Proceedings of the International Conference on Sustainable Computing and Data Communication Systems (ICSCDS-2023)
IEEE Xplore Part Number: CFP23AZ5-ART; ISBN: 978-1-6654-9199-0

2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) | 978-1-6654-9199-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCDS56580.2023.10104702

Artificial Intelligence based Security Solution for Data Encryption using AES Algorithm

1st Amit Kumar Mishra
Dept. of Computer Science & Engineering,
Graphic Era Hill University, Dehradun, Uttarakhand, (India)
amitmishraddun@gmail.com

2nd Neha Tripathi
Dept. of Computer Science & Engineering,
Graphic Era (Deemed to be University), Dehradun, Uttarakhand, (India)
nehagarg.february@gmail.com

3rd Musheer Vaqur
Department of Computer Science & Engineering,
Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, Uttarakhand (India)
musheer77@gmail.com

4th Sugandha Sharma
School Of Computer Science,
UPES, Bidholi, Dehradun, Uttarakhand, (India)
sugandhasharma2016@gmail.com

***Abstract*— The Internet of Things (IoT) has a significant impact on the transportation industry. Autonomous vehicles (AVs) were created to make daily activities easier by hauling goods, distributing packages, and easing traffic. The AVs had a wide range of uses and comprised land vehicles, aerial vehicles, and maritime vehicles. The Cyber Security (CS) enabled data transfer autonomous driving was set up by them to facilitate the solution of this challenge. A network acts as the mediator, downloading data of the transmitter to the autonomous car. For additional safety, the CS-based method Advanced Encryption Standard (AES) is involved to decrypt the data, which is transferable to cypher text. The encryption content could be deciphered by the secret key which is given by the transmitter to the peculiar AV. Customized particle swarm efficiency would be used to modify a conventional neural network. The researchers proposed product's final stage should be to decrypt the document using dual encryption technology. After the dual cryptography, steganography techniques are used to improve the retention safety of the proposed solution. Their proposed approach was implemented in the Java work area using Internet simulation.**

Keywords—Data Encryption, Advanced Encryption, Cyber Security, Autonomous Vehicle.

I. INTRODUCTION

AV production has increased dramatically in recent years. AVs were receiving a lot of attention from businesses. A variety of sensors are used by AVs to evaluate their environment. Although AVs have a lot of promise they could achieve for the transportation sector, security and privacy concerns represent new problems that should be handled [1]. Malicious tampering was possible with the detectors. Before responding to sensor signals, vehicles should check their validity. The Network of Transportation Infrastructure refers to IoT systems that comprise a variety of AVs. Assaults on the Internet of Transportation Systems were discussed [2-4]. Information was retrieved in real time from technologies like autonomous and, in the future, driverless automobiles.

Electricity transport networks necessitate energy efficiency. Challenges to the safety of such networks could result in huge harm, including crashes, fatalities, and being trapped on solitary roadways as a result of power control assaults. Data Science/ML approaches are being used to examine AV data, and applying stream analytics/learning methods to transport information would be a difficulty [4]. Machine deep learning is utilized for the huge volumes of detector data collected by Avs. For numerous applications to best locations, traveling without a person in the loop, and many others, the Internet of Transport Networks would rely largely on Data Science/AI/ML approaches [5]. The Opponent would study the machine learning algorithm and attempt to undermine them. Lastly, while the Network of Transport Networks collects high amounts of information, personal privacy must be maintained [6]. Researchers anticipate that cloud-based technologies coupled with the Network of Transport Network should be used for most of the information exchange and monitoring.

