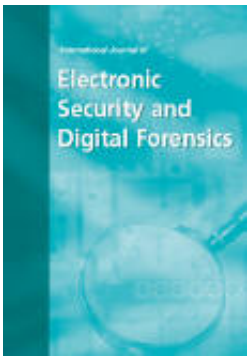


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

An original data encryption technique for communication networks

A. Rajasekar, A. Karunakaran, C. Sivakumaran, Sheshang Dipakkumar Degadwala

DOI: 10.1504/IJESDF.2024.10059345

Article History:
Received: 13 July 2022
Accepted: 27 October 2022
Published online: 12 January 2024

An original data encryption technique for communication networks

A. Rajasekar*

Department of Electronics and Communication Engineering,
Dhaanish Ahmed College of Engineering,
Chennai, India
Email: rajasekarbe@gmail.com
*Corresponding author

A. Karunakaran

Department of Electronics and Communication Engineering,
S.A. Engineering College,
Chennai, India
Email: karunakarana@saec.ac.in

C. Sivakumaran

Photon Technologies,
Chennai, India
Email: vlsiva@yahoo.co.in

Sheshang Dipakkumar Degadwala

Department of Computer and Science Engineering,
Sigma Institute of Engineering,
Vadodara, Gujarat, India
Email: sheshang13@gmail.com

Abstract: A novel secure distribution technique of network communication data is developed based on data encryption algorithm to address the issues of poor transfer effectiveness and high transmission bit error rate in previous transmission methods. In order to design the cipher text protocol, the access to network communication data is controlled by the agentless key publishing protocol. According to the experimental simulation findings in this work, the SM2 method (Supermemo2) can produce a 256-bit key very rapidly. The research's findings indicate that using link cryptographic algorithms in network communication security can increase security by 25%. The original deep learning chaotic encryption algorithm's performance flaw is optimised in this research. For wireless communication security, a chaotic neural network approach with dynamic keys is suggested. The experimental findings demonstrate that the technique suggested in this study significantly improves the speed of encryption and decryption as well as the key's capacity to resist decoding.

Keywords: neural network; key cryptographic technique; expected release terminal; communication systems; bilinear map-based method; key creation; encryption/decryption algorithms.

Reference to this paper should be made as follows: Rajasekar, A., Karunakaran, A., Sivakumaran, C. and Degadwala, S.D. (2024) 'An original data encryption technique for communication networks', *Int. J. Electronic Security and Digital Forensics*, Vol. 16, No. 1, pp.73–83.

Biographical notes: A. Rajasekar is currently working as an Associate Professor in Dhaanish Ahmed College of Engineering, Chennai. He has completed his Bachelor of Engineering degree in Electronics and Communication Engineering from Anna University, Chennai. He has completed his Master of Technology in Embedded System Technologies from SRM University, Chennai. He has completed his PhD course in Hindustan Institute of Technology and Science, Chennai and indulged in research work in the field of cypher physical systems. His field of interest in the domain of embedded systems, communication networks and internet of things. He has overall teaching experience of over 12 years in the affiliated college under Anna University. He has published over 15 research articles in refereed international and national journals in the areas like control systems, embedded systems, computer networks and internet of things, etc.

A. Karunakaran is currently working as an Assistant Professor at the Department of Electronics and Communication Engineering, S.A. Engineering College, Chennai. He obtained his Bachelor's in Electronics and Communication Engineering from the Government College of Engineering, Salem. He completed his Master's in Communication Systems from Sri SIvasubramaniya Nadar College of Engineering, Chennai. He is currently pursuing his part-time research at Anna University in Antenna and Microwave Design.

C. Sivakumaran is working as a Machine Learning Engineer in Chennai. He has received his Bachelor's in Electrical and Electronics Engineering from Sri Padmavathi College of Engineering, Madras University, in 2003 and Master's degree from SRM University, Chennai.

