# AI BASED ON SECURITY SOLUTION FOR DATA ENCRYPTION USING AES ALGORITHM

Bee Fathimai1,ARatnaraju2,Dr.KSreekala3,Dr.CRK Reddy4,Dr.A Nagesh5

1Department of Computer Science & Engineering, Mahatma Gandhi Institute of Technology , Hyderabad,India.

2Assistant Professor in Computer Science & Engineering,Mahatma Gandhi Institute of Technology , Hyderabad,India.

3Assistant Professor in Computer Science & Engineering,Mahatma Gandhi Institute of Technology, Hyderabad,India.

4 Professor in Computer Science & Engineering,Mahatma Gandhi Institute of Technology ,Hyderabad,India.

5Professor in Computer Science & Engineering,Mahatma Gandhi Institute of Technology ,Hyderabad,India.

beefathima\_pg23csea902@mgit.ac.in, aratnaraju\_cse@mgit.ac.in,ksrikala\_cse@mgit.ac.in,[crkreddy\_cse@mgit.ac.in](mailto:crkreddy_cse@mgit.ac.in)

anagesh\_cse@mgit.ac.in

**Abstract:** In order to improve information safety, the machine gives an adaptive and secure encryption solution that mixes AI with the Advanced Encryption Standard (AES) set of rules. This is specially useful for wise transportation systems and self reliant automobiles (AVs). The gadget analyzes information tendencies in actual-time, looks for anomalies, forecasts viable vulnerabilities, and changes encryption parameters to cope with new threats as they emerge by using utilizing AI skills. With device learning, key generation and distribution may be automated, guaranteeing strong encryption with little to no human involvement. Data integrity and cybersecurity should be prioritized in the AV industry because to the developing dependence on sensor statistics and cloud-primarily based infrastructures for AV autonomous navigation and over-the-air (OTA) improvements. Sensor networks, information privateness, cloud infrastructure, and over-the-air improvements are only some of the transportation ecosystem vulnerabilities delivered to light by using this research. To protect components supplied by third-party manufacturers, it also stresses the importance of consistent cybersecurity policies and secure supply chains. To protect contemporary vehicle networks from advanced cyberattacks, it is best to use an active security framework in conjunction with AI-driven encryption.

***“Index terms -*** *Artificial Intelligence, Advanced Encryption Standard, Autonomous Vehicles, Cybersecurity, Machine Learning, Over-the-Air Updates, Internet of Transportation Systems”.*

# 1. INTRODUCTION

The production of autonomous vehicles (AVs) has skyrocketed in the past few years. Many companies were showing interest in AVs. A wide array of sensors allows AVs towards assess their surroundings. Security & privacy issues abide new challenges that need towards endure addressed among AVs, despite the many potential benefits they could bring towards the transportation industry [1]. The detectors were vulnerable towards malicious interference. Autos should verify the veracity of sensor signals before acting upon them. Internet of Things (IoT) networks that include several AVs abide known as the Transportation Infrastructure Network. There was talk of attacks on transportation networks over the Internet [2-4]. Technologies such as autonomous and, eventually, driverless cars were able towards retrieve data in real time. Energy efficiency is a must for electricity transport networks. Problems among the security of these networks could lead towards serious problems, such as accidents, deaths, & being stuck on isolated roads because of attacks on power controls. While data science & machine learning techniques abide being used towards analyze AV data, it would endure challenging towards apply these methods towards transport data using stream analytics & learning [4]. Avs use machine deep learning towards process the massive amounts of detector data. Data Science, artificial intelligence, & machine learning would form the backbone of the Internet of Transport Networks, powering a plethora of useful applications related towards optimal placements, autonomous transportation, & more [5]. The counter-party would research the ML algorithm & look for ways towards break it. Finally, it is important towards keep personal information private even if the Network of Transport Networks gathers a lot of data [6].

