JPPIPA 10(11) (2024)

Jurnal Penelitian Pendidikan IPA

Journal of Research in Science Education

http://jppipa.unram.ac.id/index.php/jppipa/index

Design of Data Security Module Using Key-Policy Attribute Based Encryption (KP-ABE) Algorithm for an Internet-of-Things System

Reza Fahlevi[1*], Muhammad Salman[1]

[1] Department of Electrical Engineering, University of Indonesia, Depok, Indonesia.

Received: June 27, 2024
Revised: August 21, 2024
Accepted: November 25, 2024
Published: November 30, 2024

Corresponding Author:
Reza Fahlevi
reza.fahlevi22@ui.ac.id

DOI: 10.29303/jppipa.v10i11.8289

Abstract: Internet becomes more popular over time. Everything can be connected with the internet with larger coverage area which makes everyone have a higher dependence on it. Along with that, internet-based technology development and application is also moving to its best pattern. In the development, there are a lot of devices that can be used for Internet-of-Things system development. However, Internet-of-Things system has the following security vulnerabilities especially for access control and data protection. For the data privacy protection, it becomes more critical especially when using a standard TCP/IP based application layer protocol to secure the data before its transmitted from the client to the server. This work will be focused on the data privacy security development using a cryptographic scheme for Internet-of-Things system. Attribute Based Encryption (ABE) is one of cryptographic scheme that can be one of the best choices for data protection implementation in embedded device using NVIDA Jetson Nano. It will demonstrate the design of Key-Policy Attribute Based Encryption (KP-ABE) scheme to generate a symmetric key that will be used for Advanced Encryption Standard (AES) while encryption and decryption process. The result shows the execution time of key generation, data encryption and decryption using unique number of attributes.

Keywords: Data protection; Edge processing; Embedded system; Internet-of-things; KP-ABE algorithm

Introduction

Nowadays, internet is one of the important things for people in the world. In Indonesia, internet trend becomes more popular and the number of internet user increased in every year (Černja et al., 2019; Ceron, 2015). According to Indonesia Central Bureau of Statistics Report, the number of internet users has increased from 32.24% to 62.10% users in the period from 2017 to 2021 and has a very big possibility to increase in the future (Han, Qin, Zhao, & Hu, 2014; Kang et al., 2023; Kumar & Kumar, 2023). The factor that affect the increase in the number of internet users is better network infrastructure development with higher speed and easy accessibility with larger coverage area which makes people have a higher dependence on internet use (Doohan, Kadam, Phursule, Wadne, & Junnarkar, 2022; Elkhodr, Khan, & Gide, 2024; Prasad & Shah, 2021; Xu, Zhang, Zhang, Hou, & Wen, 2023).

Along with that, internet-based technology development and application is also moving to its best pattern and can be implemented for every needs (Khan, Ray, Kassem, & Zhang, 2022; Ma & Li, 2021; Sukaatmadja et al., 2023; Xue, Wang, & Wei, 2023). It is known as Internet-of-Things, an emerging network paradigm which realizes the interconnection among the ubiqitous things and becomes the foundation of smart society. The presence of Internet-of-Things solution will

How to Cite:
Fahlevi, R., & Salman, M. (2024). Design of Data Security Module Using Key-Policy Attribute Based Encryption (KP-ABE) Algorithm for an Internet-of-Things System. *Jurnal Penelitian Pendidikan IPA*, *10*(11), 9825–9831. https://doi.org/10.29303/jppipa.v10i11.8289

provide the ease of human activity by utilizing internet connection (Vlachogianni & Tselios, 2022; Zhang, 2020).

In the development, there are a lot of devices that can be used for Internet-of-Things system development and some of them are open-source. An Internet-of-Things device is typically an embedded hardware with some limitations (Ding et al., 2022; Krishnan, Neyaz, & Liu, 2021). Many Internet-of-Things devices are more vulnerable without any information protection technology. Data security becomes the primary concern of Internet-of-Things system since it becomes a challenge to keep the data privacy secured with a limitation in security system. Internet-of-Things system has the following security vulnerabilities either for access control or information protection. Internet-of-Things system has more than the same problems as sensor networks, mobile communication networks or the Internet, but also has its particularities, such as equipment management, privacy protection, data storage and management, etc (Chang, 2021; Guo, 2022; Yang, Zhou, Huang, & Zhou, 2021).