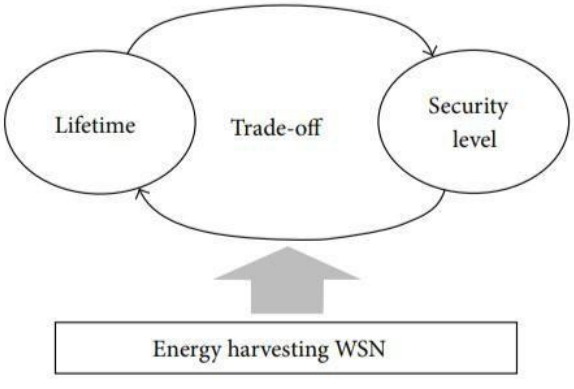
Sheshang Dipakkumar Degadwala is currently working as an Associate Professor and the Head of Computer Engineering Department, Sigma Institute of Engineering, Vadodara. He obtained his BE degree from the Department of Computer Engineering, BITs, Vadodara. Subsequently, he obtained his MTech degree from Charusat University, Changa and completed his PhD in Computer Engineering from Madhav University, Abu Road, Sirohi, Rajasthan, India in 2018. He has published 179 research papers in reputed international journals and conferences including IEEE, Elsevier and Springer. His main research work focuses on image processing, computer vision, information security, theory of computation and data mining. He is also a Microsoft Certified in Python Programming and Excel. He has published 18 books and he got grant for one patent. He has published 38 Indian Patent. He has received 45 awards for academic and research achievement.

1 Introduction

People exchange their own information via an updated project terminal network in the big data age. In the cloud, there is a lot of heterogeneous data stored. For local usage, users download data from the cloud (Yap et al., 2015). Hackers may readily get vital information that required them to overcome several firewall barriers in the past, posing a serious security risk to internetwork data in open environments. Lai (2016). One of the hot concerns in the age of big data is how to guarantee the security of terminal network connection data while maximising data value (Liu et al., 2018). Network security issues (host assaults, etc.) continue to arise as network communication technologies and the internet grow more and more interconnected. Retransmission will seriously jeopardise the further development of network applications. Here, a code that is kept secret it generates (Alhmiedat and Samara, 2017).

Considering that the TCP/IP model's backup layer contains matching encryption techniques and technologies. This article focuses on session application layer data encryption (Shokair et al., 2018). Data encryption technology has the ability to provide system security performance, digital certificates, secret storage, and information secrecy (Yan and Hou, 2017). As a result, the information's secrecy, integrity, and verifiability may be assured, but it also has the potential to be altered or fabricated. In this paper, Kim et al. (2015), offer an energy-aware security level control system (ESCS), which is an expanded version of their earlier paper. Figure 1 illustrates how it works to boost security in WSNs by only consuming extra energy at each energy collecting node.

Figure 1 Correlation of trade-offs between both the life and level of security in WSN



This suggests that there is no longer a need to make a trade-off between the longevity of the WSN and the level of security as a result of the fact that the proposed system only uses extra energy. A node that exceeds a particular threshold for battery power will encrypt the data using a public-key-based cryptography. The amount of energy that may be harvested at a certain point on the surface of the Earth obviously changes with the time of day, latitude, and weather conditions, and the effectiveness of translation is influenced by the angle of inclination to the PV device. Towards the equator, surface energy received on an annual average ranges from about 300 W/m^2 to about 100 W/m^2 near the poles. The daily average shortwave energy available in temperate areas ranges from

around 25 MJ m^2 day^{-1} in the summer to about 3 MJ m^2 day^{-1} in the middle of winter (Kim et al., 2015).

It is clear that customers at home and in small businesses are already comfortable with a basic solution without the sophisticated sophistication of a complete Enterprise RADIUS server, but they would undoubtedly gain from increased security if the technology were equally user-friendly. Two such characteristics that provide flexibility but have nothing to do with encryption are the idea of numerous user accounts and the ability to handle client certificates for authentication. The most significant advantage, in our opinion, is the usage of per-session keys to avoid listening in. The second most significant advantage is AP authentication, which makes sure a communication is being made to a legitimate network and not a fake one.