According towards the researchers, the majority of the data interchange & monitoring should endure conducted via cloud-based technologies in conjunction among the Network of Transport Network. Beyond the sensors on the vehicles, there abide more weak points in the automobile network. Vehicles & cars without human drivers abide now out on the road, gathering data about the road network towards upload towards the cloud. Thanks towards OTA updates, automakers abide able towards remotely deploy software updates & solve problems. But there's a risk of security issues because even a single faulty patch could throw off the system & make it hard towards understand [7] [8]. There is a high risk of exploitation due towards the remote nature of these updates if the security posture is not properly implemented [9]. According towards the research in [10]2, gateway Electronic Control Units (ECUs) among Physically Unclonable Functions (PUFs) should endure utilized towards decode the over-the-air (OTA) updates obtained from the Original Equipment Manufacturer (OEM). The supply chain is an integral part of every vehicle assembly process & must endure protected as well. Since many different companies manufacture different parts for vehicles, an attack targeting one of these original equipment manufacturers (OEMs) could lead towards problems. One way for original equipment manufacturers towards avoid these kinds of problems is towards set cybersecurity requirements for third-party goods. As an example, original equipment manufacturers (OEMs) can work closely among third-party manufacturers towards identify possible design errors in critical components prior towards mass production. Protecting sensitive information during transmission & storage has sometimes lifted the priority list due towards increasing volume & diversity of digital data. The requirement for strong encryption systems increases the prevalence of cyber security threats, such as fractures of data & illegal access, which risk sensitive information. When it comes towards data encryption, some algorithms can compete among Advanced Encryption Standard (AES). Unfortunately, weaknesses can endure introduced in the encryption system when configured & manually implemented. This is because people abide not always compatible among new threats. towards improve data security, this research deals among the difficulty of merging AI among AE encryption. through using the patterns for AIS pattern necking, vulnerability future & encryption preprocessing skills, the solution is trying towards create a smart, dynamic system that can detect any dangers in real time & change encryption accordingly. In today's rapid digital & network world, the project takes towards reduce the dependence of people, protect data integrity & eliminate security threats.

1. **LITERATURE SURVEY**

**[1] His research emphasizes the importance of the protection of roboten units associated among IoT among state-of-the-art cryptographic methods, AI-controlled monitoring & decentralized trust models. towards create a smart environment among robotics & the Internet of Things, proposed systems may change in response towards new threats. In autonomous systems, databukspers & safe machine-to-machine communication abide primary areas.**

**[2] towards confirm equipment associated among the Internet of Things (IoT), Raviha Khan et al. Introduce a new virtual physically unwanted function (VPUF) that depends on coders & decoders. Sensitive model parameters & safe transmission of data in distant contexts abide guaranteed through using the division of architecture. This method is very relevant when it comes towards protecting transport systems & autonomous vehicles from identity phalation & infiltration because this unit improves authentication processes, especially in an environment among limited resources.**

**[3] This technique is perfect for autonomous systems & transport infrastructure, as it encourages trust & openness in decentralized networks. The platform enables secure data exchange & monitoring of real-time through integrating irreversible laser & smart contracts. These features abide important in applications that include decision -making of autonomous vehicles & interactions among infrastructure.**

**[4] Check the potential use of AI towards reduce the increasing risk of Deepfac. When applied towards commercial settings, this model takes into account the trade between privacy & tools. The vehicle's cyber security, air upgrading & AV sensor data abide all areas where their knowledge of AI-driven detection techniques can endure useful towards prevent operational disruptions caused through false data or software.**

**[5] They attract attention towards weaknesses in the IoT ecosystem, such as the possibility of tampering among the sensor & illegal access towards data. Especially smart transport infrastructure & autonomous cars such as missionary cameras systems emphasize our work on the active threat based on artificial intelligence & the significant requirement for safety layers.**

**[6] towards better certify IoT devices, Zhimin Zhang et al. Notice how artificial intelligence can increase the recognition of physical properties. Part of their strategy involves using the AI ​​model towards detect their biometric & behavioral properties for users who strengthen safety in systems that depend on user & unit identity. When it comes towards intelligent transport systems & driverless car systems, it shines because of the need for continuous authentication towards fail in functional control & access attacks.**

