INTERNATIONAL JOURNAL OF ELECTRONICS AND COMPUTER APPLICATIONS

LITERATURE REVIEW

Article access online

OPEN ACCESS

Received: 22.02.2025

Accepted: 10.05.2025

Published: 18.06.2025

Citation: Vyavahare AJ, Pawar DS. (2025). Literature Review: Cryptography Framework using Deep Learning. International Journal of Electronics and Computer Applications. 2(1): 9-11. https://doi.org/10.70968/ijeaca.v2i1.D1011

* **Corresponding author**.

pawar.dipali@moderncoe.edu.in

Funding: None

Competing Interests: None

ISSN
Print: XXXX-XXXX
Electronic: 3048-8257

Literature Review: Cryptography Framework using Deep Learning

A J Vyavahare[1], Dipali S Pawar[2]*

1 Professor, PES's Modern College of Engineering, Pune, Maharashtra, India
2 Assistant Professor, PES's Modern College of Engineering, Pune, Maharashtra, India

Abstract

The Internet of Things has enabled the connection of medical imaging devices to the data infrastructure of the healthcare sector. This advancement, facilitated by the IoT, will accelerate the diagnosis and treatment processes in medical care. The growing dependence on interconnected devices and cloud-based systems opens up potential vulnerabilities for cyber-attacks and unauthorized access to sensitive medical information, which not only threatens patient privacy but also poses significant risks to patient safety and trust in healthcare systems. In a public channel, IoMTS must ensure information security for protection against hacker attacks. Hence, a symmetric encryption and decryption protocol was designed to ensure infosecurity of biosignals and medical images and assist in specific purposes in disease diagnosis.

Keywords: Cryptography; Deep learning; IoMT; Cybersecurity

Introduction

Linking various types of imaging devices utilized for medical imaging to the health data network, known as the Internet of Medical Things (IoMT), will assist physicians in more effectively diagnosing and treating their patients. Recently, numerous healthcare applications leveraging the Internet of Things (IoT) have been introduced to enhance efficiency within the healthcare system and improve patient accessibility. All the data which is being sent or received are susceptible to many active and passive attacks. Therefore, securing the data during transmission is the most significant concern. Cryptography achieves a crucial role to secure the communication in the network and it comes with an incredible solution to supply the needed protection against the stalkers of data. Good cryptography means that the information is encrypted in such a way that a brute force attack on the key or cryptography algorithm are all impossible. Cloud-based application in real-time healthcare systems has been restricted by concerns about data security, system availability, and other related problems. The Internet of Medical Things, also known as IoMT, refers to the application of deep learning methods within this context. It involves the integration of sensors, medical devices, and various healthcare systems into a connected framework to enable the collection, processing, and sharing of medical information aimed at improving health outcomes. The growing

digitization of medical images, records, and personal data in PACS makes them vulnerable to passive or active hacker attacks.

Between 2018 and 2022, 500 ransomware attacks targeting medical institutions around the world were discovered; it's possible that 12,961 organizations were the target of passive hacking attempts.

In public channels, to ensure a proper security level in IoMTS against the active-hacker and passive- hacker attacks, digital data transmissions must be protected using loophole detection, and secure communications protocols must be reinforced. Therefore, we intend to design an intelligent cryptography system for biosignals and medical - image infosecurity, ensuring data confidentiality, integrity, and availability.

Literature Review

The current advancements in digital technologies and the Internet have made safe data transmission via the Internet a difficult problem. The situation with medical data transmission is significantly worse. The rights of patients were violated as a result of illegal access to medical data online.

Federated learning (FL) is a recent development in artificial intelligence which is typically based on the concept of decentralized data. As cyber-attacks are frequently happening in the various applications deployed in real-time, most industrialists are hesitating to move forward in adopting the technology of the Internet of Everything (IoE). FL is a new breed of AI which advocates the on-device AI with the logic of decentralized data learning and extensive training of the prediction models using the sensitive private data of the user.

Today's security requires an increasing number of embedded systems ranging from low-end systems such as smart cards to high-end embedded systems such as routers, firewalls, storage servers and web servers. Embedded systems are used to capture, detect, store, process, transmit, private data in multiple computer systems. Encryption algorithms may be symmetric or asymmetric. Symmetric encryption is fast. It's commonly used for e-commerce transactions because it is fast.

Methodology

Taniya Hasija[(1)] explore the impact of quantum computers on cryptography, particularly focusing on symmetric key cryptography and fundamentals of symmetric key cryptography, delve into algorithmic insights of DES, IDEA, RC5, and AES and examine the vulnerabilities and challenges posed by quantum computers to these fundamental cryptographic approaches. This paper has explored symmetric key cryptography, providing a comprehensive understanding of its algorithms, algorithmic insights, and the challenges it faces in the era of quantum computing. Symmetric key cryptography has been a cornerstone of secure communication, relying on computational complexity for its strength.

Nadhan, A. S[(2)] Utilizing the ResNet-50 architecture, we perform the mapping between different image representations. The integration of these "hidden properties" into the learning model allows for the encryption technique to be customized for each specific domain. In the initial phase of decryption, we employ reconstructive networks to transform the encrypted image back into its "plaintext" format. After the hidden entities are uncovered, a Return on Investment (ROI) framework can be established, and data mining can be streamlined by directly accessing the user's local information environment.

