Hindawi
Security and Communication Networks
Volume 2023, Article ID 9868457, 1 page
https://doi.org/10.1155/2023/9868457

Retraction

Retracted: Application of Data Encryption Technology in Network Information Security Sharing

Security and Communication Networks

Received 25 July 2023; Accepted 25 July 2023; Published 26 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets 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 own 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] D. Xu and W. Zheng, "Application of Data Encryption Technology in Network Information Security Sharing," *Security and Communication Networks*, vol. 2022, Article ID 2745334, 6 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2745334, 6 pages
https://doi.org/10.1155/2022/2745334

Research Article

Application of Data Encryption Technology in Network Information Security Sharing

Dongzhi Xu and Wenjuan Zheng

Xinxiang Vocational and Technical College, Xinxiang, Henan 453006, China

Correspondence should be addressed to Dongzhi Xu; 201804207@stu.ncwu.edu.cn

Received 6 July 2022; Revised 21 July 2022; Accepted 3 August 2022; Published 21 August 2022

Academic Editor: C. Venkatesan

In order to solve the problem of user information insecurity in the process of network information security sharing, this study proposes a data encryption technology based on network information security sharing. This method applies the data encryption technology to the computer network security protection, which can not only improve the computer network security but also protect the user data information security and provide users with more efficient and high-quality computer network services. The experimental results show that it takes about 2.35 seconds to generate a 1024-bit key pair. It takes about 12.29 seconds to encrypt a 2.1 m text document with a 1024-bit public key and about 561 seconds to decrypt a 2.1 m text document. *Conclusion*. The data encryption technology based on network information security sharing can effectively solve the problem of user information insecurity in the process of network information security sharing.

1. Introduction

With the continuous development of science and technology, people are more and more widely using electronic computers. Today's era is the information age, and computers are more and more used in people's lives and studies. People are becoming increasingly inseparable from computers, but computers also have many shortcomings resulting in endless network security problems, making the maintenance of network security by technicians a difficult task [1]. Therefore, through the implementation of computer security work, the computer network environment will be more secured and computer data encryption technology will be developed [2].

With the development of the times, the progress of the society, and the rapid rise of the economy, China has seen changes and optimization in various fields, especially in the field of information technology, where network interaction is very frequent. With the continuous expansion of the openness of the network, people's access to information and data has also been substantially improved, but the subsequent problem is the theft risk of network information and data. Therefore, people pay more and more attention to the security of their privacy in the network environment [3]. Data encryption is now more widely known as a result of this demand..

Based on this background, data information also need to have strong confidentiality and security, which can not only effectively prevent illegal elements from stealing and tampering with data information but also strengthen users' security experience in the process of data information transmission. Therefore, China should continue to study data encryption technology and continue to try and optimize it in practice, so as to seek security application channels in today's computer environment [4]. Due to the influence of viruses, hackers, and other factors, computer network security incidents have shown a high incidence trend in recent years, ranging from loss and leakage of data information to

network paralysis, affecting normal applications. Applying data encryption technology to computer network security protection has an important application value [5].

2. Literature Review

Information is a macroconcept, which is composed of data. In other words, data appear as a carrier. Therefore, we must take certain measures to protect data security and avoid data theft, destruction, or intentional modification. The best way to solve the problem of data security is to prevent data leakage through file encryption [6]. In other words, even if the file is stolen by hackers and other illegal users, it does not matter because the file is encrypted and cannot be correctly interpreted without the corresponding key. Therefore, data must be encrypted during network transmission [7]. Sometimes, even if the files are not transmitted in the network communication, users also need to encrypt some of their files because everyone has a lot of keys and private information that they do not want to be known or watched by others [8]. The identity authentication technology is implemented by software technology. It is a technology that can determine the identity of the users [9]. Before transmission, the data are encrypted and converted into ciphertext and then transmitted. This can ensure that the data users cannot get the correct information even if it is intercepted or copied during transportation. The introduction of encryption can maximize the security of data transmission in networked systems. It can be said that using technical means to encrypt data is the best processing method that can be thought of at this stage. With the rapid development of the Internet, people can conduct various transactions and exchanges on the Internet, which makes our life more interesting and our work more efficient. However, whether it is an old object or a new object, the two sides are always the same, so it is the same. For example, the problem of information security on the Internet has brought a lot of trouble to people. In recent years, it has been repeatedly exposed that personal information, personal privacy, or enterprise data information have been leaked, and this leakage is increasing every year.

