encrypt data using the hybrid encryption algorithm grows at a rate that is comparable to that of the AES algorithm. The amount of time necessary to encrypt a file

using the RSA technique is hundreds of times longer than the time needed by the AES and hybrid algorithms. While this difference is minimal when dealing with smaller files, it becomes obvious when the file size is more than 5 megabytes.

As can be seen from the comparison of encryption timings presented above, using the hybrid algorithm that encrypts and decrypts using more secure encryption techniques results in a significant increase in the amount of data that can be encrypted and decrypted with the same amount of time spent encrypting the data. At the same time, the security provided by the hybrid algorithm is enhanced in comparison to that provided by the AES algorithm.

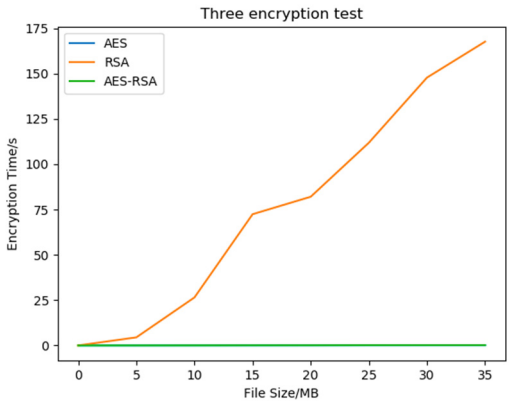

Figure 5. Encryption Process

5 Conclusion

This article proposes the use of a hybrid encryption method that is based on Advanced Encryption Standard (AES) keys and Rivest-Altman (RSA) keys for use in the road maintenance system. It does so by providing an overview of the fundamentals of both algorithms and conducting an analysis of the benefits and drawbacks of both. In addition, the advantages of using this hybrid encryption algorithm, as well as the necessity and safety of implementing it in the road maintenance system, were demonstrated by carrying out an in-depth study of the amount of time required to encrypt data using each of the three different encryption strategies.

The hybrid encryption approach described in the study has not yet had its full functionality included into the road maintenance system. The processing of encrypting and decrypting data has, up to this point, solely been the subject of academic research and practical application. In order to develop a standalone program that is capable of performing all of its functions, the integration and deployment of the application must be improved. Nonetheless, there are holes in this study that need to be addressed in the future. As an example, if the data source that is going to be encrypted is exceedingly large, it is possible that the efficiency of the encryption process may suffer if the data is first cut up into numerous smaller parts. Improving file encryption in the face of threats such as man-in-the-middle attacks, replay assaults, and analysis assaults will be the primary focus of research to be conducted in the future.

Reference

[1] Anand Dohare，et al.A Data Prediction in Wireless Sensor Networks using Deep Learning-based RSA Algorithm[J].International Journal of Innovative Technology and Exploring Engineering，2020, 9(9): 398-404.

[2] Himani Agrawal, “Matlab Implementation, Analysis & Comparison of Some RSA Family Cryptosystems”, 2010 IEEE International Conference on Computational Intelligence and Computing Research.

[3] Ji, Haoyu, and He Xu. "A Review of Applying Blockchain Technology for Privacy Protection." In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 664-674. Springer, Cham, 2019.

[4] Kumar T M，Karthigaikumar P.Implementation of a High-Speed and High-Throughput Advanced Encryption Standard[J]. Intelligent Automation and Soft Computing, 2022, 31(2): 1025-1036.

[5] McGhin T., Choo, K. K. R., Liu, C. Z., & He, D, "Blockchain in healthcare applications: Research challenges and opportunities", Journal of Network and Computer Applications, vol.135, pp.62-75, 2019.

[6] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012.

[7] Saxena R，Gayathri E.A study on vulnerable risks in security of cloud computing and proposal of its remedies[J]. Journal of Physics: Conference Series, 2021, 2040(1)8-15.

[8] Shashi Mehrotra Seth, Rajan ishra, “Comparative Analysis of Encryption Algorithms for Data Communication”, International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.