Hindawi
Security and Communication Networks
Volume 2023, Article ID 9846460, 1 page
https://doi.org/10.1155/2023/9846460

Retraction

Retracted: Encryption Technology for Computer Network Data Security Protection

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Yu, "Encryption Technology for Computer Network Data Security Protection," *Security and Communication Networks*, vol. 2022, Article ID 1789222, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 1789222, 9 pages
https://doi.org/10.1155/2022/1789222

Research Article

Encryption Technology for Computer Network Data Security Protection

Yang Yu

Yantai Vocational College, Yantai, Shandong 264670, China

Correspondence should be addressed to Yang Yu; 11231431@stu.wxic.edu.cn

Received 1 July 2022; Revised 24 July 2022; Accepted 1 August 2022; Published 22 August 2022

Academic Editor: C. Venkatesan

In order to solve the network security problem of data encryption technology, this paper proposes a research method of computer network information security maintenance based on data encryption technology. Taking the network reporting system of a mining enterprise as the research object, this paper comprehensively expounds on the design of network reporting system and data encryption in network communication from the aspects of demand investigation, demand analysis, system design, software system development, and so on and implements the development by using BS architecture + independent client. The experimental results show that the AES algorithm can be independently designated as 128 bits, 192 bits, and 256 bits. *Conclusion*. This scheme can realize the rapid and safe transmission of data information and provide an effective means for the transmission of confidential documents on the network, so it has a good application prospect.

1. Introduction

With the rapid development of computer technology, the development of today's society has been inseparable from the information network. Because the information transmitted by computer networks involves finance, science education, military, and other fields, including huge economic or national interests, it is necessary to carry out network attacks from all sides. The manifestations of network attacks are also diverse, such as virus infection, data theft, information tampering, deletion, and so on. The frequent occurrence of computer crime is also greatly related to the convenience of crime, the fact that it is not necessary for the perpetrator to visit the scene in person, and the difficulty in leaving criminal evidence. Nowadays, the protection of computer network security in various countries has become a serious social problem to curb computer crime. Network information security is related to national security and national development. With the increasing global informatization, it plays a more and more important role. We advocate the construction of network security, and vigorously guarantee the network information security is to protect the hardware and software of the network system, mainly to protect the data in the system from damage, change and leakage, and finally make the whole network system run normally and provide services.

2. Literature Review

Yu and others said that the data operation, generally speaking, includes three aspects: first, processing, second, transmission, and storage [1]. Weathersby and others said that the link of network transmission is the most prone to problems in these three aspects, so the security of data in network communication becomes particularly important [2]. Wu and others said that common means of data theft and attack include: illegally stealing data information through system vulnerabilities; malicious tampering with data distorting the data during transmission, and the data receiver cannot recognize the data information [3]. An unauthorized user logs in as an authorized user to access the system. Li and others said that the problem of safe data transmission in the network usually includes the following aspects: first, to ensure that the user is safe, that is, to verify that the user is legitimate [4]. Chen and others said that the second is to ensure that the data has not been damaged or

stolen, that is, the application of encryption technology, digital signature, and other technologies, as well as the management and traceability of access and operation logs [5]. Zhao and others said that at present, the most effective response to the problem of how to ensure communication security on the Internet is to encrypt the data [6]. Krishnakumar and others said that according to the statistical data, the biggest culprit causing data security in the process of data transmission in the network is illegal theft or destruction [7]. Therefore, in practical applications, we usually adopt the following means: Negi and others say that data, plaintext, should be encrypted into ciphertext that can only be identified by decryption before transmission on the network. This can avoid the eavesdropping of plaintext in transmission and play a very effective role in protecting data security [8]. Ncubukezi and others said that there are many technical methods of data encryption. After consulting a large number of documents and books, and referring to the technologies adopted by many Internet enterprises today, they analyzed several commonly used typical encryption technologies and algorithms and briefly introduced their various characteristics. Accurately put forward the points that are not suitable for the work of this paper, and negated them. Finally, it decided to choose the RSA algorithm as the encryption algorithm for reporting information in the network reporting system [9]. RSA was proposed in the late 1870s. Its founders were Ron Rivest, Adi Shamir, and Leonard Adleman. RSA's name is made up of the initials of three inventors. Yu and others said that RSA algorithm is an asymmetric algorithm. Generally speaking, there are two keys, that is, two completely different keys are used in the encryption process and the decryption process, and the other cannot be obtained through one. This is almost impossible to calculate now [10]. RSA algorithm is based on the century-old mathematical problem that the factor of large numbers is difficult to decompose. Here, large numbers are large integers. This mathematical problem is recognized as almost unsolvable because up to now, it is still unsolved. So, at present, the fact that the RSA algorithm has existed for many years is enough to ensure that the RSA algorithm is reliable. Therefore, RSA algorithm has been widely used since it was proposed and has been continuously optimized and developed. RSA algorithm seems simple, but it is difficult to be broken, which has become the basis for its development. Network information security is shown in Figure 1.