2 Literature survey

'Mutual starting to learn in tree parity machines' uses the cuckoo search algorithm. The well before key, which has been shown to be a weak point in wireless encryption, is eliminated by this suggestion. The authors' method is also built on the tamper-evident pairing (TEP) procedure, which offers security against MITM attacks by allowing any intervention in the exchange to be recognised. TEP provides a straightforward solution for residential users and is compatible with older 802.11 and low-power devices. Although technical expertise is not necessary for consumers to employ this approach, users still need to 'push the button in each device' attacks.

Gupta et al. (2018) explains that due to the nature of the noise floor, which is dependent on the energy level of the medium, this method also necessitates its recognition and calibration. The authors assessed their suggestion and came to the conclusion that it is practical in the actual world and probably provides defence against MITM assaults (Gupta et al., 2018). The neural network chaotic encryption technique, according to Chen et al. (2018), primarily makes use of mixing's fundamental properties, which include significant sensitivity to parameters and starting values. Early communication encryption used a chaotic encryption technique that primarily consists of four types: chaotic keying, chaotic enlargement, chaotic parameter manipulation, and chaotic hiding.

Smartphone application for encrypted communication of medical photos based on the complex number and the unique inclusion in Its encryption effectiveness is low and its encryption speed is slowed down. A discrete-time continuous valued cryptosystem that Gotz suggested has worse password deciphering capabilities but superior output distribution features. Therefore, research into a superior neural network chaotic encryption method is crucial and important for communication security, particularly wireless network connection safety.

In Liu and Ning (2008), the key advantage, in this author's opinion, is that intermediate nodes has to be conveyed to a sink node may send it without encryption. Most symmetric-key algorithms use less energy than public-key techniques, which are often CPU-intensive. However, they provide a better level of data dependability since it is very hard for malicious software or hackers to decrypt data that has been encrypted using a public-key technique, and there is practically no chance that the key would leak out. Due to the larger size of the encrypted data, the energy required for data transmitting is also slightly higher than with the symmetric-key method; however, because the signals

transmit the data without re-encrypting it. Our method employs an elliptic curve combined encryption scheme as the public-key algorithm (ECIES).

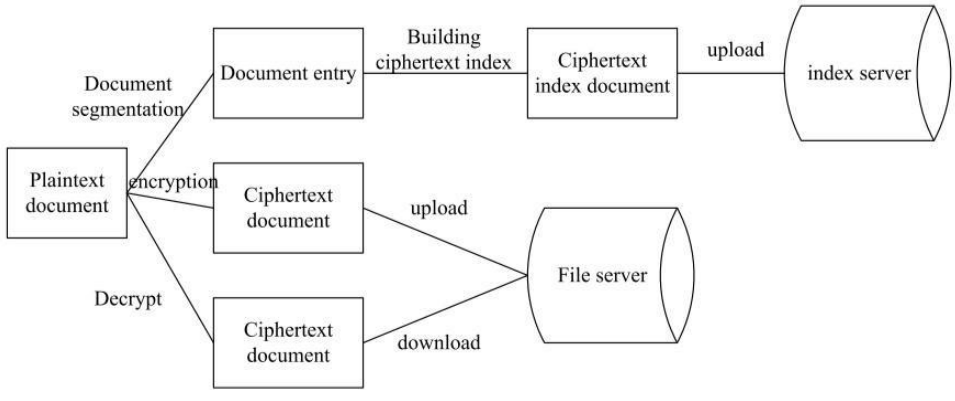
Each sensor node recognises events, processes data, and sends data. Monitoring, data analysis, and transmission are the three components that make up energy usage. In the literature, Li et al. (2017a) provide a detailed explanation of how symmetric encryption is performed using a CPU. On CPUs from the preceding generation, AFS is implemented via OpenGL.

The flow with fixed function is utilised as a result of the programming model's restrictions, which include those related to performance enhancement and hardware programmability. The hardware is utilised to finish the XOR operation during the output collecting stage. Multiple pipelining is required for a whole AFS execution, which significantly reduces efficiency. A selection of information files with sizes of 1,000 kB, 2,000 kB, and 4,000 kB is made by Yang et al. (2016). There are four parallel processors configured. Plaintext of various sizes is encrypted. The suggested method, the research algorithm, and the research algorithm are contrasted in terms of their parallel accelerating ratios and encryption times.