For the data privacy protection, it becomes more critical especially when using a standard TCP/IP based application layer protocol to secure the data before its transmitted from the client to the server (Aslan & Aslan, 2023; Hassan, Hussien, & Mohialden, 2023; McGraw-Hill, 2012). The default TCP/IP in Internet-of-Things device has no end-to-end data protection and it needs to be applied in order to improve the security level of embedded device usage when using TCP/IP layer for data transmission. Data encryption scheme can be used as an alternative for preserving data privacy when transmit and receive any data from other systems (Kaur et al., 2023; Tyagi, 2020; Vladimirov, Vybornova, Muthanna, Koucheryavy, & El-Latif, 2023).

Attribute Based Encryption (ABE) is one of crypthographic scheme that can be one of the best choices for data protection implementation in embedded device. Basically, Attribute Base Encryption (ABE) belongs to the type of asymmetrical encryption scheme. Attribute Base Encryption (ABE) is included in the type of public key encryption with user's secret key and cipher text depends on defined user attributes. Cipher text only can be decrypt if the set of key attributes matches the cipher text attributes.

Madhushree et al. (2023), Key-Policy Attribute Based Encryption (KP-ABE) is an encryption scheme with fine-grained access control. This scheme is enforcing a strict access control list about who can decrypt sensitive data whenever a user encrypts it. The Attribute Base Encryption (ABE) method was first proposed for leveraging public key cryptography to enforce access control.

Suryawan et al. (2019), in the Key-Policy Attribute Based Encryption (KP-ABE) scheme the access policy is placed on the user's key, and a set of defined attributes are in the encrypted data. If a set of attributes meets the access policy, the user can decrypt the cipher text into a plain text message. Otherwise, the user cannot decrypt the cipher text.

In general, Key-Policy Attribute Based Encryption (KP-ABE) can be described where the data sender composes cipher text built from a set of defined attributes, and the trusted key authority supplies key to the user, which include a policy defining which sort of cipher texts the key can decrypt based on attributes data matching (Kang et al., 2023; Kumar & Kumar, 2023; Xiao, Huang, Miao, Li, & Susilo, 2022). Using Key-Policy Attribute Based Encryption (KP-ABE) scheme, private keys can specify any access method on attributes.

Our works are design a Key-Policy Attribute Based Encryption (KP-ABE) scheme to generate a symmetric key that will be used for Advanced Encryption Standard (AES) while encrypt the plain text to be a cipher text before the data distribution, otherwise decrypt the cipher text to be a plain text after the data has been sent and evaluates its execution time of key generation, data encryption and decryption using unique number of attributes.

Method

The objective of this work are to develop Key-Policy Attribute Based Encryption (KP-ABE) data security application for an Internet-of-Things system. System development uses an agile development method where development will be carried out in stages accompanied by a testing process for each module. The figure of system development method is shown as below:

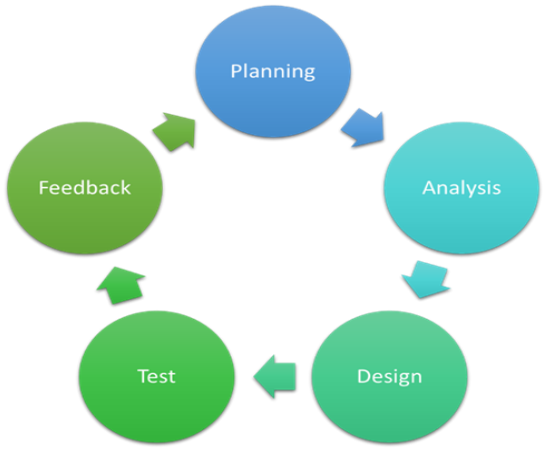

Figure 1. System development life cycle

Planning

A stage to define the objectives of the work based on previous research. Fredy Mendoza-Cardenas et al.

(2022) has developed CP-ABE scheme for an IoT system using different tools and method. The development is using python programming language. And this work uses KP-ABE scheme to develop an application for IoT system with different programming language, exactly using C++ as a lower-level programming language to build the application which has a faster execution time

Analysis

A stage to identify new measurement parameter referenced to the previous work and requirement to achive the objectives.