3. Method

AES algorithm is a symmetric key iterative block cipher algorithm. Its packet length and key length are variable. They can be independently designated as 128 bits, 192 bits, and 256 bits. It regards the plaintext data packet as a two-dimensional array of bytes (called the state array). The array has 4 rows and Nb columns (NB is equal to the packet length divided by 32). All transformations of AES algorithm will be carried out on this state matrix. Take AES-128 (key length is 128 bits) as an example, it will input plaintext packets a_0, a_1, a_2,. . .,a_{15} is mapped to a 4-row and 4-column state matrix, and several iterations are performed on this state matrix to realize the confusion and diffusion of plaintext data and achieve the purpose of data encryption. Each iteration is called one round, and there are $N_r + 1$ rounds [11, 12]. From the abovementioned four transformations, it can be seen that the decryption of AES algorithm process only converts the transformation of each round function into the corresponding inverse transformation, and transforms the state matrix obtained from the ciphertext mapping in the reverse order. The number of global data leaks is shown in Figure 2.

In elliptic curve cryptosystem, we are concerned with elliptic curves over finite fields. Elliptic curve encryption algorithms over finite fields involve mathematical knowledge such as number theory, group theory, finite field theory, and elliptic curves. Fields are abstractions of common number systems (such as rational field Q, real field R, and complex field c) and their basic properties. A field consists of a set F and two operations. These two operations are addition (represented by + and multiplication (represented by U), respectively, and meet the following arithmetic characteristics: the prime field FQ is composed of an integer set {0, 1, 2,. . ., $P - 1$}, and each such integer can be represented by a binary representation with a length of exactly $t = [\log 2q]$ (where $[x]$ represents the smallest integer not less than x), which is composed of the binary representation of an integer and a 0 with an appropriate number added to its left. The elements in F_q have the following arithmetic operations: let F_q^* represent all nonzero elements in F_q, and it can be proved that there is at least one element g in F_q so that F. Any nonzero element in G can be expressed as a power of G, as shown in the following formula:

$$F_q^* = \{g' : 0 \le i \le p - 2\}. \tag{1}$$

The multiplicative inverse of $a = g' \in F'$ is as shown in the following formula:

$$\frac{1}{a} = g^{(-i) \bmod (p-2)}. \tag{2}$$

It can be seen that one inversion operation on F_q requires $p - 1 - i$ domain multiplication. The finite field F_{2m} with the characteristic of 2 is called a binary field, which can be regarded as the m-dimensional space on the field F_{2m} (with two elements 0 and 1). That is, there are m elements a_0, a_1,. . ., $a_{m\text{-}1}$ on F so that each $a \in F_{2m}$ can be uniquely expressed as shown in the following formula:

$$a = a_0 a_0 + a_1 a_1 + \cdots + a_m a_m, a_i \in \{0, 1\}. \tag{3}$$

For a set of $\{a_0, a_1, \ldots, a_{m-1}\}$, it is called the base of F_{2m}. For the base, the domain element a can be expressed as a bit string $\{a_0, a_1, \ldots, a_{m-1}\}$. Generally, two parallel lines will never intersect, but it can be assumed that two parallel lines intersect at an infinite point, so the projective coordinate system can be established on the basis of the original plane coordinate system. For the point coordinates (x, y) on the ordinary plane rectangular coordinate system, make the following transformation: if $x = Y/Z$, $y = Y/Z$, $Z \neq 0$, point a can be expressed as (X, Y, and Z). In this way, the two-dimensional coordinates are changed into three-

