EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Lightweight Cryptographic Simulation of Power IoT Fused with Bayesian Network Algorithms

Xueqiong Zhu[1,*], Chengbo Hu[1], Yongling Lu[1], Zhen Wang[1] and Hai Xue[1]

[1]State Grid Jiangsu Electric Power Company Ltd. Research Institute, Jiangsu, China

Abstract

In the power system, the transmission and processing of information is a very important link, and the core part of it is electronic data, and the transmission and processing of electronic data is the most important link in the power system. Because information is continuously passed between network nodes, the security requirements for information are high. With the development of Internet technology, its application field has been widely expanded to various industries. Therefore, to better ensure power quality and improve network operation efficiency, it is necessary to rationally and effectively manage the entire communication system. Power Internet of Things technology combines information transmission and processing links and realizes data sharing between various communication nodes in the entire network system through intelligent management, thereby improving overall information security. This paper first introduces the research of Bayesian network algorithm, then studies the process of lightweight encryption implementation of power Internet of Things, and then simulates and compares various encryption algorithms to obtain the best encryption scheme, and finally verifies through simulation that the algorithm can effectively ensure the safe transmission of information and improve the efficiency of network operation.

Keywords: bayesian network algorithms, power internet of things, lightweight encryption emulation, iot, cryptographic

Received on 02 January 2023, accepted on 03 February 2023, published on 29 March 2023

doi: 10.4108/eetsis.v10i3.2970

1. Introduction

In today's booming Internet, various fields must be applied to network security, including communication protocols based on network chains and wireless devices, such as email, digital television networks, etc. [1]. The network chain protocol is one of them, which applies encryption technology on the Internet for information transmission. Encryption technology can ensure that information is not illegally stolen and tampered with and can also ensure that information is not leaked. In network communication protocols, the application of encryption ensures the secure transmission of data [2].

The power industry is an important core, and its development level greatly impacts the country's economy and social stability. As a basic industry of the national economy, the development level of the electric power industry is closely related to national security, so it is very necessary to carry out an effective, reasonable, scientific, and confidential design of the power sector. Therefore, effectively reducing data loss during system transmission, bit error rate, and other issues has become the key to reconstructing massive information resources and improving communication quality and reliability. The Bayesian network has the advantages of high efficiency, low Complexity, and robustness, which is a new direction in the field of intelligent information management [3].

The development of electronic technology makes the power system face different types and quantities of equipment in the operation process. This equipment is interconnected and restricted, which also reduces network information security. Therefore, it is necessary to encrypt

[*]Corresponding author. Email: zhuxueqiong187@163.com

the network information to strengthen information security. The traditional encryption method encrypts the secret key for various information, but this method still has many things that need to be improved. For example, key management and encryption technology are immature.

Contribution of the work

- This paper proposes encryption based on the Bayesian network algorithm of the traditional encryption method.
- The method can effectively compress and process data. At the same time, it can improve communication speed and reduce the number of nodes required in the network transmission process.
- The proposed method improves communication quality while realizing the high efficiency of network transmission.

2. Related Work

The importance of automated, interconnected devices is growing as time goes on, and to meet this demand, the Internet of Things (IoT) concept has been established, centering on the idea of smart devices. In order to achieve certain goals, such as automation and intelligent decision-making, IoT-enabled smart devices can exchange data with one another across a network. Users can now delegate household chores to sophisticated machines thanks to the Internet of Things since these gadgets monitor and adjust their behavior based on environmental factors. Sensors are used to gather data that is subsequently processed by a computational node, which intelligently regulates the actions of the machines. In recent years, IoT security has improved thanks to deep learning-based guessing attack defense methods. However, there remains to be a significant obstacle for IoT networks in complicated businesses. Significant training time for processing a huge dataset from the network's prior data flow is vital to such systems. Decision trees, logistic regression, and support vector machines are examples of classic deep-learning methods. The security flaws inherent to IoT networks mean that hackers can potentially gain access to the sensor/communication data and use it for nefarious ends.

Mohammad Kamrul Hasan et al. (2019) presents experimental research on cryptographic algorithms to categorize them into the asymmetric encryption algorithm and the symmetric encryption algorithm. It thoroughly compares the encryption algorithms AES, DES, 3DES, RSA, and Blowfish in terms of their time complexity, file size, and encryption and decryption speeds. The guessing attack in complicated real-time IoT applications that use deep learning has been evaluated. The simulation method was used to evaluate the encryption and decryption rates of the prioritized methods. The tests encrypt and decrypt the identical plaintext using the same algorithm five times and compare the average times. Each encryption method has a maximum allowable key size in bytes. The average time it takes for the three devices to calculate the algorithm is used for the comparison. Compared to the techniques employed in real-time deep learning networks for IoT applications, the simulated experimental test using a set of plaintexts (password-sized text and paragraph-sized text) reaches fair target results.