Generally speaking, the leakage of network information has the following factors:

(1) Stealing information: in the process of data transmission, the gateway or router is a very dangerous node, where hackers can intercept the transmitted data information. If the data are not encrypted on the network, it will lead to information leakage.

(2) Tampering with information: if the data are not encrypted on the network, the intruder can tamper with the data information after intercepting the information, so that the data receiver cannot obtain the real information.

(3) Impersonate authorized users: through the means of stealing data information and then modifying the information, pretend to be an authorized user to enter the system.

(4) Malicious damage: after entering the system as an authorized user, an unauthorized user can maliciously destroy the system information, and the consequences are very serious.

In our life, data encryption becomes more and more important, especially considering that a large number of transactions and data transmission occur on the Internet every day. At present, data encryption is the most effective way to protect information security. Through encryption technology, achieve the concealment of important information and protect the transmission security of data information. Therefore, data encryption is extremely necessary and indispensable in ensuring data security.

On the basis of current research, this study proposes a data encryption technology based on network information security sharing. The use of data encryption technology requires setting a password. This encryption method has also been accepted and used by the public. This technology guarantees the security of people when using the network, reduces the insecurity and instability of the network in the communication process, reduces the possibility of insecurity when consuming the network, and guarantees the purchased network services that can be used independently and the privileges that can be shared with people. From the operational point of view, this technology can ensure the safety and continuous operation of network communication. This technology is protected in the process. By improving the effectiveness of network communication during use, the equipment can be more secure and stable during operation, so as to meet the needs of customers for consumer services and further develop the network communication technology [10].

3. Research Methods

3.1. System Safety Design

(1) Network transmission encryption [11]: prevent someone from illegally obtaining the reported information and content in transmission by means of network eavesdropping (it is obvious that if we do not encrypt, it will be very dangerous). We must highly encrypt the data in transmission to ensure that everything is safe and that even if it is eavesdropped, it is "inaudible" (because it cannot be decrypted and understood). One-way encryption that cannot be reversed is adopted for passwords and other authentication information.

(2) Data file encryption [12]: to prevent the illegal acquisition of reported information, all reported data files must be encrypted with file encryption software based on the RSA encryption algorithm, and the downloaded data files must be decrypted with a private key.

(3) Data storage security [13]: data related to the reported content is encrypted and stored in the database to prevent data leakage caused by database security or internal personnel violations. The

database permissions are strictly managed. The database is only allowed to be accessed locally on the server to ensure that the data will not be leaked due to problems such as database password theft.

(4) Login security: the number of password errors of the specified user cannot exceed 3 times in a single day; otherwise, the account will be locked. Through this measure, it can avoid exhaustively trying out the user's password.

(5) Log management: all user operations in the system are logged. It mainly records the basic information of user name, login time, operation module, data update, and system exit.

(6) System management security [14]: the highest authority administrator has maintenance administrator authority, and the system administrator account can only log in on the server.

3.1.1. System Database. The goal of database design is to model the business data in the functional modules of the system and design the data tables and the relationship between them, so as to support the operation of business functions [15]. The E-R diagram of the network reporting system is shown in Figure 1. Here, only some entity relationships are listed for demonstration [16].

3.1.2. Solving Single Point of Failure. To avoid a single point of failure, the solution is shown in Figure 2.

For the abovementioned three modules, the master and slave are synchronized in real-time. Once the master or slave fails, there will always be another replacement. There will be no downtime and other single points of failure [17].

3.2. Working Principle of the RSA Algorithm. RSA is a kind of asymmetric key, and it is a very typical one. Here, it is its working principle: first, a key pair containing public and private keys should be generated [18]. The public key, as the name suggests, is public and available to all. It is used for encryption, and then, the encrypted data are transmitted to the public key publisher [19]. The private key is private. It is only owned by the publisher and will not be made public. It is the core secret used to decrypt data [20]. The private key cannot be calculated only by getting the key. Because the private key is confidential, the data encrypted with the public key are secure and can reach the receiver only. At the same time, in order to be more secure and improve the strength of encryption, the RSA key length should not be too short; otherwise, its reliability will be affected. Generally, we set it to 512 or 1024 bits, as shown in Figure 3.

