Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9814743, 1 page
https://doi.org/10.1155/2023/9814743

Retraction

Retracted: Application of Information Encryption Technology in Computer Network Communication Security

Wireless Communications and Mobile Computing

Received 18 July 2023; Accepted 18 July 2023; Published 19 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This article has been retracted by Hindawi following an investigation undertaken by the publisher [1].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] H. Zhang, "Application of Information Encryption Technology in Computer Network Communication Security," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9354441, 7 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9354441, 7 pages
https://doi.org/10.1155/2022/9354441

Research Article

Application of Information Encryption Technology in Computer Network Communication Security

Hongbo Zhang

Xinxiang Vocational and Technical College, Xinxiang, Henan 453000, China

Correspondence should be addressed to Hongbo Zhang; 31115412@njau.edu.cn

Received 17 June 2022; Revised 13 July 2022; Accepted 22 July 2022; Published 8 August 2022

Academic Editor: Balakrishnan Nagaraj

In order to improve the communication efficiency while ensuring the security of communication information, this paper proposes a design and research method of a computer information security communication method by introducing data encryption technology. A new communication method is proposed through the construction of computer information security communication transmission model, computer information communication user identity authentication, communication information data encryption and decryption processing based on data encryption technology, and computer secondary communication key update. The experimental results show that the new communication method and ZigBee-based communication method are applied to the same communication environment through comparative experiments. The addition of encryption time and decryption time of the experimental group can be basically controlled within 70 ms, while the addition of encryption time and decryption time of the control group exceeds 70 ms, which verifies that the new communication method has higher security and communication efficiency. The introduction of data encryption technology in the actual information communication process can provide guarantee conditions for information security.

1. Introduction

With the continuous progress of science and technology, information technology has also been rapidly developed. More and more viruses and hackers affect people's normal life and even bring economic losses to people. In this context, the computer has derived the data encryption technology to ensure the security of computer network communication and protect people's privacy. At the same time, as the global attention to the value of information is gradually increasing, people are increasingly influenced by science and technology. The greater the impact of information value on people, the more important network communication security is in the development of computers. In order to protect people's communication security and ensure that people's privacy is not infringed, computer practitioners must strengthen the research on computer network communication security and use corresponding data processing technology to ensure information security [1–3].

With the continuous development of the network age, the attacks, and intrusions of network hackers, criminals and viruses make the network information maliciously tampered and stolen, which poses a serious threat to the security of network information. If the data encryption technology is applied to the computer network communication security, it can not only avoid the tampering and stealing of the network information data and ensure the authenticity and integrity of the network information data but also protect the user's private information. Data encryption technology, as its name suggests, means that the transmitted network information data is securely converted by using encryption keys, so that the readable information data becomes a series of garbled codes (also known as ciphertext) [4, 5]. This kind of garbled code has no meaning and cannot be accurately read and understood by the thief. Only when the receiver uses the decryption key after receiving the garbled code can the garbled code be decrypted. Compared with other information technologies, data encryption technology not only has simple and clear logic but also has low technical difficulty, which reduces the learning cost of technicians in related fields and lays a solid foundation for the effective promotion and application of this technology. At the same

time, data encryption technology plays an important role in the construction of the network security system [6, 7].

The computer network security protection architecture is shown in Figure 1. From the figure, it can be clearly seen that users strengthen the stability, reliability, and security of computer network communication from the two aspects of encryption cognition and key management [8]. At the same time, various functional modules such as security protocol, virus protection, attack protection, and access control should be effectively combined and connected, so as to comprehensively improve the security level of computer network communication and create good conditions for scientifically and effectively avoiding the attacks of hackers and criminals. Therefore, it is of great practical significance to strengthen the application of data encryption technology to improve the security, integrity, and confidentiality of network information data [9].