Data exchanged between IoT devices also expands at a rate proportional to the IoT's rapid expansion. Most IoT devices are low-power, battery-operated gadgets that work together to accomplish certain goals and exchange sensitive information through a shared network. With the advent of the IoT, even systems with limited power consumption can exchange data, process information, and make critical communication decisions. Protection, low-cost computer power use, limited battery capacity, memory space, high efficiency, and minimal communication network latency are some of the issues and challenges arising in tiered IoT networks. This study by Sunil Kumar et al. (2021) discusses in depth a state-of-the-art lightweight cryptographic algorithm, covering topics such as lightweight block ciphers, hash functions, stream ciphers, high-performance systems, low power-constrained devices, and IoT network tools. Key size, block size, round size. An algorithmic structure is used to rank lightweight cryptographic methods. We also delve into the power-restricted device of the IoT system's security structure, difficulties, and primary solutions.

Tiny, low-cost gadgets are constantly exchanging data with one another, serving as the platform's backbone in the IoT. Such gadgets' storage space, RAM, and CPU power are restricted. Standard cryptographic methods demand a big hardware footprint, driving up the price of devices. Hence most of the time, they need to be implemented. Two encryption methods, four authentication methods, and a key generation/exchange protocol are implemented in this paper by Gookyi et al. (2022) for use in ultra-low-cost devices using a System-on-Chip (SoC) architecture. The idea of shared resources is used in hardware architectures to reduce the required physical footprint. Building a desktop app to bridge the cryptographic SoC and the tester hardware is a great way to verify the SoC's performance. They use Verilog HDL for implementation and synthesis with the 130 nm CMOS cell library that yields 33 k gate equivalents at a maximum clock frequency of 50 MHz. Thanks to advancements in digital technology, the globe became instantly interconnected. The Internet must reliably transport the vast quantities of digital data generated daily by billions of intelligent gadgets. When considering an embedded setting, the impossibility of storing and processing a large amount of data using a device with limited resources drives the development of the lightweight idea.

Many symmetric keys are used in sequence inside the lightweight model provided by Runa Chatterjee et al. (2019). A 64-bit input block is split into two 32-bit blocks in this topology, which is typical of a Feistel network. Once separated, each half is subjected to several symmetric key techniques, including TE (Triangular Encryption), RPPT (Recursive Pared Parity Technique), RPSPNC (Recursive Positional Substitution on Prime-Nonprime of Cluster), TB (Transformation of Bits), and bits rotation. Different encryption and decryption methods have been developed from TE's original triangular bit sequence. Bits are encrypted using logical OR in RPPT. TB encrypts and decrypts data via a method called bit-swapping. In RPSPNC, the position of a bit is compared to the position of a prime number, and any sequence of bits in between is treated as cipher text. The final step combines the two resulting sub-blocks into a 64-bit cipher text. The suggested model is validated via comparisons to two other well-known algorithms (the symmetric key method AES and the embedded algorithm RPPT+TB). Entropy, n-gram(4-gram), non-homogeneity, and histogram are only some of the software factors that get analyzed. By comparing the model's GE (Gate equivalent) to the 1000-2000GE range defined by the ISO / IEC standard, we can be confident that the model is lightweight.

Wireless communication networks have allowed the Internet of Things (IoT) to stealthily and gradually establish a foothold in our daily lives. Smart meters, healthcare monitoring, transportation and packing, and asset tracking are just a few examples of the many M2M applications that contribute to the rise of connected devices. IoT creates new challenges inside an enormous and unpredictable environment. Among the most pressing of these issues are ones of security and confidentiality. RFID tags, sensors, and contactless smart cards are a few examples of compact, low-energy, and small-footprint devices that can benefit from lightweight cryptography. This means it can be implemented in IoT applications to safeguard personal data. Bora Aslan et al. (2020) conducted an experimental study to compare the efficacy of several lightweight cryptographic algorithms for protecting data in the Internet of Things (IoT) applications. These algorithms included PRESENT, CLEFIA, PICCOLO, PRINCE, and LBLOCK. Test results were analyzed to draw conclusions about algorithmic energy usage, current measurement, active mode working time, and active mode energy consumption.

