DATA ENCRYPTION USING AES ALGORITHM: CYBER SECURITY AND ARTIFICIAL INTELLIGENCE

[1]N.Poornima, [2]C.Vishnu Vardhan Reddy, [3]E.Sravani , [4]N.Bhargavi,[5]B.Harika, [6]R.Hareesh
[1]Associate Professor, [2-6]U G Student, [1-6]Department of Computer Science & Information Technology,
[1-6] Siddharth Institute of Engineering &Technology

Abstract

In the transportation sector, the Internet of Things (IoT) has significant ramifications. Autonomous vehicles (AVs) were designed to daily tasks easier, distributing parcels, reducing traffic, and transporting commodities. Aerial and marine cars, and ground vehicles, were included in the AVs, a wide range of uses. They were deploying Cyber Security (CS) enabled data transfer autonomous driving to solve this challenge. A network serves as the intermediary, downloading data of the transmitter to the autonomous car. For additional safety, they employ a CS-based method Advanced Encryption Standard (AES) to decrypt the transferred data to cypher text. The secret key provided by the transmitter to the specific AV could decipher the encryption content. 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— Cyber Security, Cipher text, AES, Private key, AV.

1. Introduction

There has been a boom in AVs in current history. AVs were receiving a lot of attention from businesses. AVs use a range of sensors to assess their surroundings. 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 example? 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 our 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.

2. Related Works

The presence of a large incidence of false reports creates unwanted involvement of human operators [7], 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 [8] 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 [9]. 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 [10]. 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 [11]. 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. The major goal of this study was to provide a novel approach that allows a cloud computing model to accomplish the effectiveness of system resource distribution and the vitality of the security operation without requiring changes.

3. Proposed method

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 project, they were use a customized ANN 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.