2. Literature Review

In recent years, the continuous progress of network technology has greatly promoted the development of e-commerce industry. The application of data encryption technology in this field can better meet the development needs of e-commerce [10]. The emergence of e-commerce has greatly changed people's production, life, and social production mode. People can buy goods without leaving home, and businesses can sell goods without leaving home. However, it should be pointed out that the stable development of e-commerce is based on a safe and reliable computer network environment. As a trading platform for consumers and merchants, e-commerce platform must ensure the security of transactions and avoid disclosing users' address information, telephone information, and payment password. The application of SSL, set and other security protocols, digital certificates, digital signatures, and other data encryption technologies in e-commerce can effectively guarantee the information of both parties to the transaction. Moreover, the application of data encryption technology is an important measure to protect LAN. The rapid development of the current market economy has brought huge development opportunities for small- and medium-sized enterprises. During the development of enterprises, a lot of data information will be generated. Enterprises should establish a dedicated LAN inside, which is an important target of viruses and hackers. Once the LAN is damaged, it will lead to data information leakage and cause huge losses to enterprises. Through the application of data encryption technology, we can realize the effective protection of LAN, avoid information leakage, and ensure the security of enterprise internal data and information. Even if there is a problem in the enterprise LAN, the source can be identified in time and the handling work can be done well to reduce losses [11].

In the process of data encryption, it is necessary to comprehensively check the integrity and security of the information content of secret files in the computer network system to ensure that they will not be threatened by viruses. The application of computer needs a lot of software, so it is very important to encrypt the software, which is the focus that

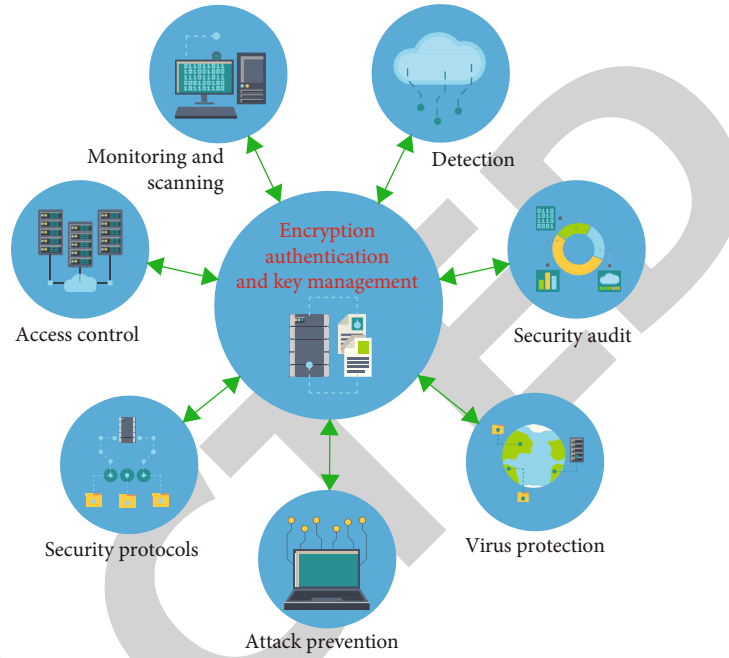

Figure 1: Computer network security protection architecture.

users have been paying attention to. At this stage, the emergence and application of microblog, WeChat, TikTok, and other software have greatly enriched people's interaction and entertainment methods. These software need to be encrypted in the application process to ensure the safe operation and application of the software. Another example is as follows: Currently, many mobile and computer games, such as King Glory, Hero League, Crossing the Line of Fire, etc., need to set multiple encryption locks during operation. From the perspective of users, online games are a way of entertainment, while from the perspective of developers, online games are for profit [12]. The higher the activity of online games, the more vulnerable they are to attacks. By encrypting the data of online games, users' passwords and information can be effectively protected to avoid losses caused by leakage. At the same time, it can safeguard the interests of game developers and ensure the safe operation of games. No matter what kind of encryption system is used, data encryption technology mainly includes plaintext, ciphertext, and encryption and decryption device or algorithm, namely, the key. The model composition of the security system is shown in Figure 2.

3. Method

3.1. Construction of Computer Information Security Communication Transmission Model. In order to realize the secure communication of computer information, it is necessary to determine the specific transmission path first. In combination with the relevant requirements of the computer communication security specification, the communication transmission model adopted in the design of the computer information security communication mechanism is shown in Figure 3 [13].