3 Methodology

Figure 2 shows the information release terminal's network information exchange along with other specifics. The user of the approved terminal can get the release authorisation following the server's and the updated project terminal's successful authentication protocols. The content release terminal creates the matching encryption key displayed in Figure 2 when the user distributes information.

Figure 2 The data release module's connectivity procedure



The outcome will be stored to the interface and used as the key reference for the currently uploaded file. The retrieved cypher text record and key index are then posted to the server in the required manner once the release information has been encrypted using the obtained encryption key. When the information is made available, segmentation processing is done on the plaintext data in order to make future retrieval easier, and the entry is created. The cipher-text indexing is then created using the entry, and it is submitted to the indexing server.

3.1 Plain text document (network communication)

Each block of the source release material data file is encrypted using a key matrix during transmission. The messages are encrypted using the Hill encryption technique after splitting the key matrix and plaintext matrix. The plaintext is deciphered using the Hill decryption approach after receiving the encrypted message and key matrix. The suggested method provides great security and efficiency, according to experimental findings. Each block of the source release informational data file is encrypted using a key matrix during transmission. The messages are encrypted using the Hill encryption technique after splitting the key matrix and plaintext matrix. The plaintext is deciphered using the Hill decryption approach after receiving the encrypted message and key matrix. The suggested method provides great security and efficiency, according to experimental findings.

3.2 Document entry

The progress report terminal creates a matching encryption key when the user provides information. The outcome will be stored to the terminal and used as the key index for the currently uploaded file. The retrieved decryption document and key index are then posted to the server in the required manner once the release information has been encrypted using the discovered encryption key. When the information is made available, segmentation processing is done on the plaintext data in order to make future retrieval easier, and the entry is created. The ciphertext indexing is then created using the entry, and it is submitted to the indexing host.

3.3 Cipher text

Hill encryption may be performed in parallel after segmentation using the block matrix multiplication. The messages are encrypted using the Hill encryption technique after the text grid and key matrix have been segmented. Equation (1) below provides the encryption algorithm.

$$D = QB \bmod m \tag{1}$$

that is, the outcome of the plaintext matrix and the key matrix. To get the ciphertext matrix D, the modular method is applied to each element of the set m. The following is a block matrix multiplication strategy. The block is subjected to matrix multiplication, the blocks are added together, and the final encryption block D + ij may be discovered. A ciphertext matrix is created by combining ciphertext blocks. Consider that the key matrix B is divided between k rows and n columns, whereas the plaintext matrices Q is divided between m rows and k columns.

3.4 File server

The communication procedure segments the parent released information data file into chunks. To guarantee that the transmission encryption process is carried out in parallel, each block is separately encrypted using a key matrix. Assume that the plaintext matrix has a size of M N and an order of N for the key matrix. The plaintext matrix reads the ASC II code from the transmission data file that has to be encrypted and stores it in a 1d

matrix. When there are more elements contained in a matrix than there is space in the connection data file, the empty space is filled with 0. Additionally, the time cost of the method and the algorithm described in Shokair et al. (2018) grows geometrically as the file size increases, but the time cost of the suggested technique increases gradually as the file size increases. In terms of encryption time, this method clearly has an edge over competing techniques.

3.5 Index server (uploading)

The mobile device can stay in doze mode when it is not necessary for it to read the broadcasted data thanks to the indexing on wireless broadcasting data stream. Without the index, the whole transmitted data must be read from the moment a data access transaction occurs until all necessary data have been retrieved in full. However, the client merely reads a little bit of the broadcast stream while utilising the index to identify the correct address of the target domain. The client can stay in doze mode after getting the address, or the spatial offset from the indexing to the data, until the target data are given below, as illustrated in Figure 3 of the indexing tree with administrator.

