
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

Security Solutions for Data Encryption with AES Based on Artificial Intelligence

[1] Medikonda Saigopi, [2] Palle Nistha, [3] Nomula Nikhilsai, [4] Rajput Rahul, [5] Pujari Pranaya, [6] Dr. D. Bhadru, [7] Mr. V. Prashanth,

[1,2,3,4,5]UG Scholar, Dept. of CS, Narsimha Reddy Engineering College, Maisammaguda, Kompally, Secunderabad, India.

[6] Professor, Dept. of CSE, Narsimha Reddy Engineering College, Maisammaguda, Kompally, Secunderabad, India.

[7] Assistant Professor, Dept. of EEE, Narsimha Reddy Engineering College, Maisammaguda, Kompally, Secunderabad, India.

Abstract—

The transportation business is greatly affected by the Internet of Things (IoT). The original aim of developing autonomous vehicles (AVs) was to facilitate common tasks like delivery of goods and services and traffic flow. Vehicles on land, in the air, and at sea were all part of the AVs, which served several purposes. To address this issue, they established the Cyber Security (CS) enabled data transmission autonomous driving. As a go-between, a network transfers transmitter data to the driverless vehicle. Data that is transferable to cypher text is encrypted using the CS-based technique Advanced Encryption Standard (AES) for further security. The transmitter provides the unique AV with a secret key that, when used, decrypts the encrypted material. An ordinary neural network would be tweaked using optimized particle swarm efficiency. Decrypting the document using dual encryption techniques should be the last step of the researchers' suggested offering. The retention safety of the suggested approach is enhanced using steganography techniques after the dual cryptography. They used online simulation to put their plan into action in the Java development environment.

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

I. INTRODUCTION

The creation of AVs has skyrocketed in the last several years. Businesses were very interested in AVs. A wide array of sensors allows AVs to assess their surroundings. There is much potential for AVs to improve transportation, but there are new issues with security and privacy that need to be addressed [1]. It was feasible to tamper with the detectors maliciously. Vehicles should verify the veracity of sensor signals before acting upon them. Many different types of AVs make up the Internet of Transportation (IoT) systems that make up the Network of Transportation Infrastructure. There was talk of attacks on the transportation network's infrastructure [2-4]. Technologies such as autonomous and, eventually, driverless cars were able to retrieve data in real time. Energy efficiency is a must for electricity transport networks. Problems with the security of these networks might lead to catastrophic consequences, such as accidents, deaths, and being stuck on isolated roads because of attacks on power control. It would be challenging to apply stream analytics/learning techniques to transport information, even if data science/ML approaches are being utilized to investigate AV data [4].

Avs uses machine deep learning to process the massive amounts of sensor data it collects. Data science, artificial intelligence, and machine learning would form the backbone of the Internet of Transport Networks, powering a plethora of useful applications [5]. In order to defeat the machine learning algorithm, the opponent would study it. The Network of Transport Networks gathers a lot of data, yet people still need their privacy protected [6]. According to the researchers, the majority of the data interchange and monitoring should be done via cloud-based technologies in conjunction with the Network of Transport Network. Not only do car sensors pose a threat to the automotive ecosystem, but there are other weak points as well. Vehicles and automobiles without human drivers are now out on the road, gathering data about the road network to upload to the cloud. Thanks to over-the-air updates, car manufacturers may remotely deploy repairs and software upgrades. On the other hand, this poses a security risk as even a single incorrect patch has the potential to render the system inoperable and muddled [7] [8]. The remote start

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

and distribution of these updates poses a serious risk of exploitation if the security posture is not properly established [9]. According to the research in [10], gateway Electronic Control Units (ECUs) with Physically Unclonable Functions (PUFs) can decode over-the-air (OTA) updates that the Original Equipment Manufacturer (OEM) receives. The supply chain is essential to the assembly of every vehicle and must thus be protected. Since many different companies manufacture different parts for vehicles, an attack targeting one of these original equipment manufacturers (OEMs) might lead to problems. One way original equipment manufacturers (OEMs) may avoid these kinds of problems is by creating cybersecurity guidelines for third-party items. For instance, before mass production begins, OEMs and third-party manufacturers may work closely together to identify any design issues with the essential components