There are other areas of vulnerability in the automotive ecosystem besides the sensors on the vehicles. The driverless cars and vehicles are moved on the roads and collecting the data of the road infrastructure which is stored in the cloud. Automakers can remotely apply software updates and problem fixes thanks to OTA updates. However, this can result in security problems because a single flawed patch could cause the system to malfunction and become confusing [7] [8]. If the security posture is not correctly implemented, there is a significant danger of exploitation because these updates are begun and distributed remotely [9]. The work conducted in [10] proposed to decrypt the OTA update obtained by the Original Equipment Manufacturer, gateway Electronic Control Units (ECUs) with Physically Unclonable Functions (PUFs) be used. Every vehicle assembly requires the supply chain, which must also be safeguarded. Each component of a vehicle is made by numerous independent contractors, therefore a hack directed at one of these OEMs could cause trouble. Establishing cybersecurity standards for goods produced by third parties is one approach for OEMs to prevent such malfunctions. For instance, OEMs can collaborate closely with outside producers to find potential flaws in the architecture of the necessary components before mass production.

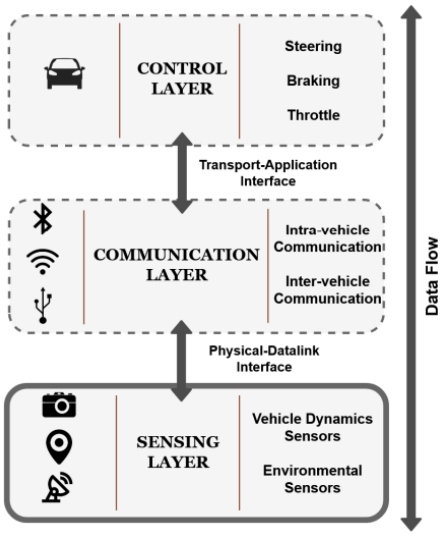

Fig. 1. Three Layer Architecture

Figure 1 shows the hierarchical architecture of IoT based applications in automotive security for categorization of risks. The hierarchy's first tier, the sensing layer, which is made up of car sensors, is frequently referred to as the AutoVSCC (Autonomous Vehicular Sensing Communication and Control) framework [11]. The Global Positioning System (GPS), Tire Pressure Monitoring Systems (TPMS), and ultrasonic sensors can all be compromised in order to mislead them into detecting items that aren't there. Threats to the sensing layer can pass from the physical datalink interface to the communication layer, where they can transform analogue data from the sensors to digital data that can be used for both intra- and inter-vehicle communications. At the communication layer, vulnerabilities to cybersecurity include intercepting messages exchanged between vehicles, sending false messages intra-vehicle (inside a vehicle's communications buses), and gaining control of a vehicle. The control layer's capacity to translate rich digital data into real-time vehicle applications like automated steering control, lane change manoeuvres, and brake application may be hampered by threats at the sensor and communication levels. This is accomplished using the transport-application interface.

II. Literature Review

The presence of a large incidence of false reports creates unwanted involvement of human operators [12], which is one of the issues with conventional IDS methods. Human analysts, for their part, conduct in-depth analyses regularly to discern the character of warnings and take necessary measures. The proposed method demonstrates the benefit of combining K-means– fuzzy–neuro methods to remove the unavoidable human evaluation intervention in situations. DARPA internet traffic samples [13] were used to evaluate the approach with a variety of background knowledge collections. The actual findings indicated a significant reduction in false reports, and an improved capacity to collect assault particles that were comparable to the training data.

The integrated approach was designed to be extendable by enabling customers to browse into many groups of IDSCs at the same time to blend product characteristics for a more uniform IDS approach [14]. An identical structure might exhibit the multiple processes of the access point on distant structures, establishing agreement on the acquisition of the IDS outcome in exciting circumstances [15]. The concept was practical in the private computer after executing a basic version of the proposed system. They successfully discussed and experienced different concerns in the virtualized environment and effectively activated the IDSs and their implementation in the cloud owing to the difficulty of the virtualized environment. Furthermore, they convincingly advocated for the use of masked IDS on the internet that should be designed to withstand multiple assaults [16]. To ensure cloud security, their original IDS solution comprised performance and skill assessment [12-13]. They envisaged two simple intrusion detection systems, to benefit from this method's flaw being compensated for the other's flaw [17][18]. This study's main objective was to present a cutting-edge methodology that enables a cloud computing model to achieve the efficiency of system resource allocation and the vitality of the security operation without the need for modifications[19][20].