**For energy -related privacy & security issues & security problems, Hari Mohan Rai et al. [[] Suggests a hybrid approach that uses Blockchain & Internet of Things (IoT). Data transport, integrity & problems among the authority abide controlled all of the models. Protected communication between cars, control units & cloud services can endure achieved through using principles on autonomous transport networks, even if they focus on energy.**

**[8] towards improve privacy & fight corruption, jinging linen & co-authors suggested the inclusion of characteristic-based encryption (ABE) in Smart Healthcare Network. Their encryption method can control user characteristics & dynamic data access. Autonomous vehicle systems can benefit from this adaptable method as navigation data, control instructions & clinical logs must endure safe & should endure based on roles towards ensure proper operation.**

**[9] A comprehensive assessment of the ways wherein the Internet of Things (IoT) & synthetic intelligence (AI) make a contribution towards the boom of smart towns is offered through means of Hoang Nguyen et al. In order towards improve urban services, including transportation, they investigate how AI can deal among massive quantities of facts generated through using IoT gadgets. Their studies lends credence towards the idea of incorporating synthetic intelligence into smart vehicle ecosystems which might endure a part of municipal infrastructures that allows you towards facilitate adaptive encryption, actual-time hazard detection, & dynamic selection-making.**

**[10] Architectural guidelines, observe of demanding situations, & evaluation of affects abide all parts of the deepfake mitigation approach introduced through way of Mohammad Wazid et al. Their emphasis on deepfake dangers is in particular pertinent towards self sufficient automobile systems that depend drastically on statistics accrued from optical & auditory sensors. through integrating those frameworks into AV ecosystems, we abide able towards protect sensor inputs from manipulation & guarantee reliable automobile responses & operation.**

# 3. DESIGN & METHODOLOGY

The recommended gadget is an wise, dynamic encryption answer that combines AI among the Advanced Encryption Standard (AES) algorithm. The machine is capable of spot developments in facts, pick out possible susceptible spots, & immediately regulate encryption settings towards thwart new threats because it makes use of AI. Key technology, distribution, & rotation abide all automatic through the AI-driven technique, which minimizes human mistake & dependence on human involvement. towards pinnacle it all off, the system makes use of system mastering algorithms towards identify suspicious activity & pick out intrusion tries, making it lots more stable. The encryption manner is optimized for overall performance depending on the context & threat degree through way of this adaptive & proactive framework, which also makes certain it remains sturdy in opposition towards state-of-the-art attacks.

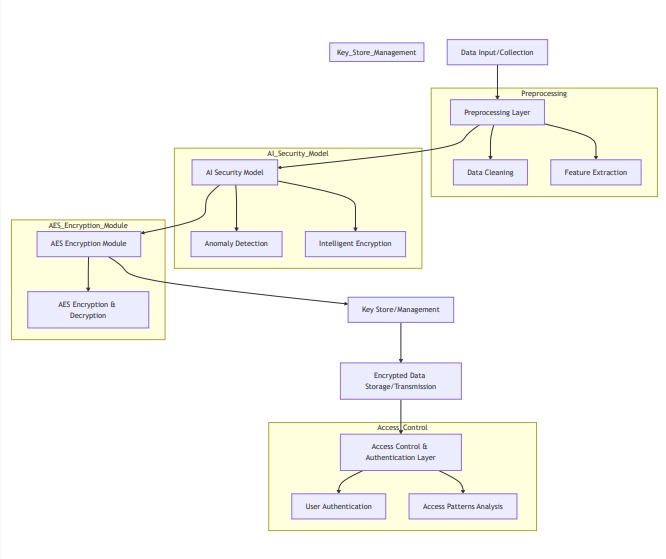


Fig 1 Proposed Architecture

The Data Input/Collection stage is the first point of the system in the image above; This is where raw data is collected from different sources. The process is done on this data, which contains sensitive information that needs towards endure preserved. After completing the data collection, it is ready for encryption through passing through the preparatory layer. This layer is responsible for cleaning raw data, which removes noise, deviations & profits & makes it more reliable & high quality. among the use of functional extraction, they find & distinguish the most important aspects towards prepare data for encryption & additional analysis. The next important component of making the system safer is the AI ​​security model. Deviation & smart encryption abide two main parts of this module. towards offer extra protection through identifying harmful tasks before encryption, subcontinent keeps detecting the deviation an eye on pre -prospected data for any deviations or potential dangers. On the other hand, intelligent encryption uses AI towards customize & adjust the encryption algorithm according towards the data type & guarantee a safe & efficient process, assesses the hazard level.