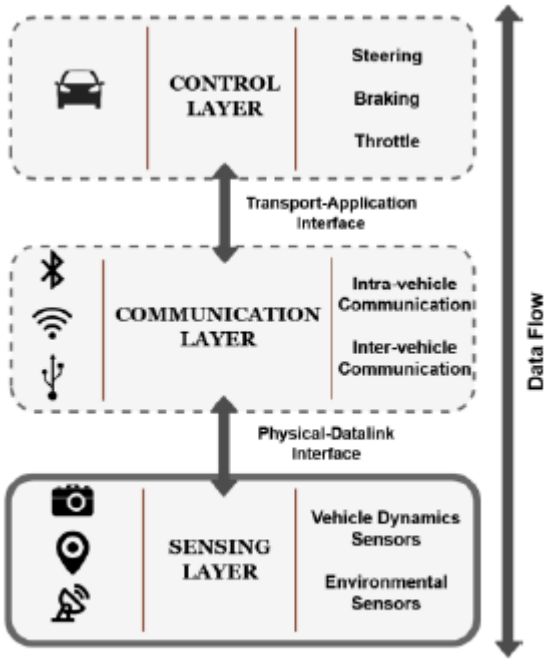

Fig. 1. Three Layer Architecture

Internet of Things (IoT) applications in vehicle security for risk classification have a hierarchical structure, as shown in Figure 1. The first level of the hierarchy, the sensing layer, is sometimes called the AutoVSCC (Autonomous Vehicular Sensing Communication and Control) framework [11]. It is composed of the sensors used in cars. Ultrasonic sensors, Global Positioning Systems (GPS), and Tire Pressure Monitoring Systems (TPMS) may all be tricked into picking up on objects that aren't really present. From the physical datalink interface, dangers may go to the communication layer, where they can convert the analogue data collected by the sensors into digital data that can be used for communications inside and between vehicles. Cybersecurity flaws in the communication layer include the ability to intercept messages sent between cars, transmit fake signals within a vehicle (via its communications buses), and even take over the vehicle itself. The ability of the control layer to transform digitally rich data into real-time automotive applications like as automatic steering control, lane change maneuvers, and brake application might be hindered by threats at the communication and sensor layers. The transport-application interface makes this possible.

II. LITERATURE REVIEW

One problem with traditional IDS approaches is the high frequency of false reports, which leads to the unnecessary intervention of human operators [12]. In order to determine the nature of alerts and take appropriate action, human analysts routinely do in-depth assessments. By integrating K-means and fuzzy neural networks, the suggested solution successfully eliminates the need for human assessment interaction. The technique was tested with a range of background knowledge sets using DARPA internet traffic samples [13]. There was a notable improvement in the

ability to gather attack particles that were consistent with the training data, and the real results showed a considerable decrease in erroneous reports. Customers may now browse across many sets of IDSCs simultaneously, blending product attributes for a more unified IDS approach, thanks to the extensible nature of the integrated approach [14]. In thrilling situations, a single identical structure may display the many access point procedures on faraway structures, creating consensus on the acquisition of the IDS result [15]. The idea worked on the home PC after running a simplified version of the suggested program. They overcame the challenges of the virtualized environment by discussing and experiencing various problems, activating the IDSs, and implementing them on the cloud. In addition, they made a compelling case for internet-wide, multi-attack-resistant concealed intrusion detection systems [16]. Their first intrusion detection system (IDS) included testing of both performance and skill levels to guarantee the safety of their cloud [12–13]. They envisioned a pair of straightforward intrusion detection systems, with the hope that one might compensate for the other's shortcomings [17][18]. In order to accomplish the efficiency of system resource allocation and the vitality of the security operation without adjustments, this research aimed to propose a cutting-edge approach that a cloud computing model may use. (1) and (2).