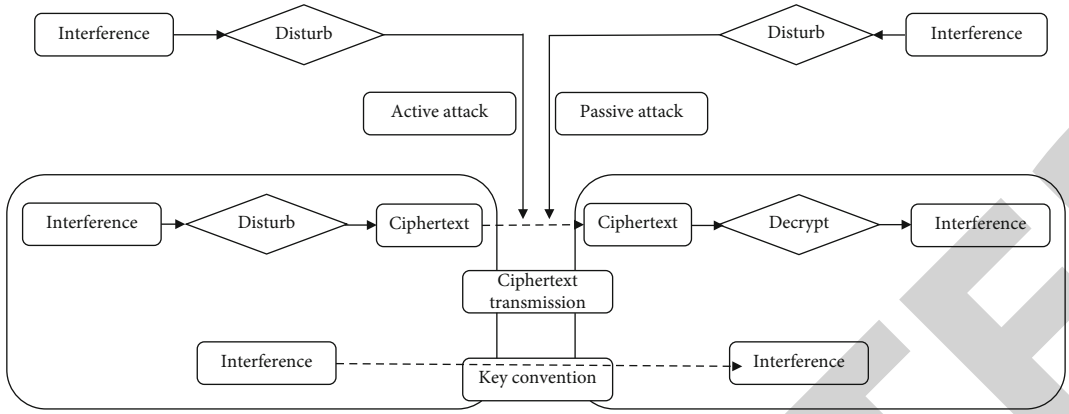

Figure 2: Composition of security system.

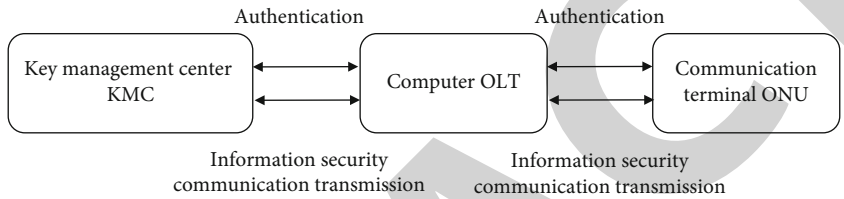

Figure 3: Computer information security communication transmission model.

Using the computer information security communication transmission model constructed above, the two-way authentication between the communication transmission terminal and each computer terminal is completed, so as to realize the identification and isolation of illegal intruders. At the same time, data encryption technology is introduced into the model to build a more perfect secure communication mechanism for communication methods. In Figure 3, the key management center is mainly used to manage the encryption key of computer network information and data and to license and authenticate the relevant equipment of the information communication network connected to the computer network. The computer OLT is mainly used to adjust the basic control unit in the network, and the communication terminal ONU is mainly used to realize the interaction of users at each communication receiving end and sending end and to manage and configure the communication information transmitted in this process. In the process of computer information security communication transmission, identity authentication can be used to identify and authenticate the identity of users at the receiving end and the sending end. Only users who have passed identity authentication can realize information communication transmission in the computer network.

3.2. Computer Information Communication User Identity Authentication. The whole process of communication authentication is as follows: first, the sending end user generates the information that needs computer communication. Secondly, SHA-1 or MD5 is used to generate a hash code for this group of information. According to the private key of the sending end user, encrypt the hash code according to RSA and put the obtained results into the communication information. Verify the identity of the receiving end user and judge whether the receiving end user matches the sending end user. If it matches, the session key is used to decrypt the communication information. If it does not match, the information receiving request of the receiving end user is directly ignored. If the symmetric password authentication mechanism is adopted, a symmetric key needs to be introduced between any communication transmission channel, which is easy to cause a large number of nodes and affect the key generation and management. Therefore, the public key mechanism is used to authenticate the identity of both sides of communication. By distributing any one of the trusted keys, the number of key nodes can be effectively reduced, so as to improve the communication efficiency of the computer. The authentication information needs to include the user ID of the receiving end or the sending end, the public key or private key information of a node in the communication channel, the random number corresponding to a node, and the connection symbol between various information data. The generation method of random numbers can be expressed by the following:

$$X = g^x \bmod p. \tag{1}$$

In formula (1), X is the generated random number, G refers to the common parameters negotiated by the users at the receiving end and the sending end, X represents the random number with the largest value selected by the user at the sending end, and P is a large prime number. According to the above formula, the random number of a group of communication information user authentication

Table 1: Communication information data encryption and decryption symbols based on data encryption technology.