3. Research on Bayesian Network Algorithms

3.1. Bayesian network algorithm

The Bayesian network is a stochastic system of probability density distribution consisting of Bayes' theorem and related functions. Due to a large amount of data, and complex and diverse structure, there are differences between sample points. Therefore, we have established a minimum problem suitable for statistical models to calculate the average dispersion time to simulate, analyse and derive predictions [4]. This method can effectively reduce the error loss caused by human reasons and reduce energy consumption, and obtain the optimal solution after optimization of the system parameters, so that the entire algorithm has more rationality and practical value, and it also provides a new idea for data analysis, that is, through the optimization of parameters, the discrete-time is minimized to get the closest optimal solution [5]. The principle based on the resulting Bayesian network algorithm is shown in Figure 1.

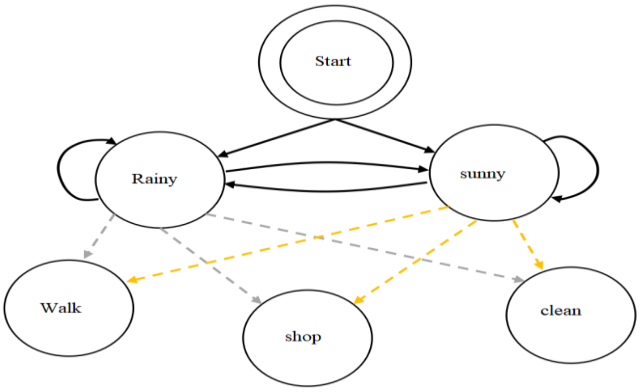


Figure 1. Bayesian network algorithm

The Bayesian network can achieve effective separation by optimizing unknown parameters according to the set of known nodes. Each node is attached to a probability distribution, where the root node X is attached to its marginal probability P(X), while the non-root node X is attached to the conditional probability distribution P(X|pa(X)).

Probability representation

The probability representation method is mainly based on statistical theory, and its main principle lies in the law obtained by analyzing a large number of random sequences without any relevant data. On the whole, a Bayesian network is a graphical representation of the joint probability decomposition of all variables in the network, which is formed by the probability distribution relationship between two random variables [6]. The probabilistic representation in a Bayesian network can be shown in Figure 2.

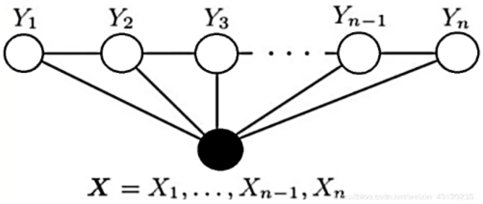


Figure 2 Probabilistic representation in Bayesian network

For a certain node X1, X2,..., Xn, multiply their probability distributions to obtain a joint distribution, and the network parameters corresponding to the nodes are shown in the formula (1).

$$\theta_{ijk} = P(X_i = k \mid pa(X_i) = j) \tag{1}$$

In formula (1), when $pa(X_i) = \phi$ P(Xi|pa(Xi)) is the marginal probability P(Xi). In formula (2) i=1,2....n; j=1,2,....qi; k=1,2,...,ri.

Conditional independence

If the connection between two nodes is independent, an algorithm can simulate natural language transmission over the network and functional relationships under certain conditions [7]. However, this method does not rely on other forms existing in the real world with the same characteristics or high degree of functional similarity, so it can only be applied to the actual structure and cannot be experimentally verified. The amount of data on the network is very large, the transmission speed requirements are high, and the communication performance is unstable, which cannot be applied to practical applications. When the node and the connection mode are independent, the node does not depend on the transmission of the network, and in practice, it cannot be achieved due to certain constraints of the communication protocol. An important feature of Bayesian networks: the structure of the network contains conditional independence. Given the parent node of the variable Xi, pa(Xi), the Xi condition is independent of nd(X), i.e., the formula (2) can be obtained.

$$P(X_i nd(X_i) \mid pa(X_i)) = P(X_i \mid pa(X_i)) \qquad (2)$$

Probability theory of Bayesian networks

The probability theory of Bayesian networks was developed based on classical theory, and its main research is based on data mining algorithms and decision tree classifiers. Decision tree classification is a random forest algorithm based on decision trees, which uses the knowledge of probability theory used in data mining as a classifier, which divides patterns by randomly selecting and constructing Bayes' formulas. A data mining algorithm is a probability theory method based on statistics, which realizes the classification of patterns by manually selecting and constructing specific data types. More basic knowledge of probability theory is involved in the inference calculation of the Bayesian network [8].