III. Proposed Methodology

Although cloud technology has piqued the interest of academics and industry, it is still a developing concept. Data protection was among the most pressing challenges to cloud technology. They have developed an effective way for sending very great safe storage information to the cloud system to increase memory safety. In this research, a customized ANN is used to detect malware in cloud data. With the support of the optimization technique, the conventional NN was updated. For mass updation, the proposed approach uses a customized particle swarm optimization algorithm. The consumer wishes to save the information in the cloud after checking the storage server penetration. Our recommended solution was to encrypt the file using encryption to improve storage safety. The decryption of the proposed solution was done using dual cryptographic techniques. Two algorithms could be safe to use a technique.

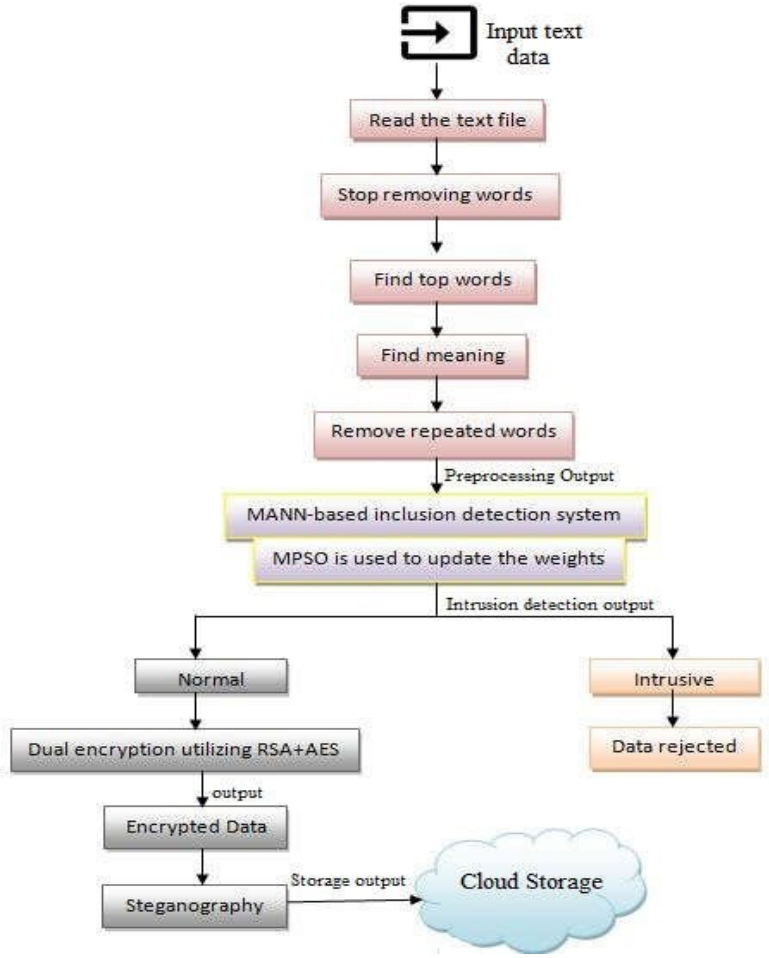

Fig. 2. Proposed Methodology

A. Description of AES Algorithm

Block cypher to 128-bit block size would be AES. It is available with keys of 128, 192, and 256 bits. The key size recommended by designers for AES is 512 bits. Ten compute rounds make up the encryption process for 512-bit secrets. The remaining rounds in each scenario were the identical, with the exception of the final round. A 512-bit input message was used to build a 4 x 4 byte matrix that served as the state array. The novel technique uses 512-bit input blocks and keys, making it more immune to cryptanalysis while increasing the permitted area. AES-512 would be useful for applications that require high safety and are space-restricted. The various transformations work on the organizational outcomes, which were referred to as states; the state was essentially a rectangular array of bytes. The first 4 elements of the timetable are XORed to the input state before round-based encryption operations could occur. The proposed work's current stage was indicated at the bottom of the page. The proposed work's key function was calculated at the beginning of the next section.