Design

Create a system design of Data Security Module using Key-Policy Attribute Based Encryption (KP-ABE) Algorithm for an Internet-of-Things (IoT) System. The figure of system design is shown as below:

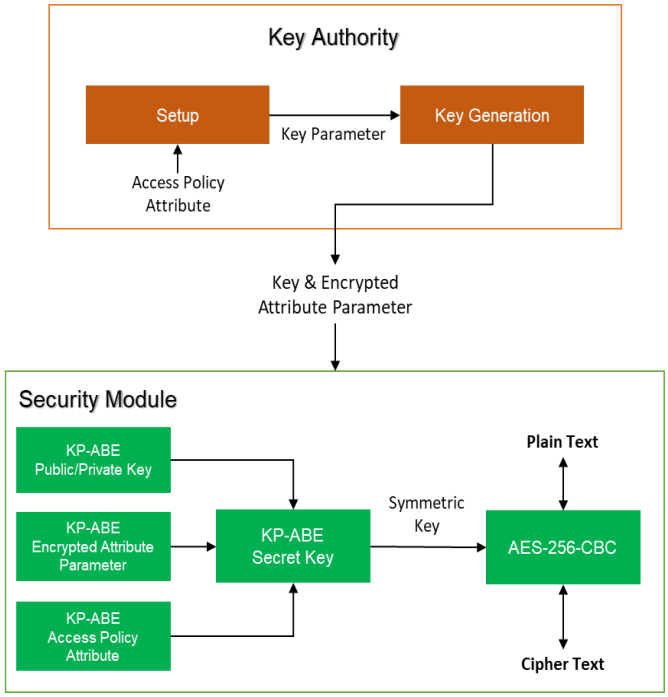

Figure 2. KP-ABE algorithm design

In the key authorithy side, setup algorithm is executed to generate public and private key. Key authority will also generate encrypted attribute data to be combined with each key to generate a symmetric key that will be used for encryption and decryption process. For the encryption purpose, a plain text message is sent to the security module and encrypted with AES-256-CBC and zero filled IV while the symmetric key is generated by Key-Policy Attribute Based Encryption (KP-ABE). The Key-Policy Attribute Based Encryption (KP-ABE) encryption process use the public key from key authority, combined with encryption attribute data and original access policy attribute. Otherwise, for the decryption process, a cipher text is also sent to security module and decrypted using AES-256-CBC and zero filled IV with symmetric key generated by Key-Policy Attribute Based Encryption (KP-ABE) using the combination of private key, encryption attribute and original access policy to get the original plain text message.

This Key-Policy Attribute Based Encryption (KP-ABE) scheme is developed using C++ programming language which referenced from open-source repository in GitHub was developed by ikalchev (2017), A lightweight Attribute-Based Encryption Scheme. In the development, there are improvements include attribute set data type changing from integer to string format, data obscurity improvement, application testing to another embedded platform and some additional functions to import/export key file generated by key authority.

Key-Policy Attribute Based Encryption (KP-ABE) scheme requires several package dependencies for the implementation.

a) FLEX: a package for fast lexical analyzer that can be used to recognize lexical pattern in text. westes (2017) has updated Flex package that derived from software contributed to Berkeley by Vern Paxson and share it to GitHub repository as an open-source package. Flex can work in combination with other package, such as BISON package.
b) BISON: a package for text file analyzer. GNU and Free Software Foundation (2014) define BISON as a programming code parser generator that used to transform an annotated context-free language into a deterministic LR or generalized LR parser.
c) M4: an application of the UNIX-Like macro processor. GNU and Free Software Foundation (2021) define M4 as a package that has built-in functions for file inclusion, shell commands execution, operates arithmetic expression and string data manipulation.
d) LIBGMP: a multiplatform open-source library for Unix-type system such as: Linux, BSD or Mac OS and also works for Windows-based OS as well. GNU and Free Software Foundation (2024) define that libgmp is used for numerical data process, include: arbitrary precision arithmetic, operating on signed integers, rational numbers and floating-point numbers.
e) PBC: stands for Pairing-Based Cryptography, an open-source library first developed by Standford University (2006) that can be used to handle the

mathematical operations required for pairing-based cryptosystems. It provides basic function of cryptosystems such as: elliptic curve generation, elliptic curve arithmetic and pairing computation

f) MBEDTLS: an open-source library that is suitable for embedded systems. Mbed-TLS (2024) has developed and updated the library that implements cryptographic primitives, SSL/TLS and DLTS protocol become an easy to use, readable and flexible TLS library. This is a lightweight version of TLS that suitable for Internet-of-Things system.

Testing & Feedback

The stage for carrying out trial and error on the application ebing developed and getting feedback and information for improvements at the next development stage.

Result and Discussion

This section describes the simulation environment used to evaluate the execution time of setup and key generation in the key authority side, data encryption and decryption using unique number of attributes. The execution time of every process is measured in milliseconds (ms) using C++ time library and the evaluation result will be calculated using arithmetic mean of three execution time measurements.