The RSA algorithm is an asymmetric and very secure algorithm. From the above, the biggest feature of this algorithm is that it uses completely different keys for encryption and decryption. The public key encryption key, private key decryption key, and the *c* principle of encryption and decryption of the RSA algorithm are as follows:

Public key PR: n: the product of two prime numbers p and q; e: the product of $(p-1)$ and $(q-1)$ is mutually prime;

Private key PU: n: product of two prime numbers P and Q

$$d = e^{-1} (\mathrm{mod}\,(p-1)(q-1)). \tag{1}$$

Encryption:

$$c \equiv m^e \mathrm{mod} n. \tag{2}$$

Decrypt:

$$m \equiv c^d \mathrm{mod} n. \tag{3}$$

The specific process is as follows:

(1) Select two different prime numbers p, q with long enough digits;

(2) Calculate the value of n according to the formula $n = p * q$;

(3) Calculate $(p-1) * (q-1)$, whose product is calculated as $f(n)$ (p, q are unknowable);

(4) Specify an integer e greater than 1, which must be less than $(p-1) * (q-1)$ and mutually prime with it, usually 3 or 17 or 65537;

(5) Through the formula $d * e \equiv 1 \mathrm{mod} f(n)$, e and $f(n)$ are known; we can find d. mod is a remainder operation, that is, the value of the remainder of B to C is equal to 1;

(6) n and e are selected by us to be used as public keys, and n and d are selected by us to be used as private keys (public keys e and n are public, and d must be kept a secret);

(7) The encryption calculation method is $C \equiv M^e \mathrm{mod} n$, when the length is long, segmentation operation is required;

(8) The decryption calculation method is $M \equiv C^d \mathrm{mod} n$, and the relationship between plaintext length and key length in the RSA algorithm is described in the algorithm implementation chapter.

It is known from the above that e and $n$are public keys, which are known by everyone and can be used for encryption. However, d cannot be obtained from e and n, which is supported by its basic theory. Therefore, only those who are legal can have d and only those who are private can decrypt [21].

3.2.1. Design Public Key KU and Private Key KR. Here, we specify the values of p and q, which are smaller for ease of calculation. Then, p is specified as 3, and q is specified as 11. Obviously, the value of n is 33, and the value of $(p-1)(q-1)$ is 20. For this purpose, we write it as $f(n)$. The value of is also taken as small as possible, so it is taken as 3 [22]. After the above values are clear, the evaluation formula of d is $d^*e \equiv 1 \mathrm{mod} f(n)$. Thus, the value of d can be calculated. Since the value is small, we can find it through trial calculation. Table 1 provides the trial calculation results.