Serial number	Symbol	Meaning
(1)	Ks	Communication key, used in encryption system
(2)	KRa	The private key of the user at the receiving end or the sending end is used in the public key encryption mechanism
(3)	KUa	The public key used by the user at the receiving end or the sending end is used in the public key encryption mechanism
(4)	EP	Public key encryption processing
(5)	DP	Public key decryption processing
(6)	EC	Symmetric encryption processing
(7)	DC	Symmetric decryption processing
(8)	||	Tandem relation
(9)	Z	Zip encryption algorithm compression processing

information is calculated. Only when the user's identity information contains all the above contents can it enter the process of identity authentication. In the absence of any content, it is considered that the information is incomplete and cannot be brought into the process of user identity authentication. The transmission of corresponding communication information or the regeneration of user identity authentication information is stopped and reauthenticated.

3.3. Encryption and Decryption of Communication Information Data Based on Data Encryption Technology. To realize the encryption and decryption of communication information data is an effective method to ensure the secure communication of computer information [14]. Therefore, after the identity information authentication of the communication user is completed, the data encryption technology is introduced to encrypt and decrypt the communication information data. According to the three different levels of computer information communication, different encryption methods are adopted. The symbols used in the encryption process are shown in Table 1.

After specifying the symbols in the encryption and decryption process, a crypto device is added between the node and the modem to generate the corresponding key. The header and message are encrypted at the same time, and the intermediate nodes in the communication information are encrypted [15]. When encrypting, the end-to-end encryption method can allow the whole communication process to be decrypted and further improve the security of communication information. In the above encryption process, the encryption results at different levels can be expressed by the following:

$$m_i : \{ci, \text{seq}, i, T_i\}. \quad (2)$$

In formula (2), m_i is the encrypted communication information, c_i represents the generated ciphertext, Seq is the session sequence number of the group of communication information in the computer network communication environment, i represents a block identifier as communication information, and T_i is the timestamp of the communication information.

After encrypting the communication information data, if the receiving end user wants to obtain the real data in the information, it also needs to decrypt [16]. After acquiring the communication content expressed in formula (2), the receiving end user authenticates the identity information of the sending end user according to the authentication code negotiated by both parties in advance and decrypts it after ensuring that the authentication passes. According to the block identification of the encrypted communication information, all the information is reorganized to recover the communication information transmitted by the user at the sending end to obtain the plaintext. Through the above discussion, complete the encryption and decryption of communication information data, ensure the security of information in the computer communication environment, and realize the accurate processing of information.

3.4. Computer Secondary Communication Key Update. If the same key is used for a long time, the probability of information disclosure will increase. Therefore, the key used in the first communication process will be updated. In the communication method designed in this paper, the key management center is responsible for setting and configuring the key update during unicast communication [17]. After completing a communication task, the key needs to be updated within the specified time. It is executed by using the key update function provided by OpenSSL and initiated by the KGC key control center. During the update process, the master key and temporary private key are selected, and the master key update program is called. All private keys are obtained through operation, and the final key parameter results are published.

4. Results and Discussion

4.1. Experimental Preparation. In order to further verify the application advantages of data encryption technology in this communication method, this method and the ZigBee-based communication method are applied to the same

computer communication environment [18]. It is known that the environment in which the two communication methods are applied in the experiment is the distribution network of a power enterprise. The simulation of the real information communication environment is realized by simulating the secure communication process of the network control center in the computer. In this experimental environment, the memory of the computer is 512 M, the main frequency is 512 mHz, including 3.2 GHz Intel i5 480 processor, and 256 mssd hard disk. In order to facilitate the follow-up discussion, the communication method based on data encryption technology proposed in this paper is set as the experimental group, and the traditional communication method based on ZigBee is set as the control group. The two communication methods are applied to the above experimental environment.

4.2. Comparative Analysis on the Security of Communication Methods between the Experimental Group and the Control Group. The capacity value is selected as the evaluation index of the feasibility of information communication security encryption, and the capacity is expressed as the loss of information data in the communication process. When a computer is threatened during communication, its capacity will change. At the same time, the greater the noise in the communication process, the greater the capacity loss. When there is no zero space in the computer communication environment, it indicates that the capacity has been lost. At this time, the information data in the communication process will be lost. That is, the larger the capacity value, the better the encryption effect of the communication method. The smaller the capacity value, the worse the encryption effect of the communication method. The calculation formula of capacity value (3) is

$$K = P - \frac{\delta}{M}. \tag{3}$$

In formula (3), K is the computer capacity value, δ represents the amount of data lost in the communication transmission channel during computer information communication, M represents the information traffic that the computer needs to complete, and P is the total space capacity of computer communication. According to the above formula, the capacity of the two communication methods of the experimental group and the control group is calculated. In order to ensure the objectivity of the experimental results, in the communication process, the experimental parameters under the application of the two communication methods are set the same. Set the information communication transmission path to 8, including 8 communication information receiving ends and 8 communication information sending ends. The total power in the communication process is 750 mW, the data frame length is 4/5, the adjustment mode of communication information is BPSK, and the fixed signal-to-noise ratio of communication transmission channel is 4.5 db. According to the above experimental parameter settings, the comparative experiment is completed, and the capacity of the two traffic methods of the experimental group and the control group is calculated according to formula (3), as shown in Figure 4.