(1) Prior probability. The so-called a priori probability means some closeness between the inferred result and the expected value without experimental verification or experimental verification. This difference will be called prediction error.

(2) Posterior probability. Posterior probability refers to the use of Bayes' formula. First, find the response spectrum of the node in a random space. It is then predicted according to the internal structure of the system.

(3) Conditional probability. Conditional probability refers to the probability calculated under certain prerequisites, which a formula can express, and probability is the average of a random variable, which reflects the size of the impact of an event after it occurs. Suppose there are two random events A and B, p(B) >0, and the probability of A occurring under the premise of event B is recorded as P(A| B), and the calculation of the conditional generalization that calls this probability the occurrence of event A is shown in formula (3):

(4)

$$P(A \mid B) = \frac{p(AB)}{p(B)} \qquad (3)$$

(5) Joint probability. Joint probability, also known as the multiplicative formula, refers to the product of the probabilities of two or more events, with two random events A and B, the joint probability representation is shown in formula (4):

$$P(AB) = p(A)p(B \mid A) or p(AB) = p(Bp(A \mid B)) \qquad (4)$$

(6) Chain rules. Chain rules are mainly used in the case of many event variables to give the propagation speed of an event on the network, that is, the probability of chain forwarding between nodes and all nodes, and calculate the number of iterations corresponding to other time values at this time point. Express the joint probability distribution as a chain of conditional probability distributions. With random variables V1, V2,..., Vk, formula (5) can be obtained:

(7)

$$p(V_1, V_2, \cdots, V_k) = \prod_i^k p(V_i \mid V_{i-1}, \cdots, V_1) \qquad (5)$$

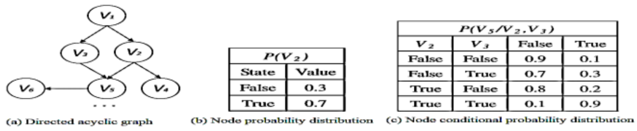
(8) Bayesian formula. The Bayesian formula is a commonly used random signal processing method that can describe correlations between data and determine different types of relationships in a network and is widely used in network algorithms for distributed tree structures based on nodes or assumptions (Bayesian formula). This method can effectively solve the traditional simulated encryption process and has been widely used in many fields. There are random variables B1, B2,.... Bk is an incompatible complete set of events for event E. If p(B) >0 is satisfied, and A is an arbitrary event of event E, then its Bayesian posterior probability representation is shown in formula (6):

$$p(B_i \mid A) = \frac{p(B_i)p(A \mid B_i)}{\sum_{i=1}^{k} p(B_i)p(A \mid B_i)} \qquad (6)$$

Structure and establishment method of Bayesian network

The Bayesian network is a directed acyclic graph with a probabilistic conditional constraint in a huge probability center. There can be an infinite number of iterations or more between nodes throughout the network. The Bayesian algorithm is a method of rules-based reasoning that simplifies and intuitively presents problems and is suitable for various types of complex systems or structural models with a certain degree of Complexity and requirements. At the same time, it can also evaluate the advantages and disadvantages of the data and the probability of future events by calculating the mining ability of the data's results to provide a reliable basis for decision-makers [9].

For a set of random variables V={V,V,.. V,}, whose Bayesian network contains a Bayesian network structure and a set of local probability distributions associated with each variable, as shown in Figure 3.



(a) Directed acyclic graph

P(V₂)	
State	Value
False	0.3
True	0.7

(b) Node probability distribution

P(V₅/V₂,V₃)			
V₂	V₃	False	True
False	False	0.9	0.1
False	True	0.7	0.3
True	False	0.8	0.2
True	True	0.1	0.9

(c) Node conditional probability distribution

Figure 3 Directed acyclic plot and probability distribution table of Bayesian networks