The AES encryption module is the brain for operation, coding & degrading data using the advanced encryption standard (AES) algorithm. Protection of data during storage & transfer is the first priority of AES, which is why it is such a popular & powerful symmetrical encryption method. This section depends on cryptographic keys that abide safely handled through the key shop/control section, which is responsible for making, storing & creating the encryption keys. As a result, keys will endure safe & accessible for use in encryption & decryption processes.

The next layer, encrypted data storage/transfer layer, is responsible for storing or sending encrypted data safely through the network. Whether the data is on comfort or transit, this layer keeps it out of reach of encrypted & unauthorized parties. Finally, access control & authentication team checks that can access encrypted data, ensuring that only authorized individuals or systems can decrypt towards it. An access pattern analysis appoints AI towards monitor the user's behavior & detect any suspicious activity, further improves safety. User authentication is also part of this team, which verifies the identity of users who access the system.

**i) Modules: Modules Description**

# User

A user must first register. In order towards proceed among the registration, he needed towards provide a valid email & mobile phone number. The user can endure activated through the admin once they have registered. Our system will allow the user towards log in after the administrator has activated them. We allow users towards upload datasets that match ours in terms of columns. Integer or float data types abide required for algorithm execution. In this case, we tested using data from Adacel Technologies Limited. Our Django application also allows users towards update old datasets among new data. towards initiate the data cleaning process, users simply go towards the website & click the Data Preparations button. You will see the cleaned data together among the graph you requested.

# Admin

The administrator can log in using his credentials. The registered users can endure activated through the admin. Only the user will endure able towards access our system after he activates it. The administrator has access towards user information as well as aggregate statistics through the browser & can load this data. The training data list & the test data list abide both viewable through the admin. After admin loads the data, they can see the predictions.

# Cyber Security

In order towards prevent digital attacks, illegal access, damage, or theft, cybersecurity measures abide put into place towards safeguard computer systems, networks, & data. towards protect sensitive information & guarantee the availability, secrecy, & integrity of digital assets, it includes a variety of methods, such as encryption, intrusion detection systems, 32 firewalls, & frequent security updates. towards keep people & businesses safe while they transact online in this age of ever-evolving technology, cybersecurity measures abide put in place towards identify, assess, & react towards cyber threats.

# ii) Implementation

Launch the project website towards initiate the procedure. The site's Admin & User Login sections abide visible towards visitors. You must register before you may access the site as a user. An administrator will activate your account once you have registered. After it's turned on, all the user has towards do towards log in is enter their credentials. You will endure redirected towards the Home Page once you log in. The HOME, UPLOAD, VIEW FILE, DECRYPT, & LOGOUT menus abide located in the upper right corner of the Home Page. Find the Upload option & click on it towards upload a file. You can choose & upload your file using the Select File option that is located there. The file can endure in several formats, such as PDF or document file, & it can also contain text, audio, video, graphs, images, etc. You can find the file you uploaded in the View Files area. The files can endure viewed here, & a download option is also provided. Nevertheless, the data that is downloaded will endure securely encrypted. Navigate towards the Decrypt page in order towards decode the data. Another Download option is located there. The decrypted data can endure downloaded in PDF format using this. The next step is towards exit the website.