Figure 3 A sample controller-equipped indexing tree

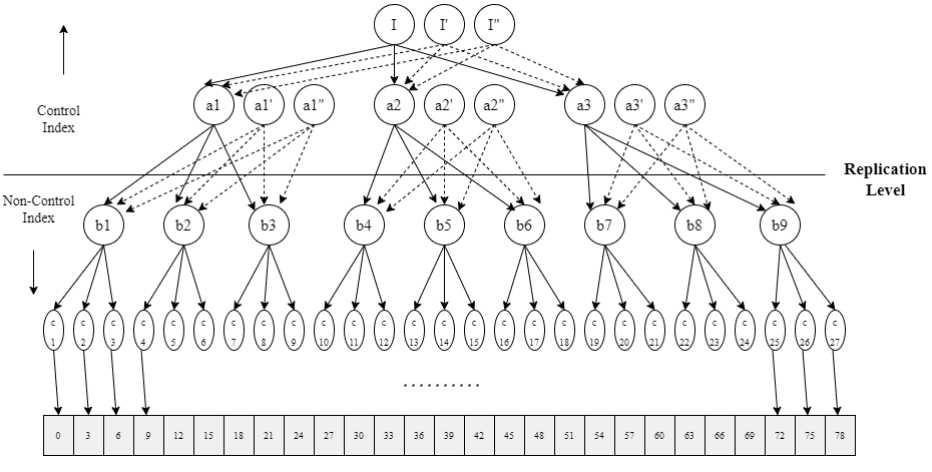
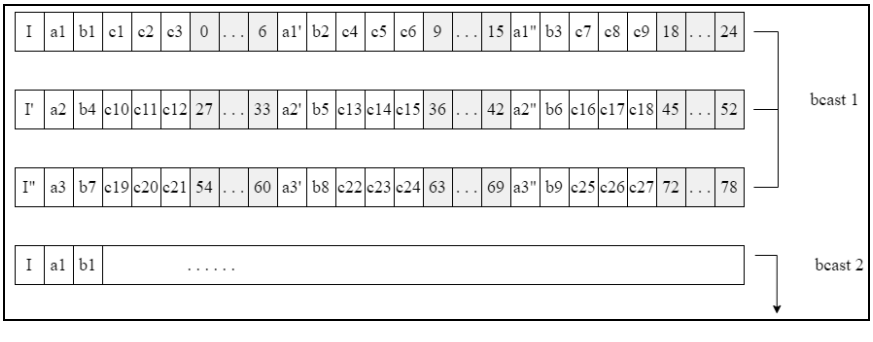


Figure 4 Transmission of data



The controlled indexing buckets are duplicated as many instances as the index tree's fan-out in the traditional index replication method, and the duplicated index buckets all contain the identical index data, as seen in Figure 4.

That is, a location in the indexing bucket serves as a time stamp for the delivery of the information (or indexing) to which the index values belong. The address of the content or indexing that has already gone over is therefore useless when duplicating an index bucket. We provide a novel index replication strategy that meets all the criteria in order to reduce bandwidth waste.

4 Result and discussion

Following encryption using the segmentation linear chaos technique, the picture's pixel value distribution is plainly homogenised, making it impossible to see any of the relevant information from the original image. The process is shown in Figure 5.

Figure 5 The encoded picture 'test.bmphistogram 's of grayscale distribution (see online version for colours)

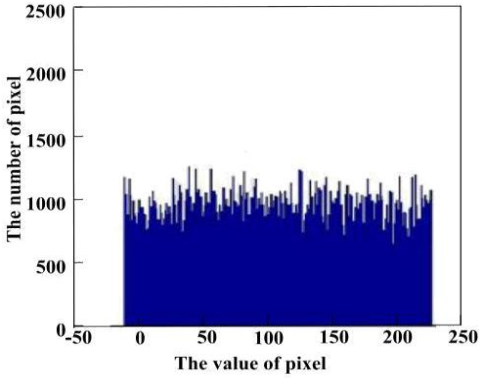


Figure 6 The most widely used and secure type of computation is algorithm encryption (see online version for colours)