Together, these two parts define the probability distribution of this set of variables V, give some important conclusions, and iteratively calculate the nodes' vicinity in discrete time to obtain its probability density function [10]. The joint probability of the random variable V can be expressed as shown in formula (7):

$$p(v) = \prod_{i=1}^{n} p(v_i \mid pav_i) \tag{7}$$

The construction of the Bayesian network model is the first step in the implementation of system fault diagnosis, and its core part is the Bayesian network algorithm, which can effectively help us diagnose the security vulnerabilities in the system and propose corresponding strategies for how to deal with the failure after the failure occurs. First of all, it is necessary to obtain a large amount of fault knowledge information for the diagnostic object, select the appropriate data set, process and analyze the information to establish a Bayesian network model, and then establish a causal relationship between each node according to the relationship between the fault phenomenon and the cause of the failure, and calculate the reconstruction relationship between the nodes in the network according to the reasoned probability formula, and finally determine the local probability distribution for the relevant nodes, and calculate the global probability distribution, to obtain the local reconstruction in the network [11]. The steps to establish a Bayesian network model are shown in Figure 4 below.

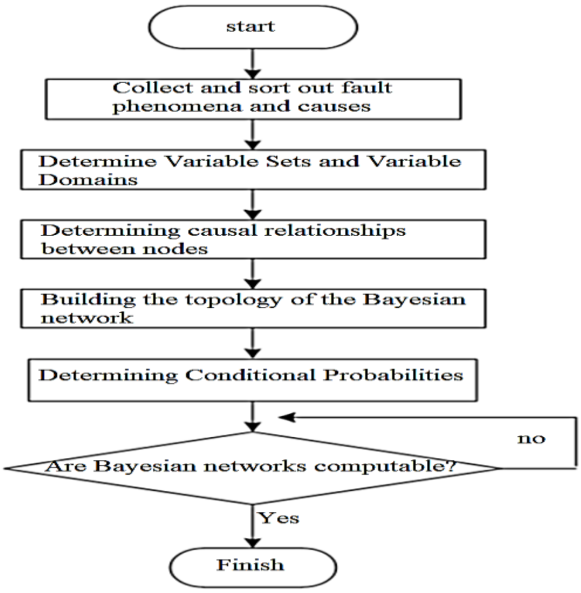

start
Collect and sort out fault phenomena and causes
Determine Variable Sets and Variable Domains
Determining causal relationships between nodes
Building the topology of the Bayesian network
Determining Conditional Probabilities
Are Bayesian networks computable?
no
Yes
Finish

Figure 4 Steps to build a Bayesian network model

3.2 Lightweight encryption implementación of power Internet of Things based on Bayesian network algorithm

Data encryption

Encryption of sensitive data (RC6 and Feistel). During data storage and transmission, sensitive information may be maliciously tampered with or damaged, resulting in unpredictable losses. Therefore, encryption technology is a method to effectively improve key security and ensure both communication parties' safe and reliable operation. Because the encryption algorithm can recheck the original ciphertext, which avoids the need to use a lot of repetitive code to verify file integrity and other operations when cracking traditional passwords, and it also has scalability and easy to implement the function of storing information during data transmission, it can solve some confidentiality problems to a certain extent, such as the efficiency and reliability of encryption algorithms, and improve key security [12].

Non-sensitive data encryption (SM4)

Non-sensitive data encryption technology is proposed based on the need of information security. It is related to sensitivity in some aspects. For example, important files, data streams, etc. are stored in the network, and these data security requirements are relatively high. Therefore, encrypting non-sensitive information is the most important to ensure network security performance and effectiveness. In order to improve confidentiality performance and protect confidential content from being leaked or stolen, the commonly used encryption algorithm is the SM4 algorithm. The SM4 algorithm is based on data encryption, which can effectively prevent the leakage of sensitive information and improve the performance of confidentiality. In the encryption and decryption process, the key is the same, the data packet and key length of plaintext and ciphertext are both 128 bits [13]. Therefore, the encryption algorithm is an effective method for protecting communication security performance [14]. The structure diagram of the SM4 algorithm is shown in Figure 5.