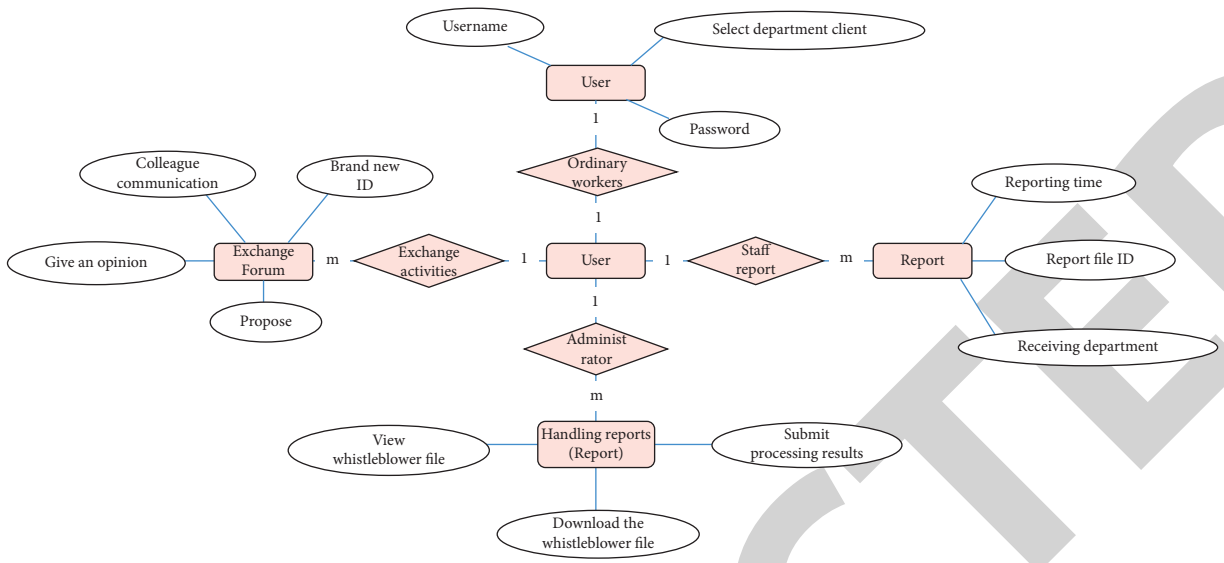

Figure 1: Database table.

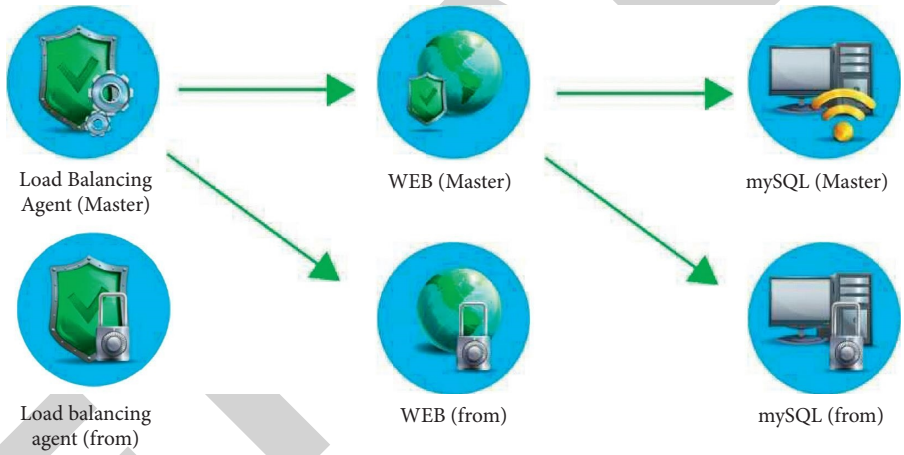

Figure 2: Fully realize no single point.

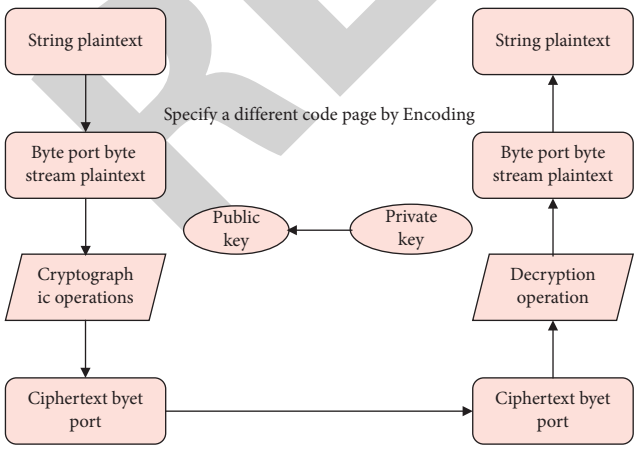

Figure 3: Diagram of the RSA basic operation process.

Table 1: Trial calculation process for obtaining d value.

D	$d * e$	$d * e \equiv 1 \bmod f(n)$
1	3	3
2	6	9
3	9	12
4	12	12
5	15	15
6	18	18
7	21	1

Through the trial calculation in the above table, we find that when $d = 7$, the identity is true. Take the value of d as 7, so you can get the private key. The two values of the private key are 7 and 33. The two values KU of the corresponding public key are 3 and 33. So far, we have generated a pair of key pairs. Let us verify it.

Table 2: Comparison table of transformation between letters and code values.