Key Generation

We use a virtual machine with certain specification which acts as a key authority and has a function for encryption/decryption key generation. The virtual machine specifications are described as follows; 2 Core CPU; 4GB RAM; 32GB SATA Storage and; Linux Ubuntu 22.04 LTS Operating system

Setup algorithm is executed to generate public and private key that will be distributed to the publisher and subscriber. It will also generate encrypted attribute data for each key for the combination material to generate a symmetric key that will be used for encryption and decryption process. The key and its encrypted attribute will be written into two separate files with .key file extension for the key and .attr file extension for the encrypted attribute. In key generation phase, the execution time is the elapsed time to obtain the public and private key with each encrypted attribute.

Table 1 shows the average value of the execution time for Key-Policy Attribute Based Encryption (KP-ABE) key generation phase. The table 1 describes the results of key generation measurement both for public and private key with respect to the number of attributes used. According to the data, the number of attributes will affect the execution time. The larger number of attributes will increase the execution time of key generation. However, the execution time for the entire tested number of attributes are less than 100 milliseconds even with up to 50 unique attributes.

Table 1. Key Generation Execution Time

Number of Attributes	Execution Time (ms)
10	16.68
15	18.07
20	21.58
25	28.44
30	32.43
35	37.77
40	39.66
45	46.09
50	50.39

Encryption and Decryption

Encryption and decryption process are executed on edge device. We use one of the new edge devices that is typically used for edge processing, NVIDIA Jetson Nano. The specification of edge device we used is described as follows: Quad-core ARM® Cortex®-A57 MPCore processor; 4GB 64-bit LPDDR4 RAM; 64GB SD Card Storage Class 10; Linux Ubuntu 18.04 LTS for Embedded Device.

Encryption and decryption process are executed by sending data to the security module application and will receive the result when the encryption or decryption process works.

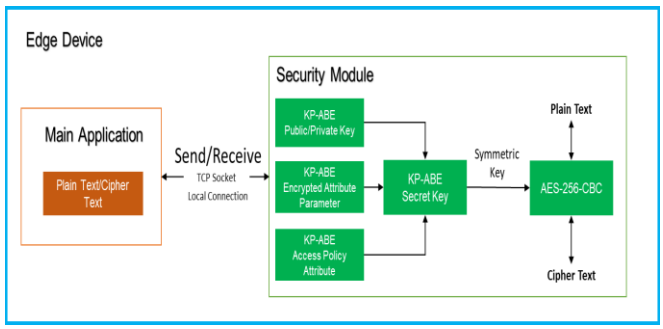

Figure 3. KP-ABE algorithm design

Main application will create a local connection using TCP/IP socket to communicate with security module. Plain text and cipher text from main application will be sent to the security module for encryption or decryption purpose. The security module will provide a response to the main application when the process is successful including the encrypted or decrypted text.

Table 2 shows the average value of the execution time for Key-Policy Attribute Based Encryption (KP-ABE) based data encryption and decryption combined with Advanced Encryption Standard (AES) where Key-Policy Attribute Based Encryption (KP-ABE) scheme is used to generate a symmetric key for the original data

encryption or decryption process using Advanced Encryption Standard (AES).

Table 2. Data Encryption Execution Time

Number of Attributes	Encryption Execution Time (ms)	Decryption Execution Time (ms)
10	23.31	23.38
15	25.16	25.34
20	25.81	25.37
25	25.92	25.91
30	26.32	26.44
35	27.53	26.86
40	28.15	27.38
45	28.41	27.72
50	29.42	28.44

The table above describes the results of data encryption and decryption measurement with respect to the number of attributes used. According to the data, the number of attributes is also affect the encryption or decryption execution time. The larger number of attributes will increase the execution time. However, the execution time for the entire tested number of attributes are even less than 50 milliseconds even with up to 50 unique attributes.