The column-by-column combination conversion works on the state and treats every section as a four-term polynomial. The goal of the phase should be to ensure that the bits are evenly distributed throughout numerous rounds. A column at a time is multiplied to achieve this. Every row value in a traditional matrix is used to calculate each column signal. Include a circular Secrete: By bitwise XOR, they attach round secret in the region to add round secret.

Using a secret schedule, a round secret could be obtained from the cypher key.

IV. RESULTS AND DISCUSSION

The performance of the developed approach was analyzed in the chapter below. The decryption and encryption times for various document formats are shown in Table 1. Designers use document sizes of 10, 20, 30, and 40 kb in our process. For dual encryption, it takes 5.796 seconds to encrypt a 10 kb document, therefore the document size changes, and the duration it takes to encode the document changes as well. An approach takes 5.796 seconds to encrypt and 5.123 seconds to decrypt the 10 kb file. Encryption and decryption times vary depending on file sizes, such as 20, 30, and 40 kb. It takes 9.864 seconds to encode a 20-kilobyte file and 8.457 seconds to decode the file. Table 1 displays the full storage value and processing duration of the proposed procedure of the proposed strategy. The number of observations was varied, and the storage quantity and processing time were calculated. The chart values for the number of iterations, storage quantity, and processing duration are shown in Figure 2. The graph was seen in the section below.

TABLE I. TIME TAKEN FOR DATA ENCRYPTION AND DECRYPTION

Size of file (kb)	Time of Encryption(s)	Time of Decryption(s)
10	5.783	5.235
20	9.986	8.742
30	13.9764	11.9458
40	17.0294	14.0631

By adjusting the number of bullets, the proposed technique reaches a memory storage quantity of 13,598,247.75 bits. The optimization approaches have a total execution time of 21,008 milliseconds. Figure 3 illustrates the system performance for the suggested technique by varying the number of repetitions. The fitness value of the proposed strategy is shown in Figure 4. In the MPSO, the message with the smallest mistake frequency was picked as the highest fitness value. The efficiency score drops as the number of observations grow in this case. Table 2 demonstrates the complete categorization validity of the recommended MANNs based back propagation technique. The recommended MANN provides 91.25 percent accuracy in this case.