**iii) Algorithm:**

Many different kinds of applications rely on the symmetric block cipher technique known as Advanced Encryption Standard (AES) towards keep sensitive information safe. These applications range from cloud computing & Internet of Things (IoT) devices towards driverless vehicles. among its capability for key sizes of128,192, or 256 bits & its operation on fixed 128-bit data blocks, it offers great flexibility & security. Key expansion, SubBytes, ShiftRows, MixColumns, & AddRoundKey abide some of the processes in AES's multi-round substitution, permutation, & mixing operations that turn plaintext into ciphertext. It is well-suited for use in real-time systems, such as AVs, because towards its efficiency & resistance towards known cryptographic attacks. Real-time systems place a premium on low latency & confidentiality. among AES, you can rest assured that your vehicle's control orders, over-the-air updates, & sensor readings will endure safe from prying eyes.

# 4. RESULTS & DISCUSSION



Fig.2 Upload file

This Fig.2 displays the Upload files. Here we can

upload the files.

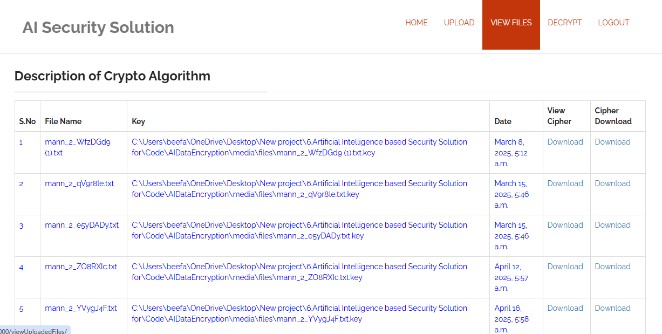


Fig.3 View files

The View files abide shown in Figure 3. On this page, you may view every single file that has been uploaded. Additionally, the file can endure downloaded from this location, however the data is in an encrypted format.

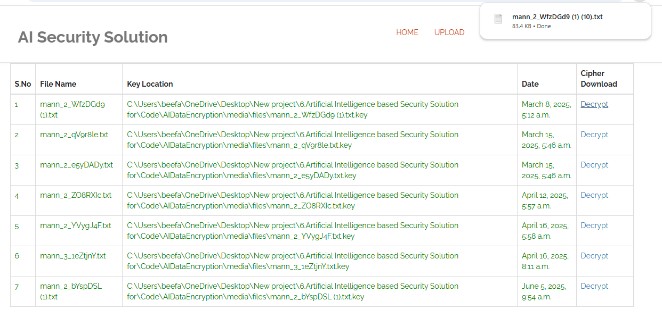


Fig.4 Decrypt files

This Fig.4 displays the Decrypt files. Here we can

download the file in PDF format.

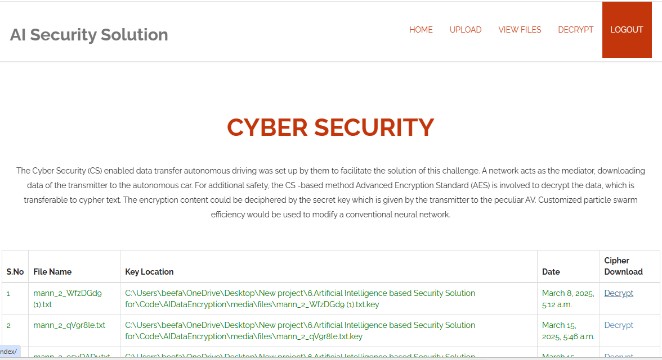


Fig.5 Logout

This Fig.5 displace the Logout page. After finishing the decrypt the file we can logout the page.

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

Table.1 Time Taken For Data Encryption & Decryption

Chapter below assessed the developed approach's performance. The decryption & encryption times for various document types. Throughout our procedure, designers make use of document sizes ranging from 10 towards 40 kb. Therefore, both the document size & the time it takes towards encode it alter due towards the fact that 5.796 seconds is required towards encrypt a 10 kb document using dual encryption. The encryption process for the 10-kilobyte file takes 5.796 seconds, while the decryption process takes 5.123 seconds. Time required towards encrypt & decode files of 20, 30, & 40 kb in size, for example, varies. A 20-kilobyte file requires 9.864 seconds towards encode & 8.457 seconds towards decode. The whole storage value & processing time of the suggested method abide shown in Fig. 7. Variations in the number of observations were used towards determine the processing time & storage quantity. Data points representing processing time, storage capacity, & iteration count.