Ismail Negabi[(3)] Proposes a design for a CNN that is nonlinear and reversible and can perform encryption and decryption processes with high performance and a very low error rate. The algorithm which must be implemented by CNN is the AES algorithm. CNN provides a useful means of controlling nonlinear systems The ability of Multi-Layer Perceptron (MLP) to mimic any input/output relationship makes it the most popular type of direct acting CNN. The MLP is designed as batch training (Block Adaptive) since it adjusts the weights following the presentation of the full block of training data. The block adaptation is more robust since the learning step is averaged over all the learning models.

Chen, P Y[(4)] uses a symmetric encryption and decryption protocol designed to ensure infosecurity of biosignals and medical images and assist in specific purposes in disease diagnosis. For a symmetric cryptography scheme, this study proposed a key generator combining a chaotic map and Bell inequality and generating unordered numbers and unrepeated 256 secret keys in the key space. Then, a machine learning - based model was employed to train the encryptor and decryptor for both biosignals and image infosecurity. After secure - data transmission, a case study is conducted for classifying medical images.

Kaur, M[(5)] proposes a lightweight image encryption approach for medical Internet of Things (MIoT) networks using compressive sensing and a modified seven-dimensional (MSD) hyperchaotic map. Initially, the 7D hyperchaotic map is modified to generate more secure and complex secret keys. SHA-512 is used to create the initial conditions for MSD, which ensures its sensitivity towards input images.

Syamamol T[(6)] develops a compact convolutional neural network by enhancing a previously existing combination of neural networks. Novel neural networks along with previous neural networks both have their own implementations of the side-channel analysis used in comparative trials. Statistically, the new network has better accuracy, quicker convergence, and more robustness. As part of the research, heatmaps were provided as a means of data visualisation. The critical interval concentration is higher, and the heat value is higher in the new network. Conventional neural networks, which serve as

the foundation for various kinds of neural networks, perform much worse than side channel studies based on feature fusion networks.

Deep Learning and Artificial Neural Networks methods are powerful AI techniques for solving complex problems. In the Deep Learning approach, the input data passes through various complicated hidden layers and produces a target output. The meaningful results can be produced by efficient feature extraction methods introduced in Deep Learning algorithms. Nowadays, Cryptography and cryptanalysis are the emerging trends of deep learning. Deep learning based cryptosystem, attacks classification, privacy preservation and encryption algorithm analysis are the various research areas in deep learning based cryptosystem. Deep learning based cryptanalysis can be applied in the field of light weight block ciphers.

Francisco Quinga Socasi [4] proposed the potential of using a deep neural network called autoencoder for cryptography concerns. The objective of this is to develop an alternative encryption system, taking advantage of the potential that integration of ANN and cryptography uses. Experimental results of the proposed system with real world text files with different sizes shown in this paper. Furthermore, experimental tasks were performed to evaluate the robustness of the system against brute force attack.

Conclusion

The recognition of cryptographic algorithms serves as the foundation for cryptanalysis, which can assist in effectively recovering the keys. AES, 3DES, and RSA, where each cipher has its own strong and weak points. Traditional cryptography ciphers apply exhaustive serial operations using complex formulas and huge prime numbers, making encryption and decryption computing consuming and somehow vulnerable. In this paper we studied deep learning with different cryptographic techniques, which is also very meaningful for the development of the modern cryptographic framework.

References

1) Hasija KRT, Ramkumar. Symmetric Key Cryptography: Review, Algorithmic Insights, and Challenges in the Era of Quantum Computers. *The 23 14th International Conference on Computing Communication and Networking Technologies DOI*. Available from: https://doi.org/10.1109/ICCCNT56998.2023.1030708.
2) Nadhan AS, Jacob IJ. Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. *Biomedical Signal Processing and Control*. 2024;88:105511. Available from: https://dx.doi.org/10.1016/j.bspc.2023.105511.
3) Lata K, Cenkeramaddi LR. Deep Learning for Medical Image Cryptography: A Comprehensive Review. *Applied Sciences*. 2023;13(14):8295. Available from: https://dx.doi.org/10.3390/app13148295.
4) Chen PY, Cheng YC, Zhong ZH, Zhang FZ, Pai NS, Li CM, et al. Information Security and Artificial Intelligence–Assisted Diagnosis in an Internet of Medical Thing System (IoMTS). *IEEE Access*. 2024;12:9757–9775. Available from: https://dx.doi.org/10.1109/access.2024.3351373.
5) Kaur M, AlZubi AA, Singh D, Kumar V, Lee HN. Lightweight Biomedical Image Encryption Approach. *IEEE Access*. 2023;11:74048–74057. Available from: https://dx.doi.org/10.1109/access.2023.3294570.
6) Syamamol T, Manjith BC. A Review of Deep Learning Application in Cryptography. *Proceedings of ACM/CSI/IEEECS Research & Industry Symposium on IoT Cloud For Societal Applications*.