TABLE II. ACCURACY OF PROPOSED MODEL

Classifier	Accuracy value for testing (percentage)
MANN (MPSO+ANN)	93.54

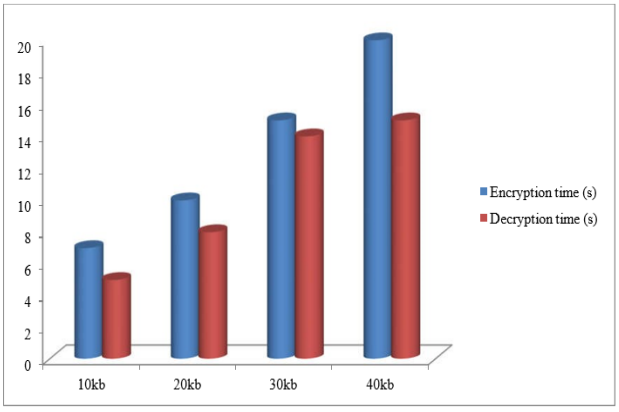

Fig. 3. Encryption and Decryption Frequency

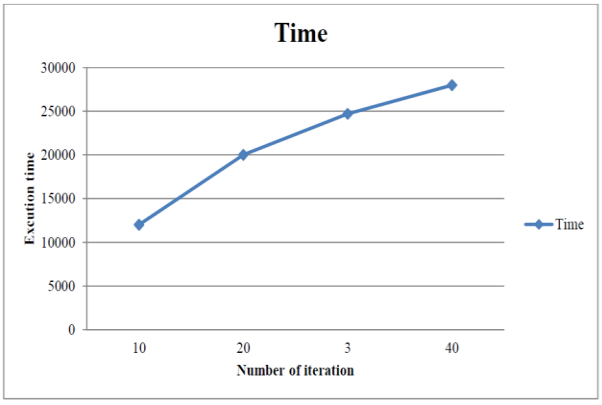

Fig. 4. Computational Time of Proposed Model

In IDS, classification performance was the most important component. It is critical for the approach to have a higher precision score to be considered the providing competitive, and this paper offers a comparison of accuracy values utilizing current intrusion detection methods. In contrast, we will use current IDS as a conventional NN and current malware detection as an evolutionary approach. The classification performance of the present approach was 85.7 percent, for the proposed methods is 91 percent, and for the proposed protocol was 93.46 percent, as shown in the chart. Because the proposed product's effectiveness is great, it appears to be superior to existing techniques.

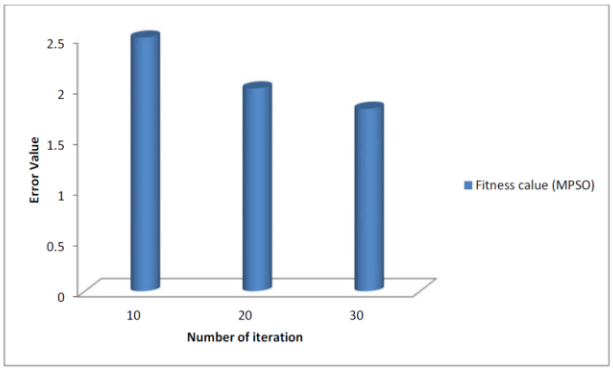

Fig. 5. Fitness Value of Proposed Model

Different security threats are conducted to validate the safety of the given method. They were utilizing a MiM assault and a DoS assault here. For an encryption process to be functional the effects of the assaults on the information should be minimal, ensuring more safety and limiting access to information are permitted. Regardless of criticisms of previous techniques, the proposed solution provides the greatest results. Table 3 compares proposed and existing approaches to a variety of assaults, including MIM and DoS assaults. Traditional systems have a higher assault percentage, while detection algorithms to a reduced assault %. The proposed solution protects the information better than current techniques, regardless of the type of assault.

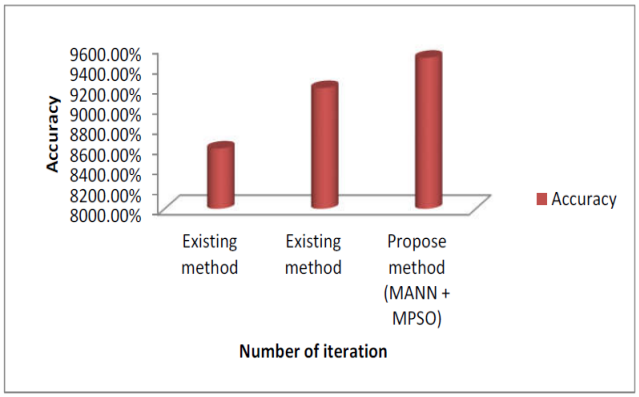

Fig. 6. Accuracy of Proposed Model

The present and proposed methods are compared. The time taken for secrete shattering in the proposed approach was longer than the time required for major breaking in the conventional methods, as shown in the table. The proposed technique attempts 128 times, whereas the present system

attempts 120 times to reach the key score in a 10 kb document space. The proposed approach tries 132 times to reach the secret score of a 20 kb document, while the existing system attempts 123 times, which was the smallest number of instances contrasted to a developed method. Similarly, the proposed technique breaks the main score fo4 30 and 40 kb 112 and 136 times, whereas the present method breaks the primary value fo4 30 and 40 kb 95 and 129 times. As a result, the proposed solution provides the highest level of security. A finding suggests that the proposed technique outperforms current methods in terms of intrusion prevention efficiency and safety. Researchers are using the KDD database to evaluate the proposed performance, and the results were compared to recent academic work. Researchers are using fuzzy C-means, ANN, and a hybrid technique to evaluate the current structure.