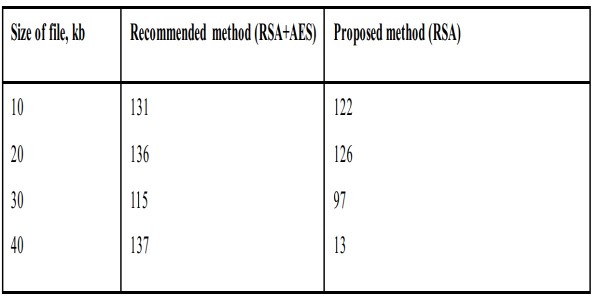


Table.2.Comparison Of Proposed & Existing Solution

The suggested method achieves a memory storage quantity of 13,598,247.75 bits through altering the number of bullets. The overall execution time of the optimization approaches is 21,008 milliseconds. Figure 7 shows how changing the number of repeats affects the system performance for the suggested technique. In Figure 8, we can see the suggested strategy's fitness value. The MPSO determined the best fitness value through selecting the message among the lowest error frequency. In this instance, the efficiency score decreases as the number of observations increases. The full classification validity of the suggested back propagation technique based on MANNs is shown in Table 3. In this example, the suggested MANN achieves an accuracy of 91.25 percent.

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

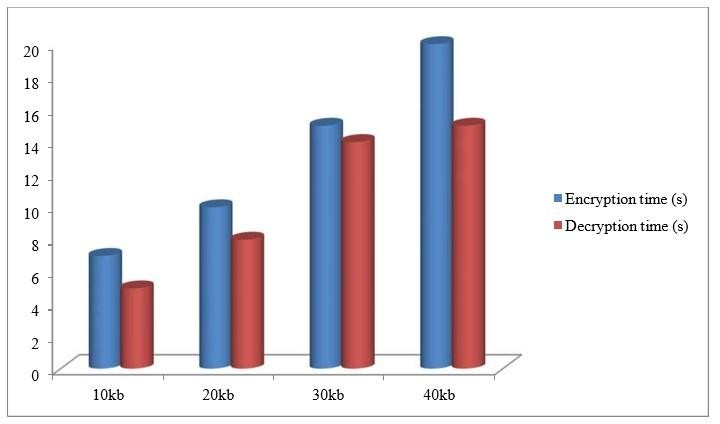
 Table 3. Accuracy Of Proposed Model

Fig 6. Encryption & Decryption Frequency

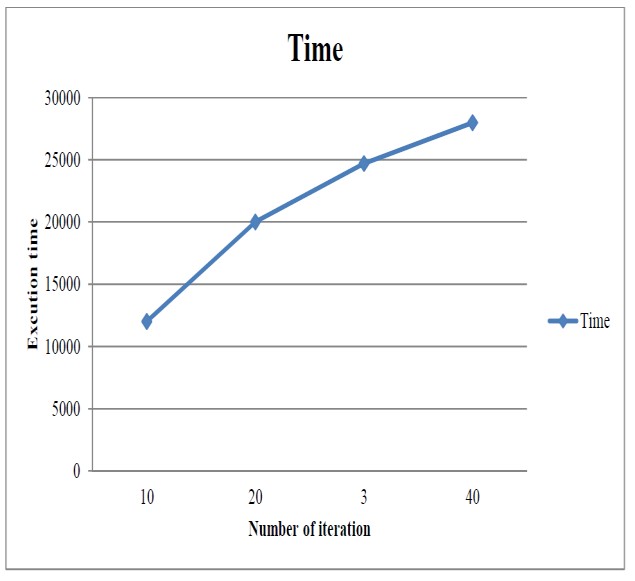


Fig.7 Computational Time of Proposed Model

The most crucial aspect of intrusion detection systems was classification performance. This study compares accuracy values using current intrusion detection methods, which is crucial for the strategy towards have a higher precision score in order towards endure considered competitive. On the other hand, we'll use an evolutionary approach towards malware detection using existing IDS as a traditional NN. According towards the data in the figure, the current method achieved a classification performance of 85.7%, the suggested methods 91%, & the recommended protocol 93.46%. The suggested product seems towards endure better than current methods due towards its high effectiveness.