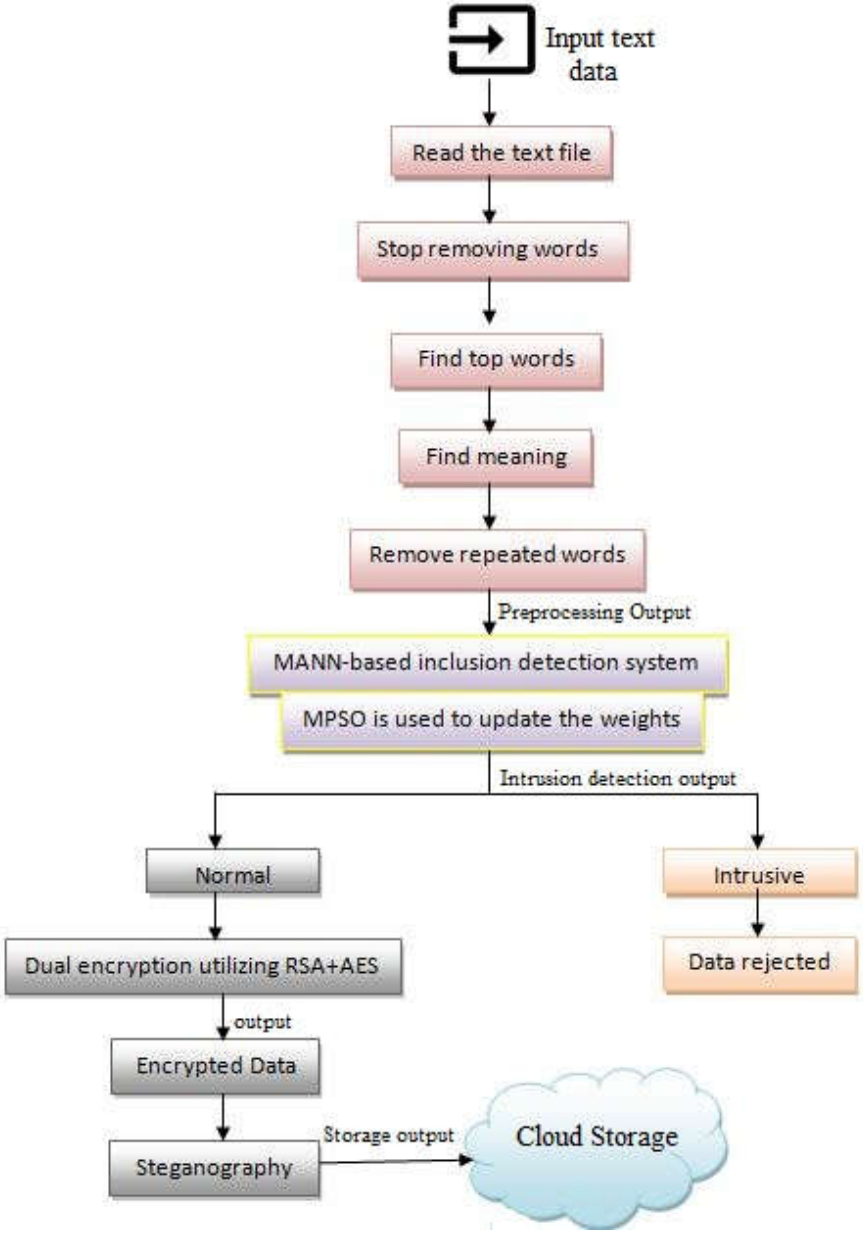

Figure 1: Proposed Methodology

3.1 AES algorithm:

AES would be block cypher to 128-bit block size. It comes in three key sizes: 128, 192, and 256 bits. Designers suggest AES to a key size of 512 bits. For 512-bit secrets, the encryption procedure consists of ten rounds of computation. Except for the last round in each scenario, the rest of the rounds were the same. The state array was a 4 x 4 matrix of bytes created from a 512-bit input message. 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 country 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. This is accomplished by multiplying a column at a moment. In a conventional matrix, each column signal is calculated by every row value. 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.

4 Performance Analysis

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 1: The time it takes to encode and decode documents of different sized.

File size (kb)	Encryption time (s)	Decryption time (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. The system performance for the proposed technique is shown in Figure 3 by adjusting 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. reduced mistake frequency, this progressive reduction in optimal solution eventually achieves the highest optimal solution. Table 2 demonstrates the complete categorization validity of the proposed MANNs based back propagation technique. The proposed MANN provides 91.25 percent accuracy in this case.

Table 2 demonstrates the proposed product's precision rate.