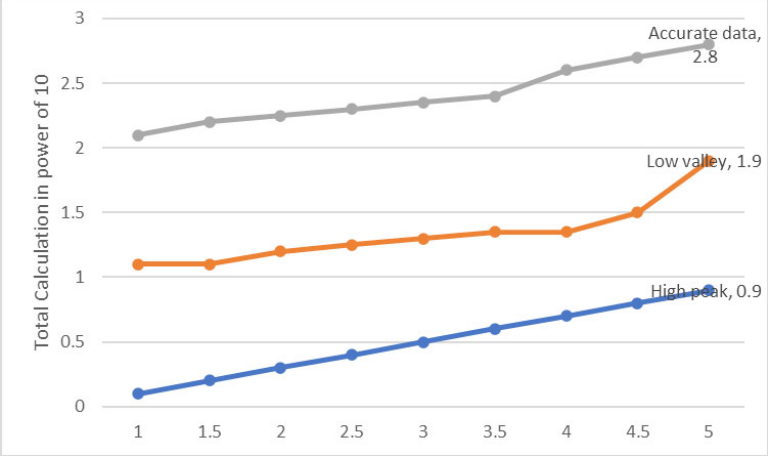
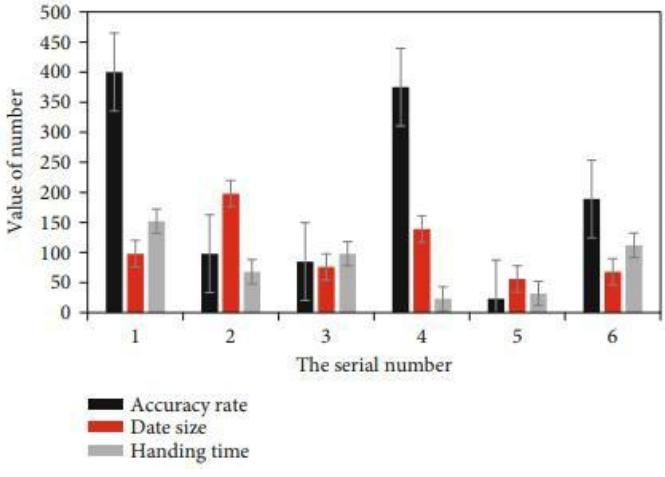


Figure 4's statistics demonstrate that employing computing connection security may boost data security strength of encrypting data algorithm technologies by 36%; the percentage of this technology used while building software is displayed in Figure 6.

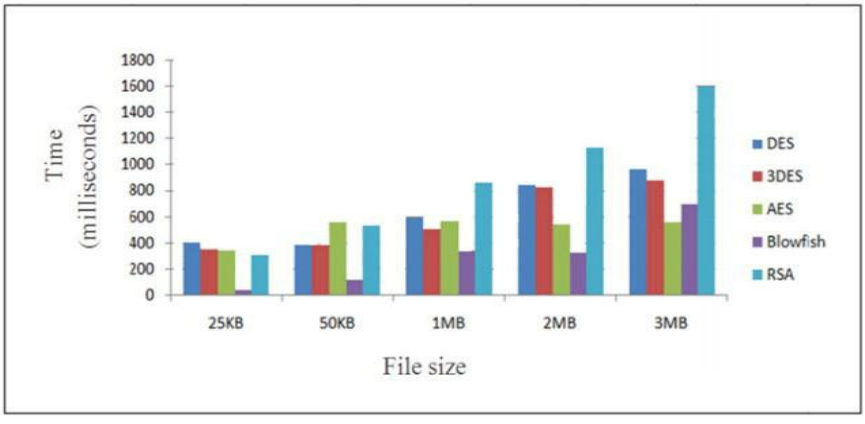
According to Figure 7, data encryption for computer network data transmission can stop 80% of hacker assaults, lower the chances of success of financial crime by 64%, and leaks of personal information about users by 25%.

Figure 7 The encrypting data algorithm technology's program protection level has significantly increased thanks to the use of secure computer network connection (see online version for colours)



The comparison of various data encryption algorithms are shown in Figure 8.