III. PROPOSED METHODOLOGY

Academics and businesses alike are showing an interest in cloud computing, although the idea is still in its early stages of development. One of the biggest problems with cloud computing was keeping user data safe. To improve memory security, they came up with a reliable method of transmitting highly secure storage data to the cloud. The goal of this study is to find malicious software in cloud data using a tailored ANN. The optimization approach was used to update the traditional NN. A tailored particle swarm optimization technique is used in the suggested method for extensive updating. The customer wants to examine the storage server penetration before deciding to store the data in the cloud. The use of encryption to safeguard the file during storage was our suggested course of action. The suggested solution was decrypted using two separate cryptographic methods. A method using two algorithms might be considered secure.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

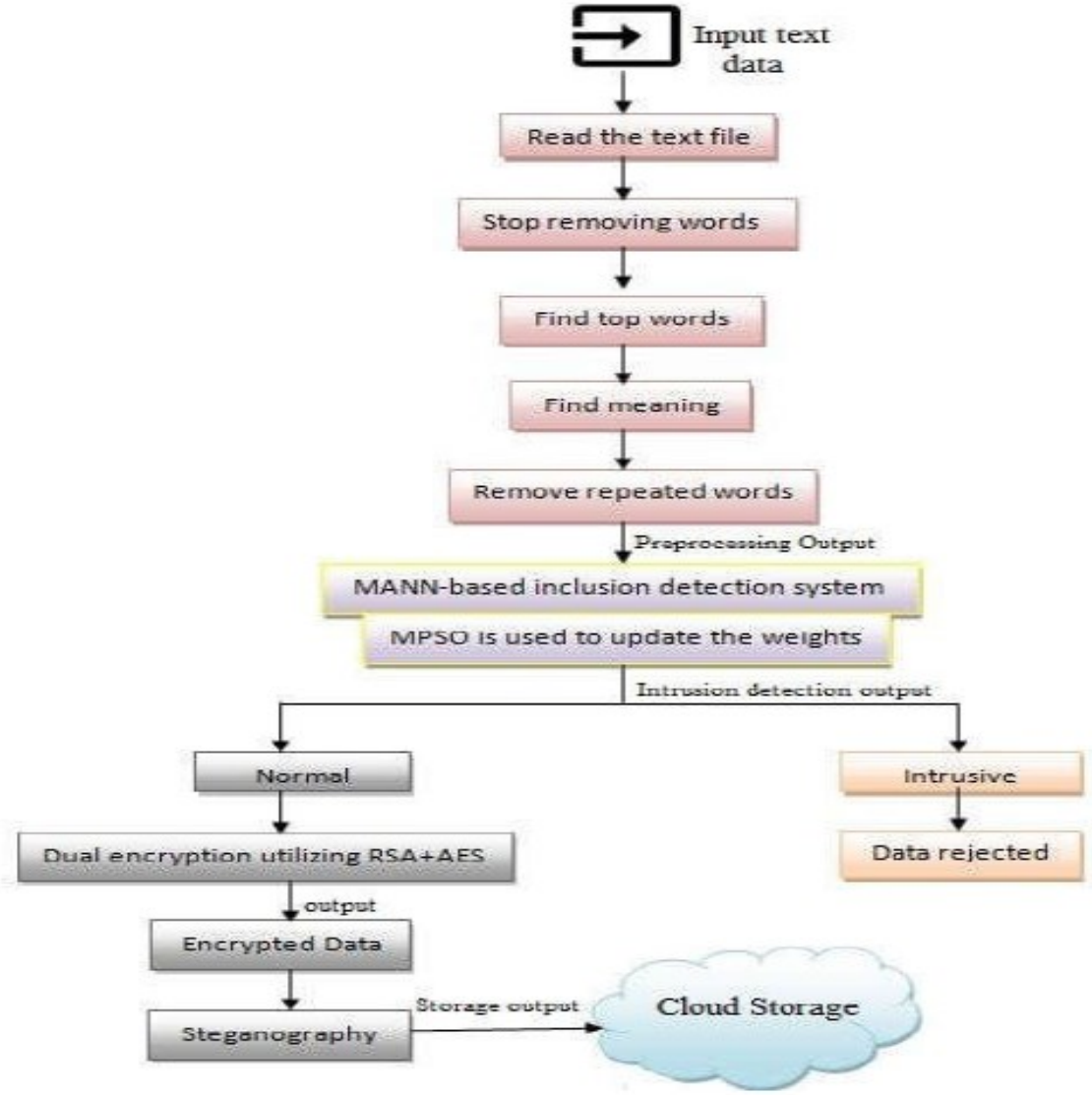

Fig. 2. Proposed Methodology

A. Description of AES Algorithm

For block ciphers with a 128-bit block size, AES is the way to go. Key sizes of128,192, and 256 bits are all on the table. Designers advise using a key size of 512 bits for AES. Encryption for 512-bit secrets consists of ten computation rounds. Aside from the last round, the rest of the rounds in both scenarios were the same. A 4-by-4-byte matrix was constructed from an input message with 512 bits to act as the state array. Using 512-bit input blocks and keys, the new method increases the allowed area and makes it more resistant to cryptanalysis. Applications with space constraints and a need for high levels of security might benefit from AES-512. The organizational outputs, or states, are affected by the transformations; a state is just a rectangular array of bytes. The input state is XORed with the first four components of the schedule before round-based encryption operations may take place. There was an indication of the present status of the intended work at the page's footer. At the beginning of the following section, the suggested work's critical function was computed. Each column is treated as a four-term polynomial in the state-by-column combination conversion. Throughout several cycles, the aim of the phase should be to spread the pieces uniformly. This is accomplished by multiplying each column individually. Each column signal in a conventional matrix is computed using the values of each row. Submit a circular cover