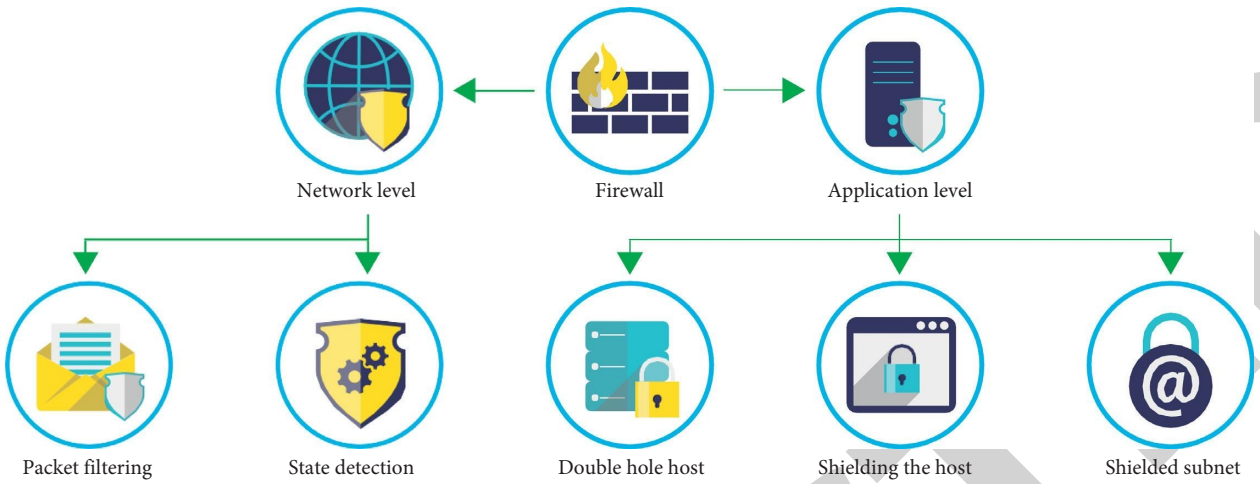

Figure 1: Network information security diagram.

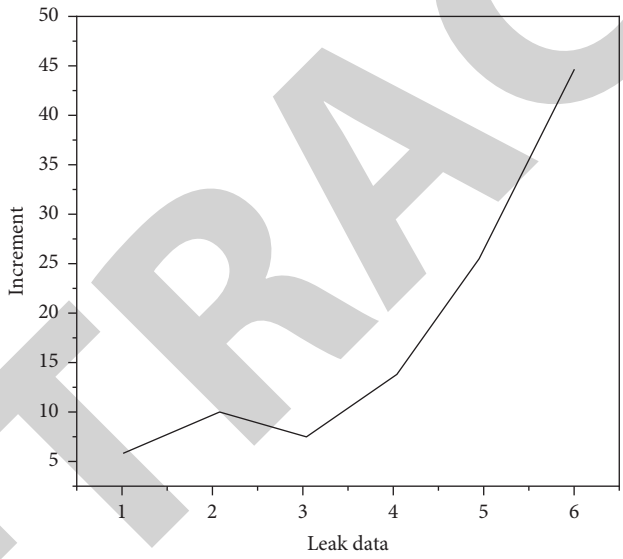

Figure 2: Global data leakage.

dimensional coordinates, and a new coordinate system is established for the points on the plane. At the same time, the equation $aX + bY + cZ = 0$ of the straight line is obtained (the general equation of the straight line in the ordinary plane rectangular coordinate system is $ax + by + c = 0$). The infinity point is the intersection of two parallel lines. The equations corresponding to the two lines are solved simultaneously, as shown in the following formula:

$$\begin{cases} aX + bY + c_1 Z = 0 \\ aX + bY + c_1 Z = 0 \end{cases} (c_1 \neq c_2). \tag{4}$$

The solution is $cZ = c_2 = -(aX + bY)$, $c_1 \neq c_2$, $Z = 0$, $aX + bY = 0$, that is, the infinity point can be represented by (X, Y, and 0). Note that the ordinary point $Z \neq 0$ and the infinite point $Z = 0$, so the corresponding equation of the infinite straight line is $Z = 0$. Several properties of the infinity point are listed below to unify parallelism and intersection: there can only be one infinity point on the straight-line L. A group of parallel lines in a plane has a common infinity. Any two intersecting lines L and $L2$ in the plane have different infinity points. All infinite points on the plane form an infinite straight line [13]. All infinity points and all ordinary points on the plane form a projective plane. Weierstrass equation and elliptic curve are defined in algebraic geometry, and algebraic curve with the specification of 1 is called elliptic curve, but defining elliptic curve in this way will make this paper deviate from the topic to be discussed. According to the Riemann–Roch theorem, any elliptic curve can always be represented by a cubic equation, which is generally called the Weierstrass equation. As shown in the following formula,

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_6, \tag{5}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$, when the characteristic of domain K is not 2, the abovementioned equation can be deformed as shown in the following formula:

$$\left(y + \frac{1}{2}a_1x + \frac{1}{2}a_3\right)^2 = x^3 + \left(\frac{1}{4}a_1^2 + a_2\right)x^2 + \left(\frac{1}{2}a_1a_3 + a_4\right)x + \frac{1}{4}a_3^2 + a_6, \quad (6)$$

or as shown in the following formula:

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \quad (7)$$

where when the characteristic of field k is not 2, 3, the equation can continue to deform as shown in the following formula:

$$(2y + a_1x + a_3)^2 = 4x\left(x + \frac{1}{12}b_2\right)^3 + \left(-\frac{1}{12}b_2^2 + 2b_4\right)\left(x + \frac{1}{12}b_2\right) + \left(\frac{1}{213}b_2^3 - \frac{1}{6}b_2b_4 + b_6\right) \quad (8)$$

$$\begin{cases} X = 36\left(X + \frac{1}{12}b_2\right) \\ Y = 108\,(2y + a_1x + a_3). \end{cases}$$