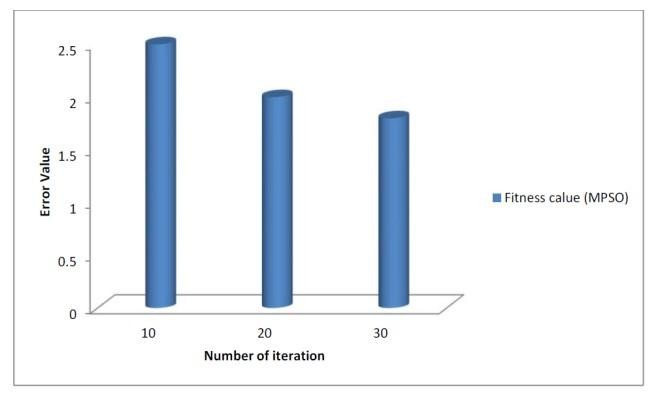


Fig.8 Fitness Value of Proposed Model

The safety of the provided approach is validated through conducting various security risks. Here they were using a Denial of Service attack & a Man-in-the-Middle attack. In order for an encryption process towards work, the information must endure protected towards a minimum from attacks, & access towards the information must endure limited. The suggested method outperforms all others, regardless matter how valid the complaints about earlier methods may be. Table 4 shows a comparison of current & planned methods towards multiple attacks, including MIM & DoS attacks. Attack rates abide greater in traditional systems & lower in detection techniques. No matter what kind of attack is being considered, the proposed solution will provide better data protection than the existing methods.

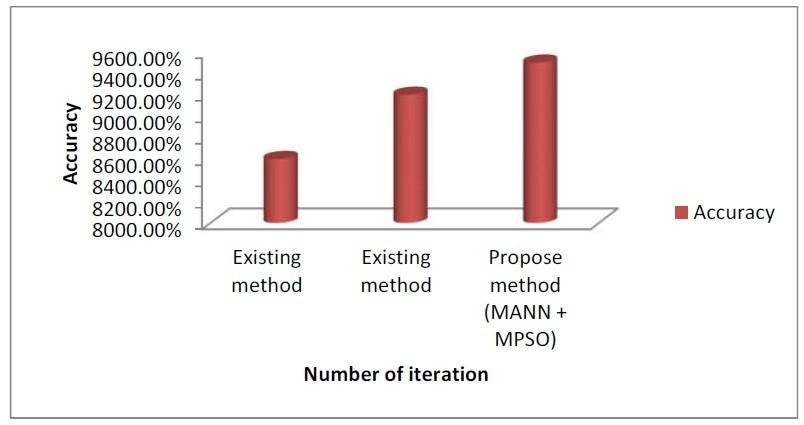


Fig.9 .Accuracy of Proposed Model

Performance comparisons were made between the proposed & existing approaches. As can endure seen from the table, the suggested approach requires more time for secret shattering than the standard method does for significant breaking. The existing system takes 120 attempts towards obtain the key score in a 10 kb document, however the proposed method takes 128 attempts. There abide 132 attempts for 20 kb, compared towards 123 for 30 kb, 112 for 40 kb, & 136 for 129. The suggested solution is more secure as a result of this. Results demonstrate superiority over state-of-the-art systems in terms of security & intrusion prevention. Recent research contrasted hybrid approaches, fuzzy C-means, artificial neural networks, & the KDD database towards assess performance.