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

letter: The round secret is attached to the area to be added using bitwise XOR. The cypher key might be converted into a round secret using a secret schedule.

IV. RESULTS AND DISCUSSION

In the chapter that follows, we examined how well the method we designed worked. Table 1 shows the timings for decrypting and encrypting different document types. The following file sizes are often used by designers: 10, 20, 30, and 40 kb. The document size and encoding time are both affected by the use of dual encryption; for example, a 10 kb document takes 5.796 seconds to encrypt. The encryption process for the 10-kilobyte file takes 5.796 seconds, while the decryption process takes 5.123 seconds. Time required to encrypt and decode files of 20, 30, and 40 kb in size, for example, varies. Encoding a 20-kilobyte file takes 9.864 seconds while decoding it takes 8.457 seconds. All of the storage values and processing times for the suggested strategy's method are shown in Table 1. We computed the processing time and storage amount after varying the number of observations. Figure 2 displays the values of the processing time, storage amount, and number of iterations in a chart format. The graph was shown in the section that followed.

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

The suggested method achieves a memory storage amount of 13,598,247.75 bits by modifying the number of bullets. The overall execution time of the optimization techniques is 21,008 milliseconds. By changing the amount of repetitions, Figure 3 shows how the system performs using the proposed approach. Figure 4 displays the fitness value of the suggested method. As far as the MPSO was concerned, the message with the lowest error rate was considered to have the best fitness value. In this scenario, the efficiency score decreases as the quantity of observations increases. The full classification validity of the suggested back-propagation method based on MANNs is shown in Table 2. In this example, the suggested MANN achieves an accuracy of 91.25 percent.