Letter	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
Code value	01	02	03	04	05	06	07	08	09	10	11	12	13
Letter	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
Code value	14	15	16	17	18	19	20	21	22	23	24	25	26

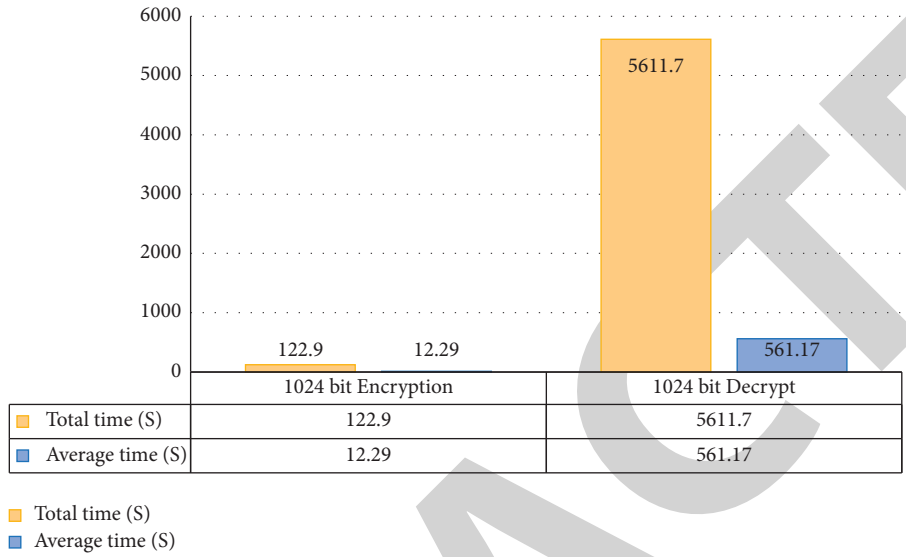

Figure 4: Ten-test data chart.

3.2.2. English Digitalization. Convert the plaintext information into numbers, assuming a transformation rule of letters and code values. The corresponding relationship assumed in this study is shown in Table 2.

It can be seen from the abovementioned table that the digital codes of English keys are 11, 05, and 25.

3.2.3. Plaintext Encryption. The user transforms the information obtained in the second step into ciphertext that others cannot read through the encryption key (3, 33). The ciphertext after transformation is obtained from $C \equiv M^e \bmod n$: 11, 31, 16.

3.2.4. Ciphertext Decryption. When we get the ciphertext, we perform transformation processing according to the formula $M \equiv C^d \bmod n$, that is, decryption, that is, we can get the digital coding information of the decrypted plaintext: 11, 05, 25. Find the corresponding letters according to Table 2, and you can get the plaintext KEY [23].

4. Result Analysis

Through ten tests, the length of time used to encrypt and decrypt a 2.1M TXT document with a 1024-bit key pair is given. Figure 4 shows the ten-test data chart.

From the above test, it can be seen that the time required to generate a key pair with 1024 bits is about 2.35 seconds. It takes about 12.29 seconds to encrypt a 2.1 m text document with a 1024-bit public key, and about 561 seconds to decrypt a 2.1 m text document.

5. Conclusion

In this study, a data encryption technology based on network information security sharing is proposed. Based on network transmission security, cryptography, and encryption algorithm, the RSA encryption algorithm is the core; combined with the requirements of file encryption, the search and test of large prime numbers are deeply studied and analyzed and implemented with software. In addition, the file encryption and decryption software has been developed to do a variety of detailed experiments on the production key of the client and the time efficiency of encryption and decryption, which show that the client can absolutely meet the use and the design requirements of users. In the actual process of data transmission, a variety of encryption methods are used to encrypt and decrypt the data, so as to provide a strong guarantee for the security of data and information in transmission. In modern society, more and more people pay attention to the future development of computer networks. Therefore, the technology of encrypting data and information should keep pace with the times, conform to the development trend of the times, and minimize the threat of damage to computer network information security.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. J. Harris and R. E. Christenson, "Real-time hybrid simulation using analogue electronic computer technology," *International Journal of Lifecycle Performance Engineering*, vol. 4, no. 1/2/3, p. 25, 2020.

[2] N. Zhang, "Research on the application of data encryption technology based on network security maintenance in computer network security," *Journal of Physics: Conference Series*, vol. 1744, no. 2, Article ID 022060, 2021.

[3] S. K. S. Chia, M. C. Lo, Z. B. Razak, Y. C. Wang, and A. A. Mohamad, "Impact of destination image on tourist satisfaction: the moderating effect of information technology (it)," *Geojournal of Tourism and Geosites*, vol. 34, no. 1, pp. 88–93, 2021.