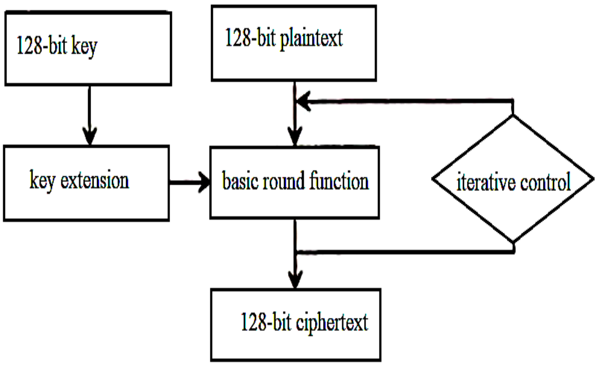


Figure 5 SM4 algorithm structure diagram

Multi-level authentication

Identity verification refers to identifying authorized users and using identity authentication technology to determine whether the trusted object is owned by me to ensure the legitimate rights and interests of authorized users. This is a common and commonly used identity authentication technology. The research object is based on the Bayesian network algorithm (RBF) and the node encryption technology in cryptography as the main content and combined with the communication protocol to verify the system key management and realize data transmission. The process is as follows: First, in the user registration stage, the user registers the credentials with the trust organization and then verifies whether the user's identity and password are valid; if they exist, it is proved to be legal authorization. Otherwise, the data transmission is rejected. Second, users must provide their ID/password to the trusted authority. The trusted authority receives the user's credentials and registers the user as a storage object for the data. Finally, users can select the corresponding identity on different nodes according to their own needs, record it as the corresponding key, and verify whether the system is legal through data analysis algorithms [15-20]. The specific process is shown in Figure 6.

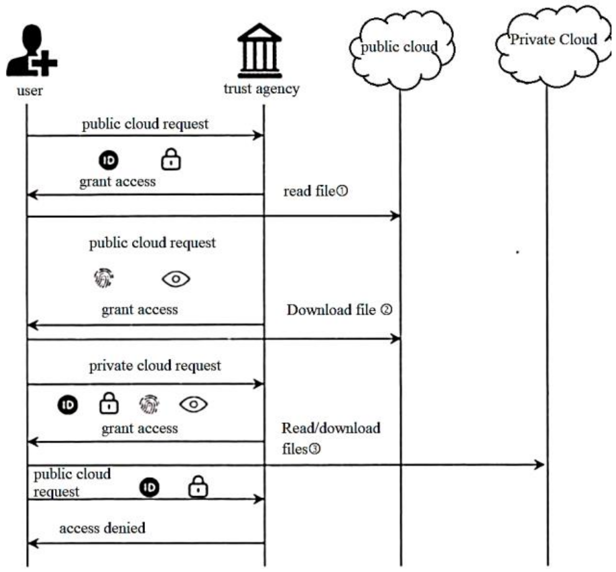


Figure 6 Multi-level authentication process

4 Simulation Results And Discussion

In Internet-based security technology, how to use the knowledge of cryptography to solve the encryption problem is a topic that researchers will focus on and focus on in the future. In addition, the simulation environment is the simulator in the Ubuntu operating system. By simulating the characteristics of the object, we can find that the system can use its special performance to solve the encryption problem at runtime [20-29]. The simulation parameters of the simulator are set as shown in Table 1.

Table 1. Simulation parameter settings

Parameter	Settings
Simulation area	1100mx1100m
User number	60
Number of Power IoT Devices	60
Number of trusted institutions	2
Number of cloud servers	3
Number of gateways	3

As shown in Figure 7, the comparison of security strength is described, mainly including the comparison of encryption algorithms such as Proposed, FCS, and MCP-ABE.

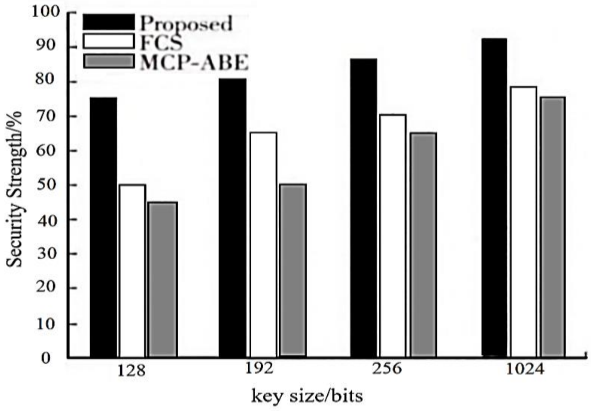


Figure 7 Comparison of security strength

Figure 8 compares encryption time and key size between different encryption algorithms. The comparison results show that the proposed encryption scheme has a shorter time [17,18].