Table 4 summarizes the findings. Kappa statistics mean extreme mistake, and root means square mistake value, correlating effectiveness to the proposed technique. The outcomes are tallied. When contrasted to DES of encoding and decoding, the median information rate for encryption was poor. In encryption and decryption operations, the proposed hybrid approach would use less storage. The median data rate is the quantity of encrypted or decrypted information encoded or decoded every second. When contrasted with the other ways, the data clearly show that the proposed methodology outperforms them.

V. CONCLUSION

The attributes of the Internet of Transport Systems about AVs, and the security and privacy problems of platforms, have been explored in this study. Following that, AI and safety could be combined. The topic of cloud-based Network Transport Networks was also brought up. Lastly, AI, safety, and the internet could be used to improve the Network of Transport Systems. Protecting the Internet of Transport Networks, has just touched the surface. To identify and mitigate assaults, researchers need to understand the many sorts of tracks and create machine learning approaches. Researchers should be considering dealing with assaults on machine learning approaches, which are required for the development of Smart Network of Transport Networks. Lastly, they must decide which types of information to transmit on the safe internet to perform statistics.

TABLE III. COMPARISON OF MIM AND DOS ATTACK

Size of File, kb	**MIM**		**DoS attack**	
	Recommended method (RES + AES) %	Current method (RSA) %	Recommended method (RES + AES) %	Current method (RSA) %
10	7.5	11.33	8.5	10.98
20	8.3	10.16	9.9	10.4
30	10.5	10.5	10.6	12.7
40	11.7	10.9	10.9	13.52

TABLE IV. COMPARISON OF PROPOSED AND EXISTING SOLUTION

Size of file, kb	**Recommended method (RSA+AES)**	**Proposed method (RSA)**
10	131	122
20	136	126
30	115	97
40	137	13

REFERENCES

[1] J. Anitha Ruth, H. Sirmathi, and A. Meenakshi, "Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks," IET Information Security, vol. 13, no. 4. Institution of Engineering and Technology (IET), pp. 321–329, Jul. 2019. doi: 10.1049/iet-ifs.2018.5295.

[2] O. Alabi, A. J. Gabriel, A. Thompson, and B. K. Alese, "Privacy and Trust Models for Cloud-Based EHRs Using Multilevel Cryptography and Artificial Intelligence," Internet of Things. Springer International Publishing, pp. 91–113, 2022. doi: 10.1007/978-3-030-80821-1_5.

[3] J. Jain, "Artificial Intelligence in the Cyber Security Environment," Artificial Intelligence and Data Mining Approaches in Security Frameworks. Wiley, pp. 101–117, Aug. 10, 2021. doi: 10.1002/9781119760429.ch6.

[4] Z. Wang, L. Shi, N. Chen, and J. Chen, "Research on computer network security evaluation based on image recognition and neural network," Journal of Electronic Imaging, vol. 32, no. 01. SPIE-Intl Soc Optical Eng, Sep. 15, 2022. doi: 10.1117/1.jei.32.1.011214.

[5] S. Gadde, J. Amutharaj, and S. Usha, "A security model to protect the isolation of medical data in the cloud using hybrid cryptography," Journal of Information Security and Applications, vol. 73. Elsevier BV, p. 103412, Mar. 2023. doi: 10.1016/j.jisa.2022.103412.

[6] M. U. Bokhari, Q. M. Shallal, and Y. K. Tamandani, "Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning," IETE Journal of Research, vol. 65, no. 2. Informa UK Limited, pp. 227–235, Jan. 28, 2018. doi: 10.1080/03772063.2017.1419835.