[4] W. M. M. Hsu, D. B. Kastner, S. A. Baccus, and T. O. Sharpee, "How inhibitory neurons increase information transmission under threshold modulation," *Cell Reports*, vol. 35, no. 8, Article ID 109158, 2021.

[5] D. Zhao, H. Song, and H. Li, "Fuzzy integrated rough set theory situation feature extraction of network security," *Journal of Intelligent and Fuzzy Systems*, vol. 40, no. 4, pp. 8439–8450, 2021.

[6] S. M. Hossein, D. De, P. Mohapatra, S. P. Mondal, and N. Senu, "Dna sequences compression by gp2r and selective encryption using modified rsa technique," *IEEE Access*, vol. 8, no. 99, p. 1, 2020.

[7] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications," *Vehicular Communications*, vol. 28, no. 1, Article ID 100306, 2021.

[8] G. Manogaran, C. H. Hsu, P. M. Shakeel, and M. Alazab, "Non-recurrent classification learning model for drone assisted vehicular ad-hoc network communication in smart cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2792–2800, 2021.

[9] Z. Chen and S. Wu, "Research on digital identity authentication technology based on block chain," *Journal of Physics: Conference Series*, vol. 1802, no. 3, Article ID 032091, 2021.

[10] Y. Yan, "Analysis on the change of big data and computer network communication technology based on multi-platform," *Journal of Physics: Conference Series*, vol. 1982, no. 1, Article ID 012192, 2021.

[11] P. Lingzhi, Z. Yizhu, Z. Di, W. Jianguang, D. Limin, and S. Lingwen, "Research and application of a new encryption transmission technology of internet of things based on plc power line carrier communication," *IOP Conference Series: Earth and Environmental Science*, vol. 791, no. 1, Article ID 012087, 2021.

[12] S. Zaineldeen and A. Ate, "Improved cloud data transfer security using hybrid encryption algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, pp. 521–527, 2020.

[13] H. Altuwaijri and S. Ghouzali, "Android data storage security: a review," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 5, pp. 543–552, 2020.

[14] S. A. A. Bokhari and S. Manzoor, "Impact of information security management system on firm financial performance: perspective of corporate reputation and branding," *American Journal of Industrial and Business Management*, vol. 12, no. 05, pp. 934–954, 2022.

[15] M. V. Grafkina and A. V. Pitryuk, "Analysis and evaluation of the database on soil contamination of the moscow region with heavy metals," *IOP Conference Series: Earth and Environmental Science*, vol. 723, no. 4, Article ID 042016, 2021.

[16] S. Wang, L. Dong, S. He et al., "Prediction and analysis of erosion failure danger point of high-pressure manifold," *International Core Journal of Engineering*, vol. 6, no. 1, pp. 103–111, 2020.

[17] V. S. Rahul, N. N. Prasanth, and S. P. Raja, "A recursive and parallelized dynamic programming implementation of hard merkle-hellman knapsack system for public key cryptography," *Cybernetics and Information Technologies*, vol. 21, no. 2, pp. 58–69, 2021.

[18] 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.

[19] A. Sharma and R. Kumar, "Performance comparison and detailed study of AODV, DSDV, DSR, TORA and OLSR routing protocols in ad hoc networks," in *Proceedings of the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, IEEE, Waknaghat, India, December 2016.

[20] M. S. Pradeep Raj, P. Manimegalai, P. Ajay, and J. Amose, "Lipid data acquisition for devices treatment of coronary diseases health stuff on the internet of medical things," *Journal of Physics: Conference Series*, vol. 1, Article ID 012038, 2021.

[21] J. Liu, X. Liu, J. Chen, X. Li, and F. Zhong, "Plasma-catalytic oxidation of toluene on Fe_2O_3/sepiolite catalyst in DDBD reactor," *Journal of Physics D: Applied Physics*, vol. 54, no. 47, Article ID 475201, 2021.

[22] 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, Article ID 1200860, 9 pages, 2022.

[23] L. Yan, K. Cengiz, and A. Sharma, "An improved image processing algorithm for automatic defect inspection in TFT-LCD TCON," *Nonlinear Engineering*, vol. 10, no. 1, pp. 293–303, 2021.