$Y^2 = X^3 - 27c_4X - 54c_6$ is obtained, and its discriminant is $1728\Delta = c_4^3 - c_6^2$. For any field K, the discriminant of the Weierstrass equation is as shown in the following formula:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27_6^2 + 9b_2b_4b_6), \quad (9)$$

where as shown in the following formula:

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2(i.e.4b_8 = b_2b_6 + b_4^2). \quad (10)$$

When $\Delta \neq 0$, $j = c_4^3/\Delta$ is called j-invariant on elliptic curve e, the full name of $j(E)$. MD5 is message digest algorithm5 (information digest algorithm), which was designed by Professor Rivest of Massachusetts Institute of Technology. This method is improved from MD4. Its function is to allow large capacity information to be "compressed" into a confidential format (that is, to transform a byte string of any length into a large integer of a certain length) before signing a private key with digital signature software. The main idea of Rivest's original design was to consider the system architecture based on 32-bit processors. Therefore, all operations in MD5 are based on 32-bit words. MD5 adds the concept of "safety belts" to MD4. Although MD5 is slightly slower than MD4, it is more secure. This algorithm obviously consists of four steps that are slightly different from MD4 design. In MD5 algorithm, the necessary conditions for the size and filling of information summary are exactly the same as those in MD4.

4. Experiment and Analysis

The actual development of the information system is almost all based on the database management system with the support of the operating system and realized through the application software [14, 15]. The security of the entire application system depends not only on the operating system, DBMS, etc., but also on the security of the most important and weakest application software in the current computer security. Therefore, applying security management and prevention strategies and technologies to the development stages and processes of information management system prosperity can strengthen the ability of the system to resist accidental or intentional bit authorized access, prevent unauthorized modification and dissemination of data, and thus improve the confidentiality, integrity, and effectiveness of enterprise information security. To build a secure computer system, we need to balance a series of requirements. The security principle must try to avoid conflicts between various factors to prevent affecting other characteristics of the system. When the security conflicts with other characteristics such as network transmission rate, the trade-offs should be made according to their importance to the system. Otherwise, it may waste financial resources by establishing a meaningless high-level protection system, or false alarm signals may occur frequently. It interferes with the normal operation of the system but actually lacks the due safety protection capability, or may affect the efficiency, or even refuse service [16]. Take security as a requirement and consider it at the beginning of system development, so that security requirements can be a part of system objectives from the beginning and play a leading role in the process of system development [17, 18]. At different levels of the system, different safety control mechanisms are used to implement different precision safety control. At the same time, the safety correlation among all levels shall be reduced as much as possible to facilitate the determination of the reliability and feasibility of safety control. In particular, the security design of application software has its particularity. In addition to the confidentiality, integrity, and availability included in the general security, special attention should be paid to the access control of users at different levels. Systematically and reasonably use the security technology and control the security granularity to balance the security and other characteristics of the system. These features include capability, efficiency, flexibility, friendly user interface, and cost [19]. When safety and other characteristics cannot be consistent, or when some safety protection cannot or is difficult to be achieved by technical means, technical deficiencies can be made up by formulating safety operation procedures for personnel at all levels, clarifying safety responsibilities, and implementing them by administrative means. Considering the operating efficiency of the system, especially the high requirements of the b/s structure for network speed performance, in the application layer, except for the user password and key data, no encryption method can be used to encrypt the data. B/s mode solves many problems under the traditional c/s mode. It has many

advantages, such as easy to realize wide area distributed management, convenient operation, stable performance, safe and reliable remote data transmission, low cost and easy maintenance, and the client software is platform independent. At present, this mode has become the mainstream system of network application systems. The development environment of the system is mostly distributed system network environment. The network protocol is based on considering the operating efficiency of the system, especially the high requirements of the b/s structure for network speed performance, in the application layer, except for the user password and key data, no encryption method can be used to encrypt the data. B/s mode solves many problems under the traditional c/s mode is adopted to realize the functions of distributed processing, resource sharing, data sharing, and supporting multi-user and multi-process concurrent operation and access. The safety level of the whole system is shown in Table 1.

Table 1: Safety level of the system.