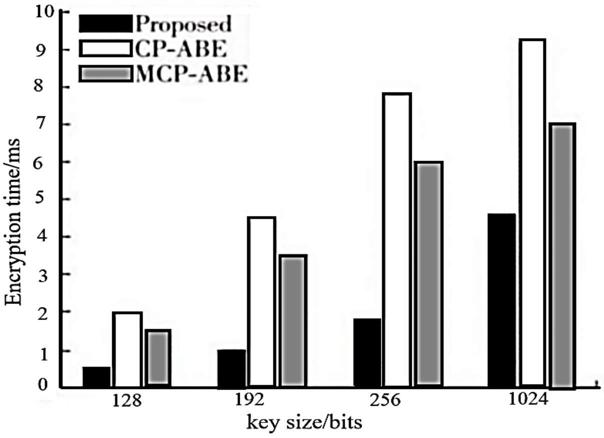


Figure 8 Comparison based on encryption time and key size

Figure 9 shows that the proposed method achieves less decryption time than CP-ABE and MCP-ABE, as follows:

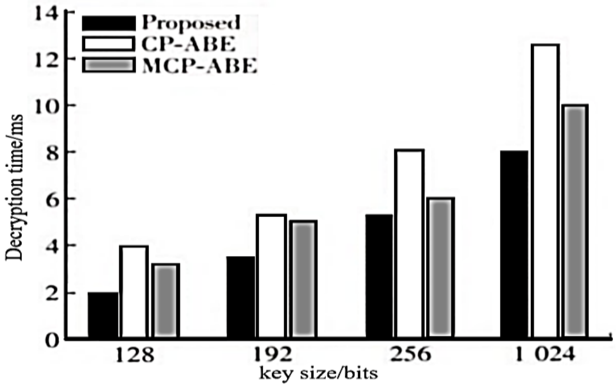


Figure 9 Comparison with key size based on decryption time

5 Conclusion

To sum up, with the rapid development of the Internet today, the most widely used, common, and efficient way of information transmission is digital data, and the security of information transmission has also attracted more and more users' attention and attention. Therefore, improving the application of data encryption algorithms has become an important issue. The continuous growth of communication services has led to the emergence of massive amounts of data. In order to ensure the security of network transmission, we need to encrypt data. This paper mainly combines the Bayesian algorithm to study the lightweight encryption algorithm of the power Internet of things and takes the algorithm as an example to verify it by simulation. It is concluded that the data encryption efficiency of the algorithm is higher, and it can also effectively ensure the security of information communication in the transmission of power Internet of things, which is of great significance.

Acknowledgements.

State Grid of science and technology project, "Development and application of low-power wide-narrow fusion wireless sensor network system integrated with electrical power sensing device," NO. 5500-202158416A- 0-0-00.

References

[1] Guoliang LI,Lining XING,Zhongshan ZHANG,Yingwu CHEN. "A New Bayesian Network Structure Learning Algorithm Mechanism Based on the Decomposability of Scoring Functions[J]." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,2017(7):14-17

[2] Suzhen Li. "Bayesian network algorithms used in the assessment of learners' learning behaviour[J]." International Journal of Continuing Engineering Education and Life-Long Learning,2021(3):31-33

[3] Diego Oliva,Marcella S.R. Martins,Valentín Osuna-Enciso,et al. "Combining information from thresholding techniques through an evolutionary Bayesian network algorithm[J]." Applied Soft Computing Journal,2020(3):90-93

[4] Mortazavi Amin,Rashidi Amir,Ghaderi-Zefrehei Mostafa,et al. "WITHDRAWN:Identification of bovine uterine transcriptomic hub genes using Bayesian network algorithms.[J]. "Asian-Australasian journal of animal sciences,2019:21-25

[5] Wang Chuanlong,Jin Yahong,Zhang Ruiting,et al. "Tunable ultraviolet-B full-spectrum delayed luminescence of bismuth-activated phosphors for high-secure data encryption and decryption[J]." Journal of Alloys and Compounds,2022:902-904

[6] Wu Lizhi,Guan Jinlan. "Application of Data Encryption Technology in Computer Network Security[J]." International Journal of Computational and Engineering,2021(1):6-11

[7] Lanlan Yin,Feng Mo,Qiming Wu,et al. "Research on Application of Data Encryption in Computer Network Security[C]//."Proceedings of the 11th International

Conference on Computer Engineering and Networks(CENet2021)Part I.,2021:706-713

[8] Srivastava, Gautam,Kumar, et al."Two-stage data encryption using chaotic neural networks[J]."JOURNAL OF INTELLIGENT & FUZZY SYSTEMS,2020:2561-2568

[9] Gonzalez-Gil, Pedro,Antonio Martinez, et al."Lightweight Data-Security Ontology for IoT[J]."SENSORS,2020:24-27