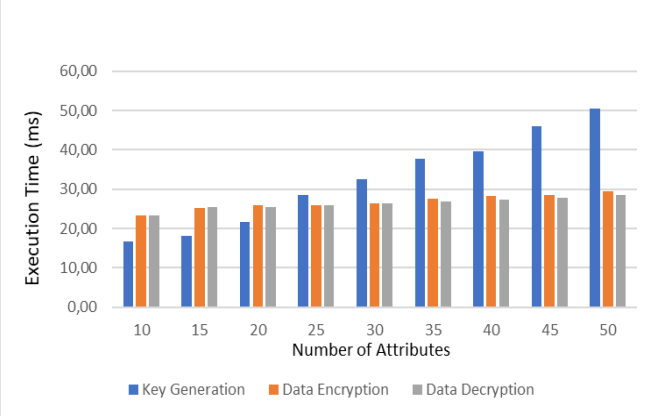

Figure 4. Summary of execution time

The encryption and decryption process takes around 30 milliseconds at the average to be executed even the security module run on the embedded device NVIDIA Jetson Nano, meanwhile the key generation process need a bit more time to be executed because of private and public key data has larger payload size.

However, with the fastest execution time for key generation, encryption and decryption time make the design of Key-Policy Attribute Based Encryption (KP-ABE) based data encryption and decryption is suitable for Internet of Things system which requires more security improvement especially for data protection with a lightweight data encryption and decryption system.

Conclusion

This work develops a lightweight data encryption and decryption scheme for Internet of Things system security improvement purpose. According to the result, the design of Key-Policy Attribute Based Encryption (KP-ABE) based data encryption and decryption is suitable to be implemented in Internet of Things system and still provides faster execution time when applied in the embedded device with common specification which is typically used for edge processing. Key-Policy Attribute Based Encryption (KP-ABE) based data encryption and decryption can be applied to the Internet of Things system using various number of attributes, in this case use up to 50 string-based attributes with various length of each attribute defined in the program and still provides a good result for each process.

For the future work, the system can be developed further with additional various number of attributes and other encryption method for data signature to get more information and evaluation.

Acknowledgments
The author wish thank to the previous researcher for their paper who have provided references related to this works and also to the people who have shared lightweight attribute-based encryption source code on GitHub. The original source code can be found at https://github.com/ikalchev/kpabe-yct14-cpp.

Author Contributions
Investigation, R.F and M.S; formal analysis, R.F and M.S; investigation R.F and M.S; resources, R.F and M.S; data curation, R.F and M.S: writing—original draft preparation, R.F and M.S; writing—review and editing, R.F and M.S: visualization, R.F and M.S; supervision, R.F and M.S; project administration, R.F and M.S; funding acquisition, R.F and M.S. All authors have read and agreed to the published version of the manuscript.

Funding
This research received no external funding.

Conflicts of Interest
The authors declare no conflict of interest.

References

Aslan, F. Y., & Aslan, B. (2023). Comparison of IoT Protocols with OSI and TCP/IP Architecture. *International Journal of Engineering Research and Development UMAGD*, *15*(1). Retrieved from https://dergipark.org.tr/en/pub/umagd/issue/72926/1063036

Černja, I., Vejmelka, L., & Rajter, M. (2019). Internet addiction test: Croatian preliminary study. *BMC Psychiatry*, *19*(1), 1–11.

https://doi.org/10.1186/s12888-019-2366-2

Ceron, A. (2015). Internet, News, and Political Trust: The Difference Between Social Media and Online Media Outlets. *Journal of Computer-Mediated Communication*, *20*(5). https://doi.org/10.1111/jcc4.12129

Chang, G. (2021). Urban air pollution diffusion status and sports training physical fitness measurement based on the Internet of things system. *Arabian Journal of Geosciences*, *14*. https://doi.org/10.1007/s12517-021-07947-x

Ding, X., Wang, H., Li, G., Li, H., Li, Y., & Liu, Y. (2022). IoT data cleaning techniques: A survey. *Intelligent and Converged Networks*, *3*(4). https://doi.org/10.23919/ICN.2022.0026

Doohan, N. V., Kadam, S., Phursule, R., Wadne, V. S., & Junnarkar, A. (2022). Implementation of AI based Safety and Security System Integration for Smart City. *International Journal of Electrical and Electronics Research*, *10*(3). https://doi.org/10.37391/IJEER.100319

Elkhodr, M., Khan, S., & Gide, E. (2024). A Novel Semantic IoT Middleware for Secure Data Management: Blockchain and AI-Driven Context Awareness. *Future Internet*, *16*(1). https://doi.org/10.3390/fi16010022

Guo, L. (2022). Application of Blockchain Based on Deep Learning Algorithm in Enterprise Internet of Things System. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/9943452

Han, F., Qin, J., Zhao, H., & Hu, J. (2014). A general transformation from KP-ABE to searchable encryption. *Future Generation Computer Systems*, *30*(1). https://doi.org/10.1016/j.future.2013.09.013