Outside the system
User
Application program
Database management system
Operating system OS
Hardware (machine, network, and other equipment)

On the one hand, the super user of the operating system has the supreme authority, so any user and his files can control users and protect files by changing user passwords and file attributes through the superuser. On the other hand, ordinary users can change their passwords and the security attributes of all files they own. The third layer is the database management system layer. The database system itself has an administrator (DBA). DBAs are responsible for creating and maintaining all tables and views that make up the application database. DBA creates users and passwords according to the access list of user rights and grants them access rights to tables or fields (query, add, delete, change, etc.). In this way, users not created by the application database, DBA do not have access to the application database, and the access rights of users created by the DBA are also restricted. In addition, other security technologies can be used to strengthen the security protection of data. Data distribution, user distribution, and processing distribution: using the characteristics of distributed database supporting data distribution, data and users can be distributed between servers according to the functions of application software, the degree of data coupling, the frequency of users accessing data, and the autonomy of the server [20]. In fact, the distribution of users also leads to the distribution of server services (processing) to customers. Set trigger: change the complex data validity and validity verification in the application to the database trigger. Using stored procedures: in stored procedures, users and data are separated. That is, the table is not allowed to be fully accessed and updated. The user provides parameters to the stored procedure, provides retrieval conditions, and retrieves the data rows returned by the stored procedure. The advantage of this method is that it completely controls the storage and retrieval of information. Any column that does not want users to access can do so. This is a more object-oriented method for data storage and retrieval, which helps to ensure the correctness and security of data. Backup and fault recovery: an important guarantee to ensure that the information system can be put into reuse as soon as possible when it is damaged due to various unexpected events [21, 22]. The fourth layer is the application layer. The security granularity of data protection is controlled at the record level or field level, but there are at least two points worth considering: too fine control granularity will bring loss of efficiency and program flexibility to the application system. For larger application systems, the work of DBA in charge of application database will become quite complex. Therefore, in combination with the characteristics of information management, except for some important data, the security granularity is generally not controlled too fine, so as to obtain the data security control of the application in a more macro aspect. The model of access supervisor is adopted to control the access of users to the program and realize the protection at the information level. The model of access supervisor is shown in Figure 3.

Such an access supervisor model can be embedded into the application software to achieve the purpose of information security protection. The program structure of the embedded access supervisor is shown in Figure 4.

The fifth layer is the external layer of the system. Safety is ensured by safety education, management, and other measures. It includes all activities that cannot be solved by the application system itself or are difficult to be solved to protect the system's security. For example, security management of client PC workstation. Data audit system: The purpose of data audit is to find and remedy the data in time when it is stolen or damaged, that is, to find the cause of the problem in time, so as to provide a guarantee for maintaining the integrity of the data. Data audit can be implemented in operating system layer, database layer, and application system layer, respectively. Among them, the implementation of the operating system and database system is more expensive, and it is better to take appropriate audit measures on the application system layer. Some operating systems can provide log functions to record the startup time, resources, and even various operations of each system user; the security audit function of database can provide a way to monitor data access. However, the startup of the audit function will affect the efficiency of the system. Common audit measures for application systems are dual track operation method: this method requires that the operation of some data must be completed by two users on different workstations. Operations of one user must be approved by another user before they can take effect [23]. Trajectory method: this method automatically records all important operations in the application system, that is, leaving a trajectory, to monitor the operation of the system. In the trajectory method, the transfer of audit data must be

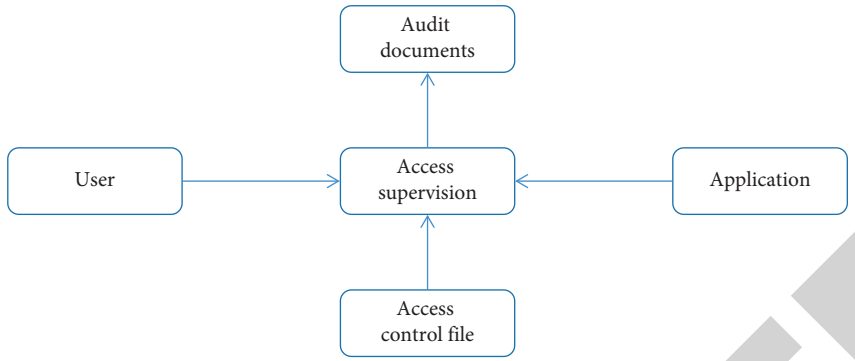

Figure 3: Access supervisor model.