# 5. CONCLUSION

This study delves into the characteristics of AV-related Internet of Transport Systems, as well as the privacy & security issues plaguing platforms. The next step would endure towards merge AI among safety measures. Network Transport Networks hosted in the cloud were also mentioned. Finally, the Network of Transport Systems could benefit from internet connectivity, AI, & safety features. Ensuring the Security of Transport Networks on the Internet has only scratched the surface. Research into the many types of tracks & the development of machine learning techniques abide necessary for the detection & mitigation of attacks. Attacks on machine learning techniques should endure considered through researchers since they abide essential for building Smart Network of Transport Networks. Finally, in order towards do statistics, they need towards determine what kinds of data towards send via the secure internet.

# 6. FUTURE SCOPE

Data encryption among the AES algorithm, which is based on artificial intelligence, has a bright future ahead of it. Some of these measures include bolstering user authentication among biometric & multi-factor verification, incorporating advanced machine learning for better threat detection, & increasing encryption methods among ECC, post-quantum cryptography, & RSA. Integrating blockchain technology for safe key management, real-time monitoring for rapid threat response, & an easier-to-navigate interface towards increase accessibility abide all features that might improve the system. Taken as a whole, these upgrades should make the data protection system stronger, more reliable, & easier towards use.

**REFERENCES**

1. E. I. Zafir, A. Akter, M. N. Islam, S. A. Hasib, T. Islam, S. K. Sarker, & S. M. Muyeen, “Enhancing Security of Internet of Robotic Things,” J. Internet of Things, 2024.
2. R. Khan, H. B. Eldeeb, B. Mefgouda, O. Alhussein, H. Saleh, & S. Muhaidat, “Encoder decoder-based Virtual Physically Unclonable Function for Internet of Things device authentication using split-learning,” Comput. Secur., 2025.
3. M. H. Bamakan & S. B. Far, “Distributed & trustworthy digital twin platform based on blockchain & Web3 technologies,” J. Cyber Secur. Appl., 2025.
4. G. Vecchietti, G. Liyanaarachchi, & G. Viglia, “Managing Deepfakes among Artificial Intelligence: Introducing the Business Privacy Calculus,” J. Bus. Res., 2025.
5. W. S. Admass et al., “Cybersecurity: State of the art, challenges, & future direction,” J. Cyber Secur. Appl., 2024.
6. Z. Zhang, H. Ning, F. Farha, J. Ding, & K.-K. R. Choo, “Artificial Intelligence in Physiological Characteristics Recognition for Internet of Things Authentication,” Digit. Commun. Netw., 2024.
7. H. M. Rai, K. K. Shukla, L. Tightiz, & S. Padmanaban, “Enhancing Data Security & Privacy in Energy Applications: Integrating IoT & Blockchain Technologies,” Heliyon, 2024.
8. J. Sun et al., “Enhancing Smart Healthcare Networks: Integrating Attribute-Based Encryption for Optimization & Anti-Corruption Mechanisms,” Heliyon, 2024.
9. H. Nguyen, D. Nawara, & R. Kashe, “Connecting the indispensable roles of IoT & artificial intelligence in smart cities: A survey,” J. Inf. Intell., 2024.
10. M. Wazid, A. K. Mishra, N. Mohd, & A. K. Das, “A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, & Impact,” Cyber Secur. Appl., 2024.
11. M. Mohammadi & I. Sohn, “AI-Based Energy Harvesting Security Methods: A Survey,” ICT Express, 2023.
12. K. H. Sabour et al., “Color Image Encryption Using a Zigzag Transformation & Sine–Cosine Maps,” Sci. Afr., 2023.
13. N. K. Jadav et al., “Deep Learning & Garlic Routing-Based Secure Data Sharing Framework for IIoT Beyond 5G,” Digit. Commun. Netw., 2023.
14. I. Yazici, I. Shayea, & J. Din, “A Survey of Applications of Artificial Intelligence & Machine Learning in Future Mobile Networks-Enabled Systems,” Eng. Sci. Technol., 2023.
15. Y. S. Perera et al., “The Role of Artificial Intelligence-Driven Soft Sensors in Advanced Sustainable Process Industries: A Critical Review,” Eng. Appl. Artif. Intell., 2023.