TABLE II. ACCURACY OF PROPOSED MODEL

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

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

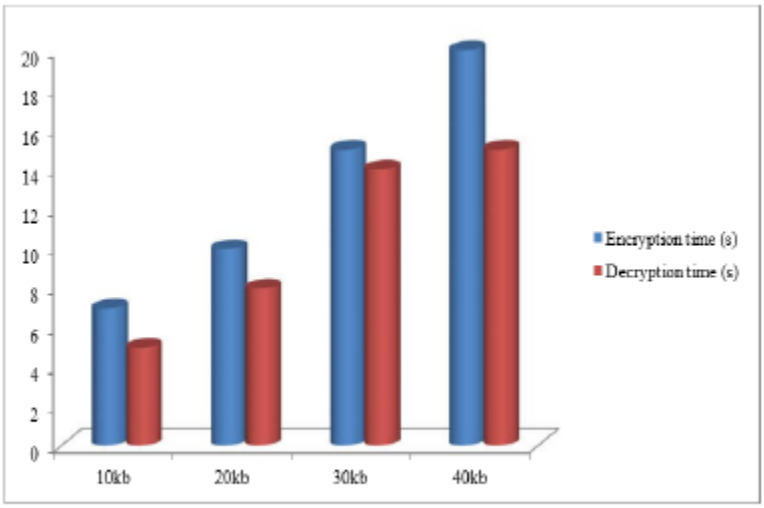

Fig. 3. Encryption and Decryption Frequency

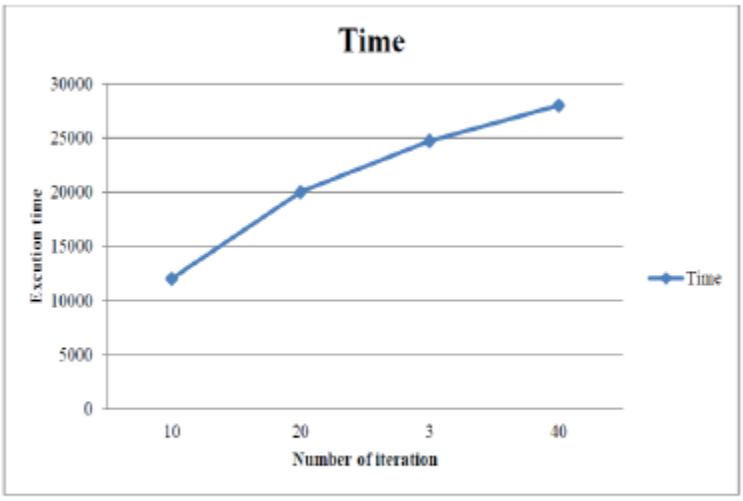

Fig. 4. Computational Time of Proposed Model

The most crucial aspect of IDS was categorization performance. This study compares accuracy values using existing intrusion detection techniques, which is crucial for the strategy to have a better precision score in order to be deemed competitive. To the contrary, we shall use present-day malware detection as an evolutionary method and current-day intrusion detection systems as a traditional NN. According to the data in the chart, the current technique had a classification performance of 85.7%, the suggested methods of 91%, and the recommended procedure of 93.46%. It would seem that the suggested product is better than current procedures due to its high efficacy.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