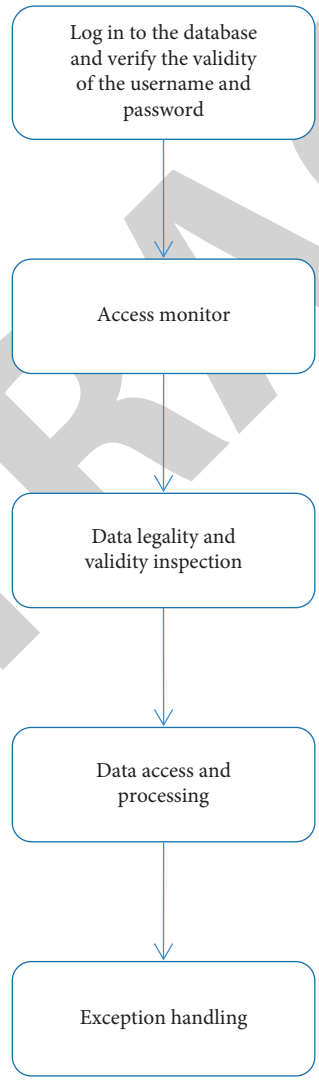

Figure 4: Application framework with embedded access supervisor.

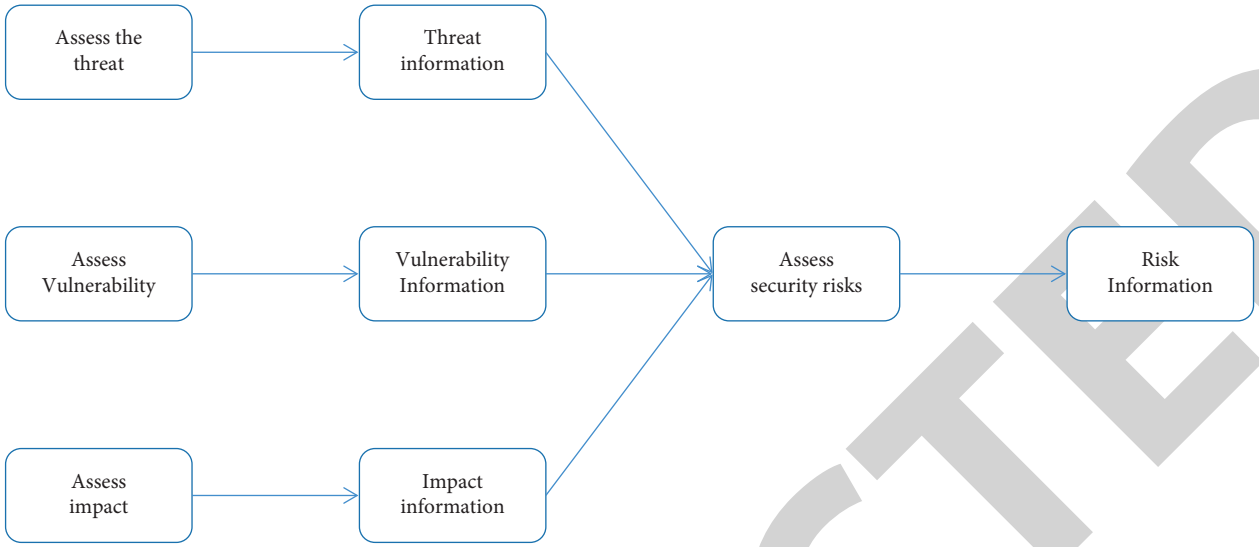

Figure 5: Assessment safety analysis.

supported by the front and background programs. The front desk transfers the data to the file server and the data exchange area, and the background transfers the data in the exchange area to the audit directory. Data backup system. The backup of information system includes four levels: hardware backup. It is to prepare redundant hardware equipment during system design and configuration, and quickly switch to backup equipment when the running equipment fails. The characteristic of this method is that the reliability of the system is high, but the system investment is large. Common backup methods are dual computer fault tolerance: that is, the system is configured with two identical servers, one as the primary server and the other as the backup server. Install a high-speed image card on two servers, which are connected through a high-speed link. When the system is running, the data is stored in both the primary server and the backup server [24, 25]. Disk array technology: multiple hot-swappable SCSR hard disks are used in the server, and RAID5 technology is used to realize real-time hot backup of the system. System backup: It refers to the backup of storage system resources on the same type of equipment. When the system fails, it can be quickly restored. Common methods include backup based on server backup volume and backup based on storage media (such as disk, tape, and optical disc). Application system backup: It is used to restore the application system when the information system is damaged. It can be done in the same way as the system backup. Data backup: Data backup can be done in the same way as system backup and application system backup. The purpose of information system risk analysis is to provide system-related personnel with an analysis method and technical details based on the protected information, computer network, and system operation mode. The object of risk analysis is a series of links from each component of the system to their functions and management. The way of risk analysis is to analyze the technical forms that threaten the security of the system and the forms of vulnerability that can be developed and utilized within the system. Potential threats to information security are widespread. Once a catastrophic event occurs, such as hacker attacks, it is easy to cause huge losses. How to effectively prevent the occurrence of catastrophic events, enhance system security, and make rational use of resources to obtain the maximum social and economic benefits is a major issue. Risk management is to seek the goal of minimizing risk and maximizing benefit in the space of economic and social benefits, risks, and costs [26]. Objectivity and uncertainty: information system risk exists objectively. In the whole information system life cycle, the risk exists all the time, but it is uncertain. Multi-level and diversity: information system risks include physical security, logical security, security management, and other multi-level risks. Physical security includes three elements: perimeter control, area access control, and facility security in the area. Logical security includes confidentiality, integrity, and availability of information. Safety management includes personnel role management, system management, emergency management, etc., so it faces various risks. Variability and dynamic: information system risk is dynamic and variable with the development of information technology. Some risks are eliminated due to the adoption of timely and effective measures; some risks actually occur and are handled; some risks have increased from minor risks to major risks; some risks decrease or even disappear. New risks may arise at each new stage. Measurability: uncertainty is the essence of risk, but this uncertainty is not total ignorance of risk. Any specific risk is the result of many risk factors and other factors. Through the observation and statistical analysis of a large number of risk event data, we can find the obvious movement law. In information security risk control, risk management is the main and prevention technology is the subsidiary. The process-based information security model comes from the capability maturity framework SSE-CMM (system security engineering capability maturity) model. SSE-CMM model divides information system security engineering into three processes: risk process, engineering process, and trust process. The SSE-CMM process