[10] Tu T. Vo,Ngoc T. Luong,Doan Hoang. "MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network[J]." Wireless Networks,2019(7):25-27

[11] Adwan Yasin,Abdelmunem Abuhasan. "Enhancing anti-phishing by a robust multi-level authentication technique (EARMAT).[J]." Int. Arab J. Inf. Technol.,2018(6):15-16

[12] Guo Huiping,Li Hongru. "An efficient Bayesian network structure learning algorithm using the strategy of two-stage searches[J]." Intelligent Data Analysis,2020(5):24

[13] D. Jerusha,T. Jaya. "Cryptographic Lightweight Encryption Algorithm with Dimensionality Reduction in Edge Computing[J]." COMPUTER SYSTEMS SCIENCE AND ENGINEERING,2022(3):42-44

[14] Tanh Nguyen Van,Tri Ngo Quang,Giang Nguyen Linh,Duy Tien-Le. "A Solution to Improve the Security of the Internet of Things Network with Lightweight Encryption Methods[J]." Journal of Physics: Conference Series,2021(1):1933

[15] Pejman Panahi,Cüneyt Bayılmış,Unal Çavuşoğlu,et al. "Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications[J]." Arabian Journal for Science and Engineering,2021:18-20

[16] Henschen L,Lee J. "A Very Lightweight Encryption Method Based on Multiple Substitution Tables[J]. "Journal of Physics: Conference Series,2021(1):1828-1830

[17] Bo-fan GONG. "Hybrid Compression and Lightweight Encryption of Color Image[C]//".Proceedings of 2020 5th International Conference on Multimedia Systems and Signal Processing(ICMSSP 2020).,2020:38-41

[18] Amna Shifa,Muhammad Babar Imtiaz,Mamoona Naveed Asghar,et al. "Skin detection and lightweight encryption for privacy protection in real-time surveillance applications[J]." Image and Vision Computing,2020,94-96

[19] Mohammad Kamrul Hasan, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, Doris Esenarro Vargas, "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications", *Complexity*, vol. 2021, Article ID 5540296, 13 pages, 2021.

[20] Sunil Kumar et al., “A Survey of Lightweight Cryptography for Power-Constrained IoT Devices: Security Challenges and Issues,” Green Engineering and Technology, 1st Edition, 2021.

[21] Gookyi, D.A.N.; Ryoo, K. A Lightweight System-On-Chip Based Cryptographic Core for Low-Cost Devices. *Sensors* **2022**, *22*, 3004.

[22] Runa Chatterjee et al., “Design of Lightweight Cryptographic Model for End-to-End Encryption in IoT Domain” J. Sustain. Wireless Syst. Vol.01/ No. 04 Pages: 215-224

[23] Bora Aslan, Füsun Yavuzer Aslan, M. Tolga Sakallı, "Energy Consumption Analysis of Lightweight Cryptographic Algorithms That Can Be Used in the Security of Internet of Things Applications", *Security and Communication Networks*, vol. 2020,2020.

[24] Y. Zhang, Y. Shen, H. Wang, J. Yong and X. Jiang, "On Secure Wireless Communications for IoT Under Eavesdropper Collusion," in *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281-1293, July 2016.

[25] Y. Shen, T. Zhang, Y. Wang, H. Wang and X. Jiang, "MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation," in *IEEE Communications Magazine*, vol. 55, no. 9, pp. 86-93, Sept. 2017, doi: 10.1109/MCOM.2017.1700104.

[26] J. Yin, M. Tang, J. Cao, M. You, H. Wang and M. Alazab, "Knowledge-Driven Cybersecurity intelligence: Software Vulnerability Co-exploitation Behaviour Discovery," in *IEEE Transactions on Industrial Informatics*, 2022, doi: 10.1109/TII.2022.3192027.

[27] You, M., Yin, J., Wang, H. *et al.* A knowledge graph empowered online learning framework for access control decision-making. *World Wide Web* (2022).

[28] Ge, YF., Orlowska, M., Cao, J. *et al.* MDDE: multitasking distributed differential evolution for privacy-preserving database fragmentation. *The VLDB Journal* **31**, 957–975 (2022).

[29] Y. -F. Ge *et al*., "Distributed Memetic Algorithm for Outsourced Database Fragmentation," in *IEEE Transactions on Cybernetics*, vol. 51, no. 10, pp. 4808-4821, Oct. 2021, doi: 10.1109/TCYB.2020.3027962.