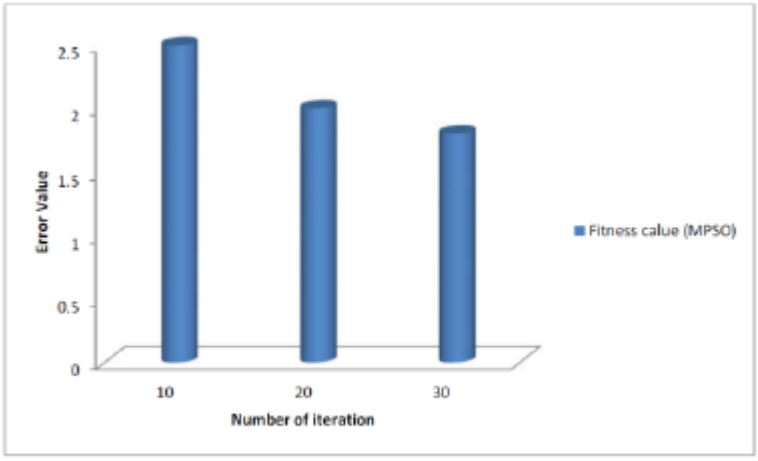

Fig. 5. Fitness Value of Proposed Model

In order to ensure the safety of the provided approach, several security risks are tested. They were launching a denial-of-service attack and a MiM assault simultaneously. To be effective, an encryption procedure must reduce the impact of attacks on the data to a minimum, making it more secure while yet allowing for limited access. The suggested approach outperforms all prior methods, regardless of their flaws. Table 3 shows a comparison of current and planned methods against various attacks, such as MIM and DoS attacks. The attack rate is greater in traditional systems and lower in detecting techniques. No matter what kind of attack is being considered, the suggested approach would safeguard the data better than the present methods.

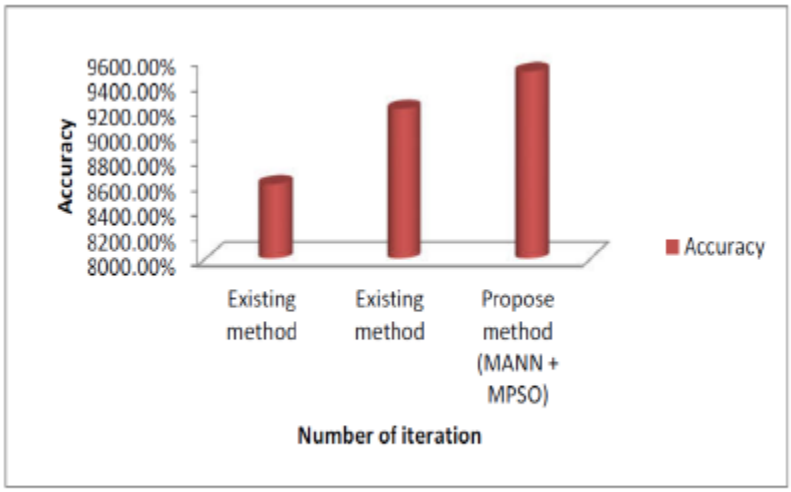

Fig. 6. Accuracy of Proposed Model

We contrast the current approach with the one that has been suggested. According to the data in the table, the suggested technique took more time to shatter secrets than the usual approaches did to break them significantly. In a 10 kb document area, the current system tries 120 times to attain the key score, whereas the suggested approach tries 128 times. While the current system tries 123 times—the smallest number of instances compared to a created method—to get the secret score of a 20 kb text, the suggested technique tries 132 times. In a similar vein, the current approach breaks the principal value of fo4 30 and 40 kb 129 times, whereas the suggested strategy breaks it 112 and 136 times, respectively. Therefore, the most stringent safety measures are provided by the suggested solution. It seems that the suggested strategy is more effective and safer than existing approaches when it comes to intrusion prevention. The projected performance is being assessed by researchers using the KDD database. The findings have been compared to current academic work. Fuzzy C-means, artificial neural networks (ANNs), and a hybrid

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

approach are being used by researchers to assess the present structure. The results are summarized in Table 4. The root value of the squared error indicates the efficacy of the suggested method, while the kappa statistic indicates the severity of the error. We have totaled the results. The median information rate for encryption was low when compared to DES of encoding and decoding. The suggested hybrid method would reduce storage requirements for encryption and decryption processes. The amount of data encrypted or decrypted each second is called the median data rate. The results clearly demonstrate that the suggested technique outperforms the other alternatives.