includes the analysis of threats, vulnerabilities, impacts, and related risks. SSE-CMM defines four risk processes: threat assessment process, vulnerability assessment process, event impact assessment process, and security risk assessment process. The assessment safety analysis is shown in Figure 5.

The risk information generated by the risk assessment process area depends on the threat information, vulnerability information, and impact information. Although the activities of collecting threat, vulnerability, and impact information are clustered into separate process areas, they are interrelated. The identification of information system security factors includes information leakage, integrity damage, business rejection, illegal use, etc. The main achievable threats include infiltration and implantation. Infiltration threats include counterfeiting, bypass control, and authorization infringement; embedded threats include trojans and trap gates. An implementation of such a threat will directly lead to an implementation of any basic threat [27, 28]. Potential threat: any potential threat may lead to some more basic threats. Vulnerability threat: it including analyzing system assets, defining specific vulnerabilities, and providing methods for assessing the vulnerability of the whole system. Risk analysis the analysis of vulnerability is based on two ways: treat vulnerability as a weak link that damages the confidentiality, integrity, and applicability of assets in security devices; treat vulnerability as a lack of safety devices and safety control functions. The risk analysis shall consider the relative effectiveness of the currently used control and safety devices. The safety devices to be analyzed can be divided into management safety, physical equipment safety, software safety, hardware safety, personnel safety, environmental safety, and communication safety. Possibility analysis of impact: the impact can be tangible, such as income loss, or intangible, such as reputation loss.

5. Conclusion

With the development of computer technology and the breakthrough in mathematics, people's encryption algorithms have also got the opportunity to flourish. The demand for secure information transmission and data storage will inevitably increase. At present, in practical applications, symmetric encryption technology is often used to deal with large amounts of data. However, its key is too short, which brings huge hidden dangers to information security. How to enhance the security of encryption key without weakening its operation speed is an important research direction for encryption algorithms. This paper is to meet this need and carry out in-depth research, and design a more valuable network file encryption transmission system.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] G. Yu, "Research on computer network information security based on improved machine learning," *Journal of Intelligent and Fuzzy Systems*, vol. 40, no. 3, pp. 1–12, 2020.

[2] A. Weathersby and M. Washington, "Extracting network based attack narratives through use of the cyber kill chain: a replication study," *It - Information Technology*, vol. 64, no. 1-2, pp. 29–42, 2022.

[3] L. Wu, J. Zhou, and Z. Li, "Applying of ga-bp neural network in the land ecological security evaluation," *IAENG International Journal of Computer Science*, vol. 47, no. 1, pp. 11–18, 2020.

[4] Q. Li, J. Yu, T. Kurihara, H. Zhang, and S. Zhan, "Deep convolutional neural network with optical flow for facial micro-expression recognition," *Journal of Circuits, Systems, and Computers*, vol. 29, no. 01, pp. 2050006-2050007, 2020.

[5] J. Chen, F. Zhao, and H. Xing, "Research on security of mobile communication information transmission based on heterogeneous network," *International Journal on Network Security*, vol. 22, no. 1, pp. 145–149, 2020.

[6] J. Zhao, "Research on network security defence based on big data clustering algorithms," *International Journal of Information and Computer Security*, vol. 15, no. 4, p. 343, 2021.

[7] P. Krishnakumar, "An overview on wormhole attack in wireless sensor networks," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 8, no. 2, pp. 63–66, 2020.