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

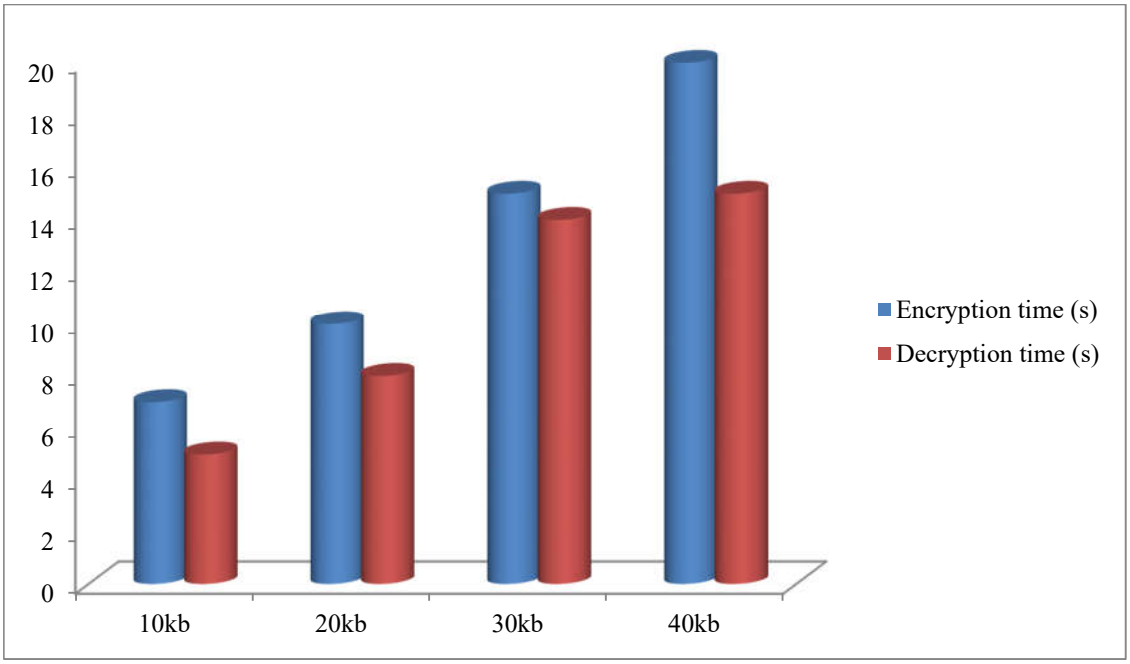

Figure 2: Frequency to encryption and decryption as a function of file size

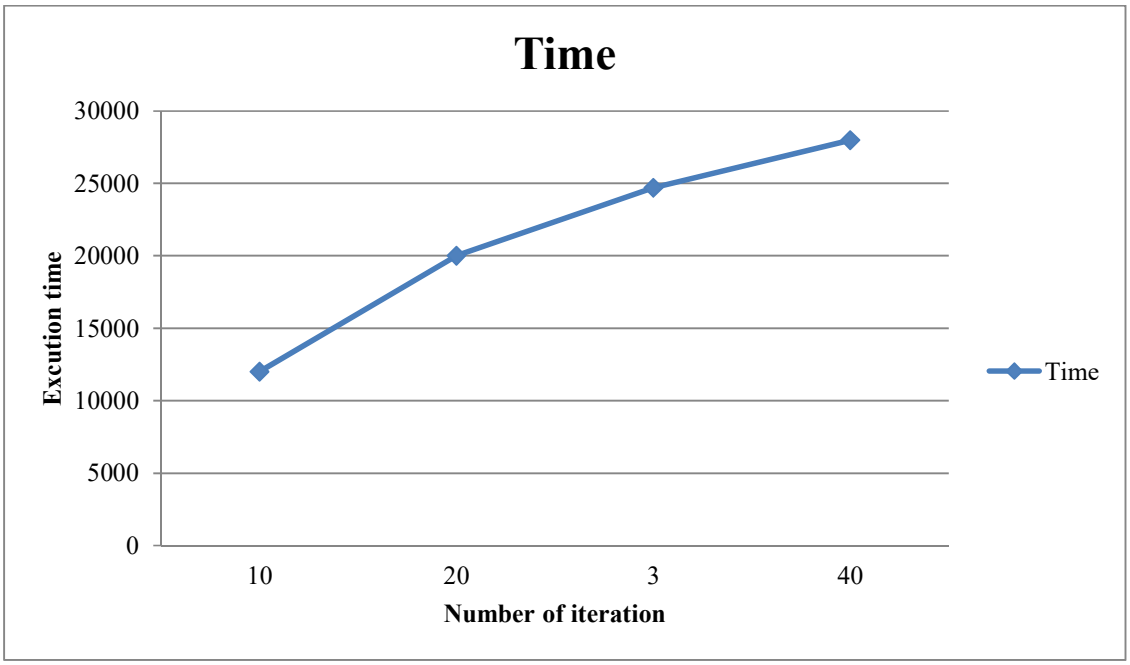

Figure 3: The proposed method's computational time.

In IDS, classification performance was the most important component. It's 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'll 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.