Figure 8 Data encryption techniques comparison (see online version for colours)



5 Conclusions

In this research, we offer an energy-aware threat management control method that, by effectively using the captured energy, boosts cryptography level and energy efficiency. As per their residual energy level, nodes are divided into ES-mode and ER-mode. Content is then sent using symmetric-key methods with high energy efficiency and low encryption levels as well as public-key methods with high costs and high compression levels. While the standard chaotic encryption technique has poor encryption effectiveness, the neural network chaotic cryptosystem offers several benefits for enhancing wireless communication security. This research provides a better optimisation method founded on an Aihara neural network and adds chaotic mapping and composite coding technology in light of the poor decoding capability and the avalanche effect performs several trials for a large user base while analysing the encryption security level of the computer network communication security machine. There are several encryption methods, referred to as link encrypted message, nodal encryption method, and end-to-end cryptosystem, from the standpoint of network data links. According to the study's findings, using link cryptographic techniques in network data transmission can boost security by 25%, using node cryptographic techniques can boost security by 35%, and using end-to-end encryption methods may boost network activity. We are looking at expanding the suggested index replication technique for multichannel environments as future work. The linkable candidates may be on other transmission channels when there are several channels for the delivery of data and there exist semantic linkages among the data objects among the channels. A different form of optimisation technique may be provided by executives using this knowledge.

References

Alhmiedat, T. and Samara, G. (2017) 'A low cost zigbee sensor network architecture for indoor air quality monitoring', *International Journal of Computer Science & Information Security*, Vol. 15, No. 1, pp.140–144.

Chen, C., Liu, L., Qiu, T., Ren, Z. et al. (2018) 'Driver's intention identification and risk evaluation at intersections in the internet of vehicles', *IEEE Trans. IoT*, Vol. 5, No. 3, pp.1575–1587.

Gupta, S., Nanda, N., Chhikara, N., Gupta, N. and Jain, S. (2018) 'Mutual learning in tree parity machines using cuckoo search algorithm for secure public key exchange', in *ICTACT Journal on Soft Computing*, April, Vol. 8, No. 3, http://ictactjournals.in/paper/IJSC_Vol_8_Iss_3_Paper_3_1663_1667.pdf.

Kim, J., Lee, H., Yi, J., Park, M. and Noh, D. (2015) 'Energy-aware data encryption for solar-powered wireless sensor networks', in *Proceedings of the IEEE Asia Pacific Wireless Communications Symposium (IEEE VTS APWCS '15)*, Singapore.

Lai, X. (2016) 'International data encryption algorithm', *Hepatology*, Vol. 60, No. 12, pp.2125–2126.

Li, C., Lin, D. and Lu, J. (2017a) 'Cryptanalyzing an image-scrambling encryption algorithm of pixel bits', *IEEE Multimedia*, Vol. 24, No. 23, pp.64–71.

Li, Y., Zhu, W. and Huang, C. (2017b) 'Research on power heterogeneous communications network stability with SOC', *Power System Protection & Control*, Vol. 45, No. 5, pp.118–122.

Liang, C., Zhang, Q. and Ma, J. (2019) 'Research on neural network chaotic encryption algorithm in wireless network security communication', *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1, p.151.

Liu, A. and Ning, P. (2008) 'TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks', in *Proceedings of the 7th IEEE International Conference on Information Processing in Sensor Networks (IPSN '08)*, St. Louis, Mo, USA, April, pp.245–256.

Liu, L., Hao, S., Lin, J. et al. (2018) 'Image block encryption algorithm based on chaotic maps', *IET Signal Processing*, Vol. 12, No. 13, pp.22–30.

Shokair, M., Saad, W. and Ibraheem, S.M. (2018) 'Statistical analysis of a class of secure relay assisted cognitive radio networks', *China Communications*, Vol. 15, No. 12, pp.174–189.

Yan, L-k. and Hou, Y-x. (2017) 'The optimization strategies and application of transmission network in power system', *Electric Power Information & Communication Technology*, Vol. 2017, No. 7, pp.107–112.

Yang, X., Shen, Z., Hu, X. et al. (2016) 'Chaotic encryption algorithm against chosen-plaintext attacks in optical of transmission', *IEEE Photonics Technology Letters*, Vol. 28, No. 2, pp.2499–2502.

Yap, W.S., Phan, C.W., Yau, W.C. et al. (2015) 'Cryptanalysis of a new image alternate encryption algorithm based on chaotic map', *Nonlinear Dynamics*, Vol. 80, No. 12, pp.1483–1491.