[8] S. Negi, M. Jayachandran, and S. Upadhyay, "Deep fake : an understanding of fake images and videos," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 7, no. 3, pp. 183–189, 2021.

[9] T. Ncubukezi, "A proposed: integration of the Monte Carlo model and the bayes network to propose cyber security risk assessment tool for small and medium enterprises in South Africa," *International Journal of Computer Science and Information Security*, vol. 3, no. 18, pp. 152–155, 2020.

[10] Y. Yu, L. Li, Y. Lu, and X. Yan, "On the value of order number and power in secret image sharing," *Security and Communication Networks*, vol. 2020, no. 3, pp. 1–13, Article ID 6627178, 2020.

[11] W. Lian, G. Nie, B. Jia, D. Shi, Q. Fan, and Y. Liang, "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," *Mathematical Problems in Engineering*, vol. 2020, no. 9, pp. 1–15, Article ID 2835023, 2020.

[12] H. Xie, Y. Wang, Z. Gao, B. P. Ganthia, and C. V. Truong, "Research on frequency parameter detection of frequency shifted track circuit based on nonlinear algorithm," *Nonlinear Engineering*, vol. 10, no. 1, pp. 592–599, 2021.

[13] Z. Liu, N. Su, Y. Qin, J. Lu, and X. Li, "A deep random forest model on spark for network intrusion detection," *Mobile Information Systems*, vol. 2020, no. 1, pp. 1–16, Article ID 6633252, 2020.

[14] H. Zhou and G. Yu, "Research on fast pedestrian detection algorithm based on autoencoding neural network and adaboost," *Complexity*, vol. 2021, no. 6, pp. 1–17, Article ID 5548476, 2021.

[15] S. K. Prasad, J. Rachna, O. I. Khalaf, and D. N. Le, "Map matching algorithm: real time location tracking for smart

security application," *Telecommunications and Radio Engineering*, vol. 79, no. 13, pp. 1189–1203, 2020.

[16] R. Huang, P. Yan, and X. Yang, "Knowledge map visualization of technology hotspots and development trends in China's textile manufacturing industry," *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 243–251, 2021.

[17] W. Qiu, Q. Tang, Y. Wang, L. Zhan, Y. Liu, and W. Yao, "Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3457–3468, 2020.

[18] J. Chen, S. Guo, X. Ma et al., "Slam: a malware detection method based on sliding local attention mechanism," *Security and Communication Networks*, vol. 2020, no. 1, pp. 1–11, Article ID 6724513, 2020.

[19] P. Elechi and C. O. Ahiakwo, "Design and implementation of an automated security gate system using global system for mobile communication network," *Journal of Network and Computer Applications*, vol. 7, no. 1, pp. 1–10, 2021.

[20] J. Liu, X. Liu, J. Chen, X. Li, T. Ma, and F. Zhong, "Investigation of ZrMnFe/sepiolite catalysts on toluene deg-radation in a one-stage plasma-catalysis system," *Catalysts*, vol. 11, no. 7, p. 828, 2021.

[21] L. N. Nguyen, J. D. Smith, J. Bae, J. Kang, J. Seo, and M. T. Thai, "Auditing on smart-grid with dynamic traffic flows: an algorithmic approach," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2293–2302, 2020.

[22] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A mean convolutional layer for intrusion detection system," *Security and Communication Networks*, vol. 2020, no. 176, pp. 1–16, Article ID 8891185, 2020.

[23] S. Kannan, G. Dhiman, Y. Natarajan et al., "Ubiquitous vehicular ad-hoc network computing using deep neural network with iot-based bat agents for traffic management," *Electronics*, vol. 10, no. 7, p. 785, 2021.

[24] T. Y. Lin and C. S. Fuh, "Quantum-resistant network for classical client compatibility," *Information Technology and Control*, vol. 50, no. 2, pp. 224–235, 2021.

[25] H. S. Yahia, S. R. M. Zeebaree, M. A. M. Sadeeq et al., "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling," *Asian Journal of Research in Computer Science*, vol. 8, no. 2, pp. 1–16, 2021.

[26] S. Abdelgaber, S. Marwa, and T. Munif, "Converting Kuwait from electronic government to smart government," *International Journal of Computer Science and Information Security*, vol. 18, no. 10, pp. 45–54, 2020.

[27] G. Veselov, A. Tselykh, A. Sharma, and R. Huang, "Special issue on applications of artificial intelligence in evolution of smart cities and societies," *Informatica*, vol. 45, no. 5, p. 603, 2021.

[28] P. Ajay, B. Nagaraj, R. A. Kumar, R. Huang, and P. Ananthi, "Unsupervised hyperspectral microscopic image segmentation using deep embedded clustering algorithm," *Scanning*, vol. 2022, pp. 1–9, Article ID 1200860, 2022.