Hassan, G. M., Hussien, N. M., & Mohialden, Y. M. (2023). Python TCP/IP libraries: A Review. *International Journal Papier Advance and Scientific Review*, *4*(2). https://doi.org/10.47667/ijpasr.v4i2.202

Kang, P., Zhao, K. Q., Liu, B., Guo, Z., Feng, C. S., & Qing, Y. (2023). A KP-ABE Scheme Supporting Large Universe and Security Classification. *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, *51*(9). https://doi.org/10.12263/DZXB.20210493

Kaur, K., Kaur, M., Kaur, K., & Madaan, A. (2023). A Comparative Study of OSI and TCP/IP Models. *International Journal of Engineering and Management Research*, *13*(2). http://dx.doi.org/10.31033/ijemr.13.2.20

Khan, N., Ray, R. L., Kassem, H. S., & Zhang, S. (2022). Mobile Internet Technology Adoption for Sustainable Agriculture: Evidence from Wheat Farmers. *Applied Sciences (Switzerland)*, *12*(10). https://doi.org/10.3390/app12104902

Krishnan, S., Neyaz, A., & Liu, Q. (2021). IoT Network Attack Detection using Supervised Machine Learning. *International Journal of Artificial Intelligence and Expert Systems (IJAE), 10*, 18–32. Retrieved from https://www.cscjournals.org/manuscript/Journals/IJAE/Volume10/Issue2/IJAE-201.pdf

Kumar, D., & Kumar, M. (2023). Outsourcing decryption of KP-ABE using elliptic curve cryptography. *International Journal of Information and Computer Security*, *22*(2). https://doi.org/10.1504/IJICS.2023.134961

Ma, H., & Li, J. (2021). An Innovative Method for Digital Media Education Based on Mobile Internet Technology. *International Journal of Emerging Technologies in Learning*, *16*(13). https://doi.org/10.3991/ijet.v16i13.24037

Prasad, V., & Shah, P. K. (2021). A data security module based on crypto and steganography techniques. *2021 2nd International Conference for Emerging Technology, INCET 2021*. https://doi.org/10.1109/INCET51464.2021.9456373

Sukaatmadja, I. P. G., Yasa, N. N. K., Santika, I. W., Rahanatha, G. B., Rahmayanti, P. L. D., & Muna, N. (2023). The role of international networking to mediate internet technology capabilities and international entrepreneurship orientation to export performance. *Uncertain Supply Chain Management*, *11*(2). https://doi.org/10.5267/j.uscm.2023.2.004

Tyagi, A. (2020). TCP/IP Protocol Suite. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://doi.org/10.32628/cseit206420

Vlachogianni, P., & Tselios, N. (2022). Perceived usability evaluation of educational technology using the System Usability Scale (SUS): A systematic review. *Journal of Research on Technology in Education*, *54*(3), 392–409. https://doi.org/10.1080/15391523.2020.1867938

Vladimirov, S. S., Vybornova, A., Muthanna, A., Koucheryavy, A., & El-Latif, A. A. A. (2023). Network Coding Datagram Protocol for TCP/IP Networks. *IEEE Access*, *11*. https://doi.org/10.1109/ACCESS.2023.3266289

Xiao, M., Huang, Q., Miao, Y., Li, S., & Susilo, W. (2022). Blockchain Based Multi-Authority Fine-Grained Access Control System with Flexible Revocation. *IEEE Transactions on Services Computing*, *15*(6). https://doi.org/10.1109/TSC.2021.3086023

Xu, C., Zhang, J., Zhang, Z., Hou, J., & Wen, X. (2023). Data and Service Security of GNSS Sensors Integrated with Cryptographic Module. *Micromachines*, *14*(2).

https://doi.org/10.3390/mi14020454

Xue, Q., Wang, H., & Wei, J. (2023). Internet technology and regional financial fraud: evidence from Broadband expansion in China. *Journal of Applied Economics*, *26*(1). https://doi.org/10.1080/15140326.2023.2281167

Yang, D., Zhou, Y., Huang, W., & Zhou, X. (2021). 5G mobile communication convergence protocol architecture and key technologies in satellite internet of things system. *Alexandria Engineering Journal*, *60*(1). https://doi.org/10.1016/j.aej.2020.09.019

Zhang, M. (2020). Influence of internet technology on mental health and positive emotions of college students. *Revista Argentina de Clinica Psicologica*, *29*(2). https://doi.org/10.24205/03276716.2020.271