[7] P. Garikapati, K. Balamurugan, and T. P. Latchoumi, "<i>K</i>-means partitioning approach to predict the error observations in small datasets," International Journal of Computer Aided Engineering and Technology, vol. 17, no. 4. Inderscience Publishers, p. 412, 2022. doi: 10.1504/ijcaet.2022.126601.

[8] B. Tadele Bekele, J. Bhaskaran, S. Dufera Tolcha, and M. Gelaw, "Simulation and experimental analysis of re-design the faulty position of the riser to minimize shrinkage porosity defect in sand cast sprocket gear," Materials Today: Proceedings, vol. 59. Elsevier BV, pp. 598–604, 2022. doi: 10.1016/j.matpr.2021.12.090.

[9] E. Altayef, F. Anayi, and M. Packianather, "A new enhancement of the k-NN algorithm by Using an optimization technique," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, Apr. 28, 2022. doi: 10.1109/icacite53722.2022.9823537.

[10]M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover Internet of Things, vol. 1, no. 1. Springer Science and Business Media LLC, Feb. 24, 2021. doi: 10.1007/s43926-020-00001-4.

[11]Y. Alkali, I. Routray, and P. Whig, "Study of various methods for reliable, efficient and Secured IoT using Artificial Intelligence," SSRN Electronic Journal. Elsevier BV, 2022. doi: 10.2139/ssrn.4020364.

[12] P. Nirmala, S. Ramesh, M. Tamilselvi, G. Ramkumar, and G. Anitha, "An Artificial Intelligence enabled Smart Industrial Automation System based on Internet of Things Assistance," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). IEEE, Jan. 28, 2022. doi: 10.1109/accai53970.2022.9752651.

[13]S. D. Putra, A. D. W. Sumari, A. S. Ahmad, S. Sutikno, and Y. Kurniawan, "Cognitive Artificial Intelligence Countermeasure for Enhancing the Security of Big Data Hardware from Power Analysis Attack," Advanced Sciences and Technologies for Security Applications. Springer International Publishing, pp. 61–86, 2020. doi: 10.1007/978-3-030-35642-2_4.

[14] H. Sharma and N. Kumar, "Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey," Physical Communication, vol. 57. Elsevier BV, p. 102002, Apr. 2023. doi: 10.1016/j.phycom.2023.102002.

[15] J. Zhang and Z. Zhang, "Ethics and governance of trustworthy medical artificial intelligence," BMC Medical Informatics and Decision Making, vol. 23, no. 1. Springer Science and Business Media LLC, Jan. 13, 2023. doi: 10.1186/s12911-023-02103-9.

[16]A. E. Adeniyi, K. M. Abiodun, J. B. Awotunde, M. Olagunju, O. S. Ojo, and N. P. Edet, "Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach," Multimedia Tools and Applications. Springer Science and Business Media LLC, Jan. 13, 2023. doi: 10.1007/s11042-023-14338-9.

[17] N. K. Pandey, A. K. Mishra and V. Kumar, "An Extended Intelligent Water Drop Strategy for Process Scheduler in Cloud," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-4, doi: 10.1109/ISCON52037.2021.9702311.

[18] M. Wazid, M. S. Obaidat, A. K. Das, and P. Vijayakumar, "SAC-FIIoT: Secure Access Control Scheme for Fog-Based Industrial Internet of Things," in IEEE Global Communications Conference (GLOBECOM' 20), Taipei, Taiwan, 2020, pp. 1–6.

[19] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," in *IEEE Access*, vol. 8, pp. 95956-95977, 2020, doi: 10.1109/ACCESS.2020.2995917.

[20] D. M. Dumbere and N. J. Janwe, "Video encryption using AES algorithm," Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014, Coimbatore, India, 2014, pp. 332-337, doi: 10.1109/ICCTET.2014.6966311.