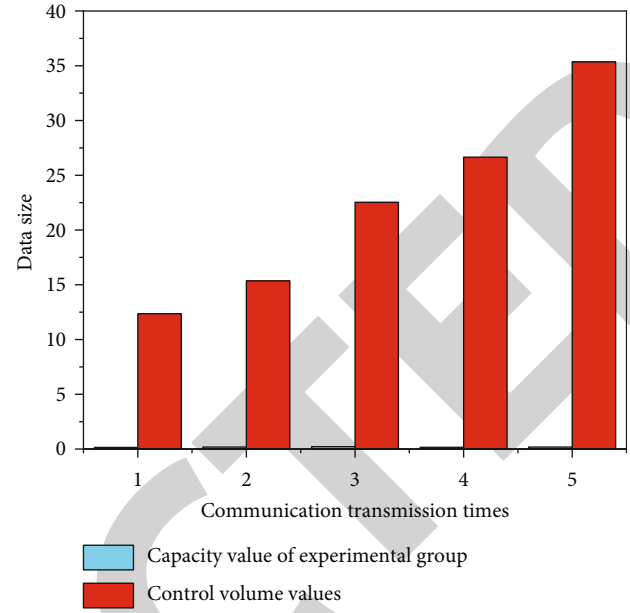

Figure 4: Record of capacity value of communication method between the experimental group and control group.

Table 2: Comparison record of communication efficiency between the experimental group and control group.

Communication transmission path	Experimental group time		Control group time	
	Encryption	Decrypt	Encryption	Decrypt
Path I	26 ms	26 ms	38 ms	39 ms
Path II	31 ms	28 ms	42 ms	46 ms
Path III	22 ms	22 ms	48 ms	48 ms
Path IV	25 ms	26 ms	45 ms	49 ms
Path V	26 ms	25 ms	39 ms	51 ms

From the data recorded in Figure 4, it can be seen that in the five communication transmissions, the capacity value of the experimental group is obviously smaller, and with the continuous increase of the amount of communication information data, the capacity value of the control group shows an increasing trend, while this phenomenon does not occur in the experimental group. Therefore, it is proved that the communication method based on data encryption technology proposed in this paper can effectively reduce the capacity value of the computer in practical application, will not be affected by the amount of information data, and has higher communication security and stability [19].

4.3. Comparative Analysis on Communication Efficiency of Communication Methods between the Experimental Group and Control Group. Choose the time-consuming situation in the process of encrypting and decrypting communication

information as the evaluation index and compare the time-consuming situation of encrypting and decrypting information in the process of communication between the two communication methods. Select 5 random information communication transmission paths from the above 8 as the research object, perform encryption and decryption processing for different information on different communication transmission paths, record the corresponding time, and draw it into Table 2.

From the data obtained in Table 2, it can be seen that the addition of encryption time and decryption time of the experimental group can be basically controlled within 70 ms, while the addition of encryption time and decryption time of the control group exceeds 70 ms. In the actual process of computer information communication, there is a network delay phenomenon. The whole communication time of the experimental group, that is, the sum of encryption and decryption time and network delay, can still be controlled at the MS level, while the control group communication method can not achieve this effect. Therefore, the above experimental results further prove that the communication method based on data encryption technology in this paper can further improve the efficiency of communication and effectively ensure the needs of computer information communication on the premise of ensuring information security [20].

5. Conclusion

In this paper, a new communication method is proposed, and the feasibility and advantages of this method are verified from two aspects of security and communication efficiency through comparative experiments. In practical application, the communication method proposed in this paper effectively solves the problem of low efficiency of computer information communication to a certain extent by introducing data encryption technology and greatly improves the security and reliability of communication. However, this communication method is only applicable to ensure the secure communication transmission of information from three aspects: computer access authentication, information encryption, and information signature. If it needs to be more reliable, it also needs to comprehensively consider the entire security scheme according to the computer security system. Therefore, in the follow-up research, more in-depth research will be carried out to provide innovative directions for the further improvement and optimization of the general methods in this paper.