V. CONCLUSION

This research delves into the characteristics of AVs in the context of the Internet of Transport Systems, as well as the privacy and security issues plaguing platforms. After that, we can integrate AI with safety features. Also mentioned were Network Transport Networks on the cloud. Finally, the Network of Transport Systems might be enhanced with the use of internet, safety features, and AI. The surface level of protecting transportation networks on the internet has only barely been scratched. Research into the many types of tracks and the development of machine learning techniques are necessary for the detection and mitigation of attacks. Assaults on machine learning methodologies should be considered by researchers as they seek to construct Smart Network of Transport Networks. Finally, they need to figure out what data to send via the secure internet in order to compile 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 dat a storage and intrusion detect ion in the cloud using MANN and dual encryption through various attacks," IET Informat ion Security, vol. 13, no. 4. Inst itut ion 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 Mult ilevel Cryptography and Art ificial Intelligence,” Int ernet of Things. Springer International Publishing, pp. 91–113, 2022. doi: 10.1007/978-3-030-80821-1_5.

[3] J. Jain, “Art ificial Int elligence in the Cyber Security Environment,” Art ificial 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 evaluat ion based on image recognit ion and neural network,” Journal of Elect ronic Imaging, vol. 32, no. 01. SPIE-Int l Soc Opt ical Eng, Sep. 15, 2022. doi: 10.1117/1.jei.32.1.011214.

[5] S. Gadde, J. Amutharaj, and S. Usha, “A securit y model to protect the isolat ion of medical data in the cloud using hybrid cryptography,” Journal of Informat ion Security and Applicat ions, 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 Encrypt ion and Decrypt ion 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. Garikapat i, K. Balamurugan, and T. P. Latchoumi, “&lt ;i&gt ;K</i>-means part itioning approach to predict the error observat ions in small dat aset s,” 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 experiment al analysis of re-design the faulty position of the riser to minimize shrinkage porosity defect in sand cast sprocket gear,” Materials Today: P roceedings, vol. 59. Elsevier BV, pp. 598–604, 2022. doi: 10.1016/j.matpr.2021.12.090.

[9] E. Alt ayef, F. Anayi, and M. P ackianather, “A new enhancement of the k-NN algorithm by Using an opt imizat ion t echnique,” 2022 2nd Internat ional Conference on Advance Comput ing 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 Int ernet of Things (IoT) cybersecurit y,” Discover Int ernet 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, “ St udy of various met hods for reliable, efficient and Secured IoT using Art ificial Int elligence,” SSRN Electronic Journal. Elsevier BV, 2022. doi:10.2139/ssrn.4020364.

[12] P. Nirmala, S. Ramesh, M. Tamilselvi, G. Ramkumar, and G. Anitha, “An Art ificial Intelligence enabled Smart Indust rial Automat ion System based on Internet of Things Assist ance,” 2022 Internat ional Conference on Advances in Comput ing, Communication and Applied Informat ics (ACCAI). IEEE, Jan. 28, 2022. doi: 10.1109/accai53970.2022.9752651.

[13]S. D. Putra, A. D. W. Sumari, A. S. Ahmad, S. Sut ikno, and Y. Kurniawan, “ Cognit ive Art ificial Int elligence Count ermeasure for Enhancing the Security of Big Data Hardware from Power Analysis Attack,” Advanced Sciences and Technologies for Security Applicat ions. Springer International Publishing, pp. 61–86, 2020. doi: 10.1007/978-3-030-35642-2_4.

[14] H. Sharma and N. Kumar, “ Deep learn ing based physical layer security for terrest rial communicat ions in 5G and beyond networks: A survey,” Physical Communicat ion, 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 t rustworthy medical art ificial 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, “Implement at ion of a block cipher algorithm for medical information security on cloud environment : using modified advanced encrypt ion st andard approach,” Mult imedia Tools and

Applicat ions. 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 Informat ion 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, “ SACFIIoT: Secure Access Control Scheme for Fog-Based Indust rial Internet of Things,” in IEEE Global Communicat ions 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 Authent icated 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 encrypt ion using AES algorithm," Second Internat ional Conference on Current Trends In Engineering and Technology - ICCTET 2014, Coimbatore, India, 2014, pp. 332-337, doi: 10.1109/ICCTET.2014.6966311.