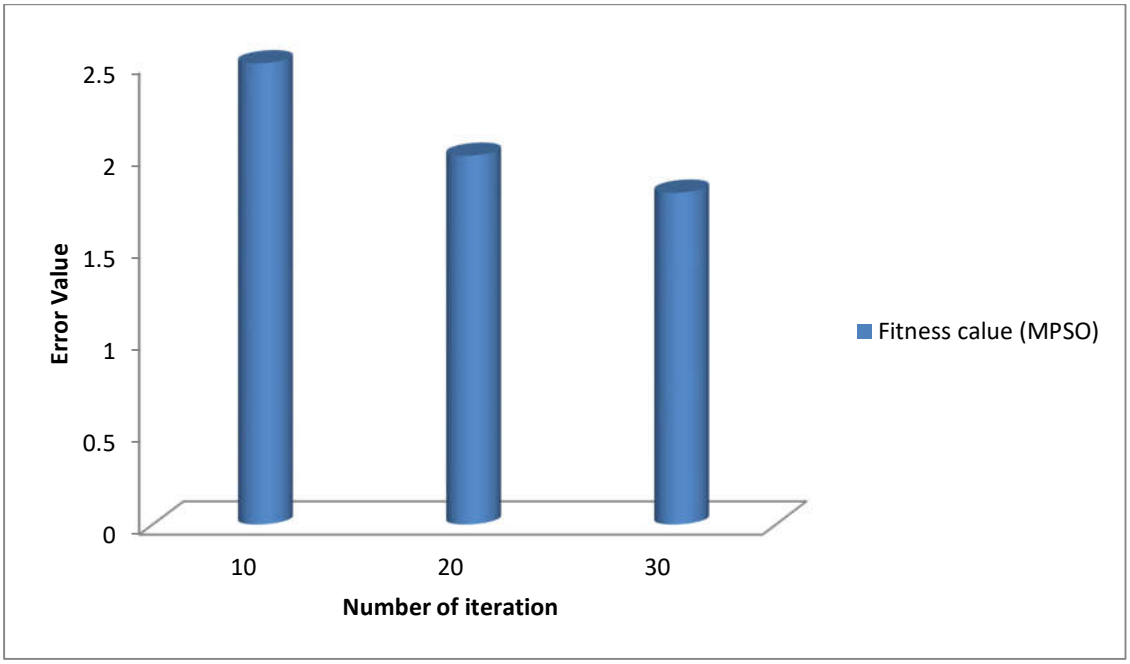

Figure 4: The proposed method's fitness value

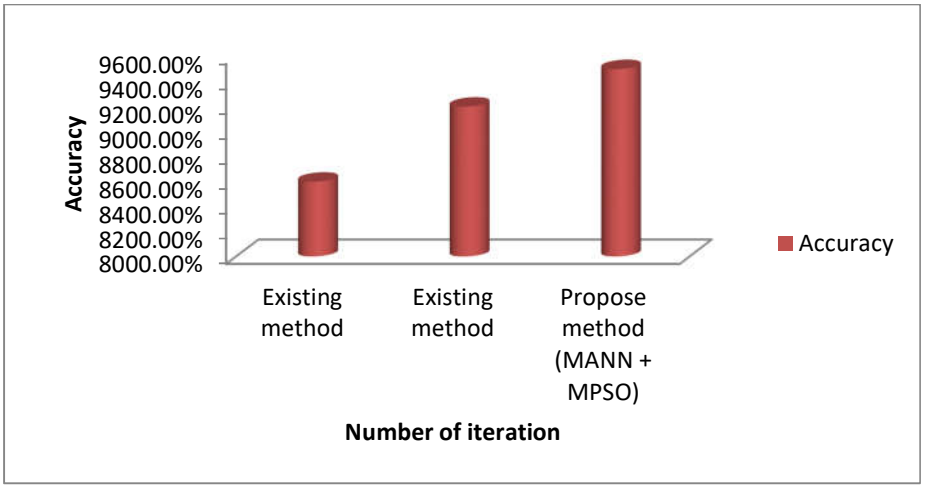

Figure 5: Precision score comparative graph

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.

Table 3 Comparison of percentage of attacks utilizing MIM and DoS attacks

File size, kb	**MIM**		**DoS attack**	
	Proposed method (RES + AES)%	Existing method (RSA) %	Proposed method (RES + AES)%	Existing 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

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 amount 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 Comparison of proposed and current solutions to major breaking times

File size, kp	Proposed method (RSA+AES)	Existing method (RSA)
10	131	122
20	136	126
30	115	97
40	137	13=

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.

5. Conclusions

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, we'll look at AI and safety could be combined. The topic of cloud-based Network Transport Networks was also brought up. Lastly, they talked about AI, safety, and the internet could be used to improve the Network of Transport Systems. Protecting the Internet of Transport Networks, they've 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.

References

[1] Ruth, J. A., Sirmathi, H., & Meenakshi, A. (2019). Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks. *IET Information Security*, *13*(4), 321-329.

[2] Alabi, O., Gabriel, A. J., Thompson, A., & Alese, B. K. (2022). Privacy and Trust Models for Cloud-Based EHRs Using Multilevel Cryptography and Artificial Intelligence. In *Artificial Intelligence for Cloud and Edge Computing* (pp. 91-113). Springer, Cham.

[3] Vähäkainu, P., & Lehto, M. (2019, February). Artificial intelligence in the cyber security environment. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019* (p. 431). Academic Conferences and publishing limited.

[4] Chen, Y., & Chen, Z. (2021, June). Preventive Measures of Influencing Factors of Computer Network Security Technology. In *2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)* (pp. 1187-1191). IEEE.

[5] GÜRFİDAN, R., & ERSOY, M. (2020). A New Hybrid Encryption Approach for Secure Communication: GenComPass. *International Journal of Computer Network & Information Security*, *12*(4).

[6] Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2019). Reducing the required time and power for data encryption and decryption using K-NN machine learning. *IETE Journal of Research*, *65*(2), 227-235.

[7] Balamurugan, K., Uthayakumar, M., Sankar, S., Hareesh, U. S., & Warrier, K. G. K. (2018). Preparation, characterization, and machining of LaPO4-Y2O3 composite by abrasive water jet machine. *International Journal of Computer-Aided Engineering and Technology*, *10*(6), 684-697.

[8] Deepthi, T., Balamurugan, K., & Uthayakumar, M. (2021). Simulation and experimental analysis on cast metal run behavior rate at different gating models. *International Journal of Engineering Systems Modelling and Simulation*, *12*(2-3), 156-164.

[9] Balamurugan, K. (2020). Metrological changes in surface profile, chip, and temperature on end milling of M2HSS die steel. *International Journal of Machining and Machinability of Materials*, *22*(6), 443-453.

[10] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover the Internet of things*, *1*(1), 1-14.

[11] Jayanthi, P., & Iyyanki, M. (2020). Cryptography in the Healthcare Sector With Modernized Cyber Security. In *Quantum Cryptography and the Future of Cyber Security* (pp. 163-183). IGI Global.

[12] Putra, S. D., Sumari, A. D. W., Ahmad, A. S., Sutikno, S., & Kurniawan, Y. (2020). Cognitive artificial intelligence countermeasure for enhancing the security of big data hardware from power analysis attacks. In *Combating Security Challenges in the Age of Big Data* (pp. 61-86). Springer, Cham.

[13] Hidayat, T., & Mahardiko, R. (2020). A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. *International Journal of Artificial Intelligence Research*, *4*(1), 49-57.