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 declares that he/she has no conflicts of interest.

References

[1] K. Mbise, "The role of it professional certifications in instructors' teaching quality," *The International Journal of Education and Development using Information and Communication Technology*, vol. 17, no. 1, pp. 176–187, 2021.

[2] S. Shi, Y. Wang, C. Zou, and Y. Tian, "AES RSA-SM2 algorithm against man-in-the-middle attack in IEC 60870-5-104 protocol," *Journal of Computer and Communications*, vol. 10, no. 1, pp. 27–41, 2022.

[3] E. W. Lee and G. A. Seomun, "Structural model of the healthcare information security behavior of nurses applying protection motivation theory," *International Journal of Environmental Research and Public Health*, vol. 18, no. 4, p. 2084, 2021.

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

[5] D. A. Chaudhari and E. Umamaheswari, "A new adaptive XOR, hashing and encryption-based authentication protocol for secure transmission of the medical data in Internet of Things (IoT)," *Biomedical Engineering/Biomedizinische Technik*, vol. 66, no. 1, pp. 91–105, 2021.

[6] M. Park, J. Kim, Y. Kim, E. Cho, and T. T. Kwon, "An SGX-based key management framework for data centric networking," in *International Workshop on Information Security Applications*, p. 1, Springer, Cham, 2020.

[7] M. Ahmad and E. A. Solami, "Evolving dynamic S-boxes using fractional-order Hopfield neural network based scheme," *Entropy*, vol. 22, no. 7, p. 717, 2020.

[8] T. Yan, J. Liu, Q. Niu, J. Chen, and M. Niu, "Network security protection technology for a cloud energy storage network controller," *Global Energy Interconnection*, vol. 3, no. 1, pp. 85–97, 2020.

[9] L. Teng, H. Li, S. Yin, and Y. Sun, "A modified advanced encryption standard for data security," *International Journal of Network Security*, vol. 22, no. 1, pp. 112–117, 2020.

[10] Y. Song, H. S. Lim, and J. Oh, "We think you may like this: an investigation of electronic commerce personalization for privacy-conscious consumers," *Psychology and Marketing*, vol. 38, no. 10, pp. 1723–1740, 2021.

[11] J. L. Ding and B. Shi, "Analysis and modeling of enterprise competitive intelligence based on social media user comments," *Entrepreneurship Research Journal*, vol. 11, no. 2, pp. 47–69, 2021.

[12] J. Calvo and L. Urriolagoitia, "McDonald's Japan and Pokémon Go: IoT gamification," *Asian Case Research Journal*, vol. 24, no. 2, pp. 105–121, 2021.

[13] F. Liu and C. Masouros, "A tutorial on joint radar and communication transmission for vehicular networks - part iii: predictive beamforming without state models (invited paper)," *IEEE Communications Letters*, vol. 25, pp. 327–331, 2020.

[14] R. Marqas, S. M. Almufti, and R. Rebar, "Comparing symmetric and asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms," *Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture & Technology*, vol. 12, no. 3, pp. 3110–3116, 2020.

[15] S. Das and A. Singh, "Function modulation – the theory for green modem," *International Journal on Advances in Networks and Services*, vol. 2, no. 2&3, p. 121, 2020.

[16] J. Gu, W. Wei, R. Yin, C. V. Truong, and B. P. Ganthia, "Complex circuit simulation and nonlinear characteristics analysis of GaN power switching device," *Nonlinear Engineering*, vol. 10, no. 1, pp. 555–562, 2021.

[17] P. Ajay, B. Nagaraj, R. Arun 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.

[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 (Slovenia)*, vol. 45, no. 5, p. 603, 2021, http://www.informatica.si/index.php/informatica/article/view/3600.

[19] M. 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," in *Journal of Physics: Conference Series, Volume 1937, International Conference on Novel Approaches and Developments in Biomedical Engineering-2021 (ICNADBE 2021)*, Coimbatore, India, April 2021.

[20] N. Yuvaraj, K. Srihari, G. Dhiman, K. Somasundaram, and M. Masud, "Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking," *Mathematical Problems in Engineering*, vol. 2021, 12 pages, 2021.