**Artificial Intelligence based Security Solution for Data Encryption**

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

**Existing Systems**

1. **AES (Advanced Encryption Standard)**
   * **Description:** A widely-used symmetric encryption algorithm, AES encrypts data in fixed block sizes of 128 bits using keys of 128, 192, or 256 bits.
2. **RSA (Rivest-Shamir-Adleman)**
   * **Description:** An asymmetric encryption algorithm used primarily for secure data transmission.
3. **DES (Data Encryption Standard)**
   * **Description:** An older symmetric-key algorithm that encrypts data in 64-bit blocks using a 56-bit key.

**Advantages of Existing Systems**

* **AES:** Provides a good balance between security and performance, suitable for a wide range of applications from secure communications to data storage.
* **RSA:** Offers high security and is particularly useful for securing data transmission and establishing secure connections.
* **DES:** Historically significant and provided a foundation for understanding symmetric encryption, though it's no longer considered secure.

**Disadvantages of Existing Systems**

* **AES:** Key management can be challenging, especially in large-scale deployments.
* **RSA:** Computationally intensive, making it less suitable for encrypting large amounts of data.
* **DES:** Security weaknesses due to its short key length, making it obsolete in modern applications.

**Algorithms Used in Existing Systems**

* AES
* RSA
* DES

**Proposed Systems**

1. **AI-Based Encryption System**
   * **Description:** An encryption system enhanced with artificial intelligence to dynamically adjust encryption strategies based on threat analysis. This system uses machine learning to predict and adapt to emerging security threats in real-time.
2. **Quantum Encryption Algorithms**
   * **Description:** Utilizes principles of quantum mechanics to create encryption algorithms that are theoretically unbreakable by classical computers. This includes algorithms like Quantum Key Distribution (QKD).
3. **Homomorphic Encryption**
   * **Description:** A type of encryption that allows computations to be carried out on ciphertext, thus producing an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

**Advantages of Proposed Systems**

1. **AI-Based Encryption System**
   * **Dynamic Threat Response:** Can adapt to new threats quickly by learning from data, providing enhanced security over static systems.
   * **Improved Efficiency:** AI can optimize encryption processes, reducing the computational load and improving system performance.
2. **Quantum Encryption Algorithms**
   * **Unmatched Security:** Quantum encryption methods are resistant to all known classical computational attacks, providing a high level of security.
   * **Future-Proofing:** As quantum computers become more prevalent, quantum encryption will be essential to counter their capabilities.
3. **Homomorphic Encryption**
   * **Data Privacy:** Allows data to be processed without being decrypted, thus maintaining privacy and security throughout data processing activities.
   * **Cloud Security:** Ideal for secure cloud computing applications where data can be processed by third parties without compromising confidentiality.

**Algorithms Used in Proposed Systems**

1. AI-Based Encryption System
2. Quantum Encryption Algorithms
3. Homomorphic Encryption

**SYSTEM SPECIFICATION:**

**HARDWARE REQUIREMENTS:**

* **System :** Intel i7
* **Hard Disk :** 1 TB.
* **Monitor** : 14’ Colour Monitor.
* **Mouse :** Optical Mouse.
* **Ram :** 8GB.

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 10.
* **Coding Language :** Python.
* **Front-End :** Html. CSS
* **Designing :** Html,css,javascript.
* **Data Base :** SQLite.

**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.